Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Informačná bezpečnosť

Manažment IB

doc. RNDr. Daniel Olejár, PhD.,
mimoriadny profesor FMFI UK

KPMG
cutting through complexity™

Upozornenie

Táto prezentácia bola vytvorená v rámci projektu MF SR "Vypracovanie štandardov základných znalostí, metodických materiálov, analýz dokumentov a súvisiacich vykonávacích predpisov a realizácia školení pre oblasť informačnej bezpečnosti." pre MF SR. Je určená pre účastníkov vzdelávania poriadaného MF SR. Rozmnožovanie a iné upravy textov prednášky v papierovej a elektronickej forme, preberanie častí textov do iných prednášok, vystavovanie na webe a iné používanie tejto prezentácie je možné len s písomným súhlasom MF SR a s uvedením úplnej citácie.

Obsah kurzov IB

1. **Úvod do informačnej bezpečnosti**
2. **Manažment IB**
3. Architektúry a modely
4. Riadenie prístupu
5. Aplikačná bezpečnosť
6. Bezpečnosť prevádzky
7. Fyzická bezpečnosť
8. Kryptológia
9. Internet a počítačové siete
10. Kontinuita činnosti
11. Právo a etika

Obsah prednášky

- Vzdelávanie v IB
- Základné pojmy
- Manažment IB
- Klasifikácia informácie
- Prehľad štandardov

Informačná bezpečnosť
vzdelávanie

Prečo potrebujeme informačnú bezpečnosť?

- V tejto spoločnosti sa asi nemusíme presviedčať o potrebe IB, ale často to však musíme vysvetľovať laikom
- Preto:
  - Každá organizácia má nejaký zmysel existencie (poslanie)
  - Na jeho naplnenie vyvíja nejakú činnosť
  - Na túto činnosť potrebuje zdroje
  - Informácie sú kľúčovým zdrojom
  - Aby sa dalo spracovávať potrebné množstvo informácií, používajú sa IKT
  - Narušenie IKT a informácií môže organizácii spôsobiť problémy
  - Bez IKT sa informácie v požadovanom množstve a čase nedajú spracovávať
  - IKT a informácie potrebujeme chrániť ► dostatočná úroveň IB je nutnou podmienkou fungovania organizácie

Ľudský činiteľ

- Pri riešení IB (Národná stratégia IB, Kritická infraštruktúra, Prehľady stavu IB) narážame na závažný problém:
  - IKT sa používajú skoro všade
  - Nemôžeme bez nich dobre existovať (kritická infraštruktúra)
  - Stali sa predmetom záujmu zločincov, podvodníkov, teroristov, politických aktivistov, profesionálnych útočníkov
  - Nedá sa spoliehať na to, že sme nezaujímaví, bezvýznamní (hrozby útokov sú reálne)
  - Úroveň IB je nedostatočná (ľudia, znalosti, prostriedky, podpora)
- IB je rovnako veľká a zložitá na Slovensku, ako v Nemecku alebo v USA. Nemáme dosť kvalifikovaných ľudí na adekvátne zabezpečenie svojich IKT (problém aj najvyspelejších krajín)

Vzdelávanie v kontexte Národnej stratégie IB

- Národná stratégia identifikovala problémy a stanovila priority SR v IB
- Kľúčový predpoklad: musíme mať ľudí, ktorí IB rozumejú a dokážu ju presadzovať
- Ale
  - S IKT pracujú dnes skoro všetci
  - IB môže narušiť hocikto – obyčajný používateľ aj privilegovaný administrátor, vedúci pracovník zlým rozhodnutím
- Vzdelávať potrebujeme všetkých, ktorí pracujú s IKT
- Našťastie všetci nemusia vedieť všetko

Koho to teda potrebujeme vzdelávať v IB?

- Kategorizácia podľa potrieb
  - Laici (neprivilegovaní používatelia)
  - Vedúci pracovníci
  - Informatici, ktorí sa nešpecializujú v IB
  - IB špecialisti
  - Učitelia/lektori IB
- Špecializácií v IB existuje podstatne viac
- Ostaneme pri základnom členení, časom jemnejšie členenie kategórií na roly, napr. informatici
  - Manažéri IKT
  - Správcovia a operátori systémov a sietí
  - Vývojári

Koncepcia vzdelávania v IB

- Rámcový návrh schválila Vláda SR (2009)
- Teraz sa konkretizuje a realizuje (MF SR 2010, 2012)
- Znalostné štandardy pre jednotlivé kategórie
- Úvodné školenia (vedúci pracovníci, informatici a špecialisti IB; učitelia/lektori a laici)
- Učebnice
- Postgraduál pre špecialistov
- Tematické bloky
- Obnovovacie kurzy
- Metodické materiály
- Odborné semináre a konferencie
- Špecializácia v rámci štúdia informatiky (časom právna informatika)

Vzdelávanie v IB (špecialisti)

- Nemáme IB špecialistov? Tak si ich pripravíme! Koľko?
- USA 30.000, SR ???
- Nebude to jednoduché, lebo
  - „Základná“ a „aplikovaná“ IB
  - IB je nová, interdisciplinárna oblasť, ktorá sa rýchle rozširuje (zložitý predmet skúmania = hrozby voči IKT a spôsoby ochrany pred nimi)
  - priveľký rozsah poznatkov presahujúci možnosti jedného človeka (pozri sústavu špecializácií amerického DoD)
  - V SR Neexistuje študijný odbor (v zahraničí sa už IB dajú študovať špecifické zamerania – kryptológia, bezpečnosť systémov, právo, manažment),
  - Keby aj, nie je to odbor pre pregraduálne štúdium
- Špecialisti v IB sú samouci, odkázaní na celoživotné vzdelávanie (špecifickosť potrieb a nutnosť neustále si dopĺňať vzdelanie)
- Vzdelávanie v IB je lukratívna komerčná záležitosť (veľa balastu, málo kvality, chýbajú učitelia IB)

Vzdelávanie v IB (laici)

- bezpečnosť informačných systémov nezávisí len od niekoľkých málo profesionálov, ale aj od laických používateľov, manažérov a pod.
- popri zvyšovaní odbornej úrovne profesionálov (IKT a IB) potrebujeme budovať aj bezpečnostné povedomie laických používateľov IKT
- je ich veľa a vzdelávať laikov býva ťažšie, ako školiť profesionálov
  - Motivácia (načo)
  - Obsah (čo)
  - Metodika (ako)
  - Lektori (kto)
- Školy žiakov v rámci informatiky (vyškolenie učiteľov, učebnice)
- Dospelí laici
  - V organizáciách
  - ECDL
  - Samovzdelávanie, masovokomunikačné prostriedky (?)

Ostatní

- Vedúci pracovníci (bezpečnostné minimum, kurzy, učebnica) hľadáme vhodné formy
- Informatici
  - doplnenie znalostí z IB
  - V ideálnom prípade znalosti potrebné na to, aby implementovali opatrenia a vedeli komunikovať so špecialistami IB
  - Reálne: z nich budú špecialisti v IB (technicky orientovaní)
  - Aj lektori IB
- Učitelia IB
  - Poznatky a metodika vzdelávania
  - Základná úroveň (laici) doškolenie učiteľov informatiky
  - Vyššia ?? Špecialisti IB + didaktické skúsenosti

Ciele kurzu

- Tento kurz je súčasťou systému vzdelávania v IB, príprava niekoľko rokov:
  - Nevystačíme so všeobecnými poznatkami
  - Konkrétne znalosti rýchle zastarávajú
  - Individuálne štúdium je časovo náročné a málo efektívne
- Žiaden rýchlokurz geniality
  - Doplnenie a systematizácia poznatkov o IB
  - Vytvorenie uceleného obrazu o IB
  - Informačné zdroje
  - Argumenty na presadzovanie IB v organizácii
  - Námety pre zvyšovanie bezpečnostného povedomia kolegov
  - Použiteľné riešenia

Pripomíname: Kurz je len čiastkové riešenie, na budovanie a udržiavanie potrebného know-how v dostatočnom rozsahu potrebujeme ucelený systém vzdelávania

Obsah kurzu (1)

- Pokrýva navrhované znalostné štandardy pre špecialistov IB v plnom rozsahu (pozor, rozlišujeme rozsah a úroveň)
- Štandardy
  - kompatibilné s medzinárodnými znalostnými štandardami CBK (Common Body of Knowledge) SANS Institute a EBK (Essential Body of Knowledge) amerického HSD
  - Pokrývajú všetky oblasti špecifikované v rade noriem ISO/IEC 27000, z ktorých vychádzajú bezpečnostné štandardy Výnosu MF SR
- obsah je preusporiadaný podľa ISO/IEC 27002

Obsah kurzu (2)

- Obsah kurzu je usporiadaný do 10 tematických oblastí:
  - Manažment IB
  - Architektúry a modely
  - Riadenie prístupu
  - Aplikačná bezpečnosť
  - Bezpečnosť prevádzky
  - Fyzická bezpečnosť
  - Kryptológia
  - Internet a počítačové siete
  - Kontinuita činnosti
  - Právo a etika
- Vrátime sa k nim na konci úvodnej prednášky

Spôsob vzdelávania

- Základ: prednášky
- Samoštúdium
  - Učebnica
  - Doplnkové zdroje uvedené na prednáškach a v učebnici
- Záverečné testovanie (bude?)

Potrebujeme nastaviť úroveň, odladiť obsah a formu, nastaviť hodinové rozsahy.

Pripomienky a nápady vedúce k vylepšeniu vzdelávania sú vítané.

Základné pojmy

Čo je informačná bezpečnosť (IB)?

- Často sa vyskytujúci dôležitý pojem, ale nie je poriadne definovaný a používa sa v rozličných významoch (=zdroj nedorozumení)
  - Želaný stav IKT (všetko funguje v súlade s požiadavkami a potrebami organizácie) [úroveň IB v organizácii]
  - Činnosť smerujúca k dosiahnutiu ideálneho stavu [Systém manažmentu informačnej bezpečnosti]
  - Medziodborová vedná disciplína zaoberajúca sa vývojom metód ochrany informácie a IKT
- Pojem IB budeme používať vo všetkých troch významoch, najmä však v druhom

Ciele informačnej bezpečnosti

- Všeobecný cieľ je jasný (mať vždy včas k dispozícii informácie, na ktoré sa môžeme spoľahnúť), ale treba ho konkretizovať, aby bolo možné na jeho dosiahnutie niečo spraviť
- Informácie sú zaznamenané v podobe údajov (údaj = **forma**, informácia = **obsah**), ak to nebude podstatné, budeme pojmy údaj a informácia chápať ako synonymá
- Spracovanie informácií: vytváranie, získavanie, prenos, uchovávanie, vlastné spracovávanie, využívanie, archivovanie, ničenie informácií
- Čo potrebujeme chrániť: informáciu od vytvorenia až po zničenie

  Chrániť = zaistiť dôvernosť, integritu, dostupnosť údajov

Základné bezpečnostné požiadavky

- **Dôvernosť údajov (confidentiality)** – k informácii, ktorú údaje obsahujú nemajú prístup nepovolané osoby
- **Integrita údajov (data integrity)** – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla
- **Dostupnosť údajov (data availability)** – oprávnená osoba má údaje k dispozícii kedykoľvek, keď o to požiada
- CIA = základné bezpečnostné atribúty údajov/informácie alebo základné bezpečnostné požiadavky na ochranu údajov

Poznámky

- Okrem CIA existujú aj iné bezpečnostné požiadavky na ochranu údajov
- Rozdiel medzi prístupom k údajom a prístupom k ich obsahu
- Spôsob zabezpečenia dôvernosti (ochrana prístupu a šifrovanie)
- Dôvernosť – všeobecný pojem a dôverné = druhý stupeň klasifikačnej schémy utajovaných skutočností
- Integrita: absolútna požiadavka – nemennosť údajov – je nerealistická
- Riešenie integrity – ochrana prístupu, logy a kryptografické prostriedky
- Dostupnosť – prípustné omeškanie, alebo max. % nedostupnosti

Čo chrániť?

- Informácia počas celého životného cyklu – rôzne formy, v rozličných systémoch, rozliční ľudia,
- Rôzne informácie môžu mať rôzne požiadavky na ochranu
- Vnesieme do ochrany informácií systém/poriadok:
- **Aktívum (asset)** – čokoľvek, čo má pre organizáciu hodnotu a vyžaduje si ochranu (príklady: pracovné procesy, činnosti a služby organizácie, informácie, hw, sw, sieť, personál, sídlo, organizačná štruktúra, dobré meno,...)

Základné pojmy IB (1)

- ***Hrozba*** – objektívne existujúca možnosť, ktorej naplnenie môže poškodiť niektoré aktívum (prírodné javy, technické poruchy, chyby, omyly, ľudia)
- Hrozba má ***nositeľa*** (hrozba záplavy, nositeľ rieka, kanalizačné potrubie)
- ***Zraniteľnosť*** : chyba, nedostatok, spôsob použitia aktíva, ktoré spôsobujú, že sa hrozba voči aktívu môže uplatniť (príklad: hrozba krádeže, zraniteľnosť – umiestnenie počítača v nezabezpečenej miestnosti)

Základné pojmy IB (2)

- Existujú rozsiahle katalógy hrozieb aj zraniteľností
- Naplnenie hrozby, v širšom zmysle akákoľvek odchýlka od stanovených pravidiel, ktorá môže viesť k narušeniu bezpečnosti – ***bezpečnostný incident***
- ***Útok*** – cieľavedomý pokus o narušenie informačnej bezpečnosti
- Pôvodca útoku: ***útočník***
- ***Útočný potenciál:***
  - Motivácia
  - Znalosti
  - Príležitosť
- Príklad: krádež PC a krádež údajov z databázy organizácie

Základné pojmy IB (3)

- ***Dopad*** – negatívne dôsledky toho, že sa naplnila hrozba voči aktívu (ukradnutý počítač, prezradené heslo)
- ***Riziko*** = veličina umožňujúca merať prakticky závažnosť hrozieb: stredná hodnota dopadu hrozby (dopad x pravdepodobnosť toho, že hrozba nastane)
- Príklad: organizácia má 100 PC, pravdepodobnosť poruchy 15%, cena opravy 200 Euro, riziko poruchy je 100 x 0.15 x 200 = 3000 Euro

Základné pojmy IB (4)

- *opatrenie*: riešenie (technické, organizačné, personálne, právne, iné), ktoré znižuje riziko (pravdepodobnosť naplnenia a/alebo dopad hrozby)
- *Analýza rizík* – stanovenie a vyhodnotenie rizík vyplývajúcich z hrozieb relevantných vo vzťahu k aktívam organizácie
- *Hranica akceptovateľného rizika* – úroveň rizika, ktorú sa organizácia rozhodla znášať (napr. preto, lebo znižovanie rizika pod akceptovateľnú úroveň nie je z ekonomického hľadiska efektívne)

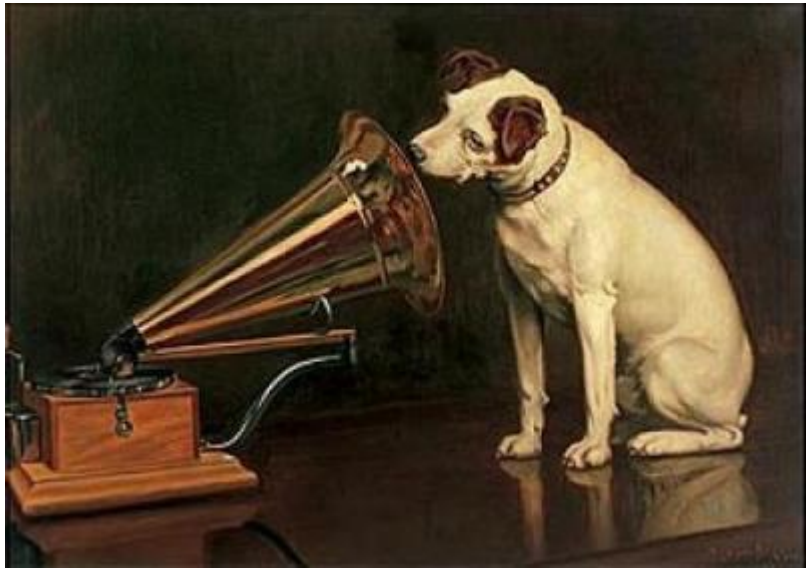
Základné pojmy IB (5)

- Informačné a komunikačné technológie (IKT, anglicky ICT)
- Informačný systém – ucelený systém, ktorý slúži na spracovanie informácie (A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NIST SP 800-53)
- Zaujímajú nás IS postavené na IKT
- Systém a jeho okolie (hranica systému)
- Bezpečnostné prostredie/okolie systému – všetko, čo má vplyv na bezpečnosť systému

Základné pojmy IB (6)

- *His master voice*, (Ilustračný obr. Wikimedia Commons) alebo ako zistiť , kto je kto vo virtuálnom priestore?

- Entita
- Identita
- Oblasť použiteľnosti identity
- Identifikátor
- Identifikácia
- Autentizácia



Základné pojmy IB (7)

- Veľa pojmov s predponou cyber-
- Nemá to logiku, lebo
- Kybernetika = veda o riadení v živých organizáciách a strojoch (Wiener, Ashby, Ampér)

- *William Gibbson Neuromancer* 1984 Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.

Základné pojmy IB (8)

- William Gibson o cyberspace

  All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.

Základné pojmy IB (9)

- V súčasnosti cyberspace označuje
  - informačnú a komunikačnú infraštruktúru
  - Sociálne vzťahy budované na základe a udržiavané prostredníctvom Internetu, sociálnych sietí a pod.
- V SR digitálny priestor
  - Národná informačná a komunikačná infraštruktúra a
  - jej okolie
- Kybernetický priestor
  - Podpriestor digitálneho priestoru, v ktorom sa spracovávajú utajované skutočnosti
- Cybercrime: kybernetický zločin
  - Trestné činy, pri ktorých sa počítače používajú ako nástroje
  - Trestné činy zamerané na IKT

Základné pojmy IB (10)

- Ďalšie pojmy zavedieme v texte
- V učebnici krátky výkladový slovník pojmov IB (250 pojmov)
- veľký výkladový slovník IB MF SR (1500 pojmov) mal byť koncom roka na webe

Manažment informačnej bezpečnosti

Obsah kurzov IB

1. Úvod do informačnej bezpečnosti
2. **Manažment IB**
3. Architektúry a modely
4. Riadenie prístupu
5. Aplikačná bezpečnosť
6. Bezpečnosť prevádzky
7. Fyzická bezpečnosť
8. Kryptológia
9. Internet a počítačové siete
10. Kontinuita činnosti
11. Právo a etika

Obsah prednášky

- Bezpečnostná politika
- Analýza rizík
- Systém manažmentu informačnej bezpečnosti

Prečo máme riešiť IB v organizácii?

- Objektívna potreba ochrany informácií
- (najdôležitejšie) legislatívne požiadavky na ochranu informácií
  - Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
  - Výnos č. 312/210 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
  - Zákon 45/2011 Z. z. o kritickej infraštruktúre,
  - Zákon č. 215/2004 Z.Z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
  - Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
  - Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Podrobnejšie v prednáške o legislatíve a etike

Ako?

- Celá škála prístupov (od najhoršieho po najlepšie)
  - Nerobiť nič (a dúfať, že sa nič nestane)
  - *Ad hoc* prístup (reakcia na objavujúce sa problémy)
  - Zákonné minimum (Potemkiniáda – bezpečnosť na papieri)
  - Outsourcing IB (zaplatíme si IB)
  - Systematické riešenie bez certifikácie
  - Certifikované riešenie
- Výnos MF SR o štandardoch pre ISVS definuje ako štandard ISMS (systematické riešenie)

Kde začať?

- Prirodzené požiadavky na systematické riešenie
  - Dostatočná úroveň bezpečnosti, primeraná pre podmienky organizácie
  - Primerané náklady na zavedenie a udržiavanie
  - Trvalá/dlhodobá udržateľnosť
  - Splnenie zákonných požiadaviek
  - Využitie toho, čo už organizácia má spravené
- Nemusíme objavovať to, čo je známe:
  - ISO normy radu 27000 (manažment IB)
  - Metodické materiály amerického NISTu, nemeckého BSI a iných inštitúcií
  - (budeme o nich hovoriť v samostatnej prednáške)

Ideme zaviesť ISMS v organizácii

- ISMS = Information security management system (Systém manažérstva informačnej bezpečnosti)
- Plán
  - Rámcová stratégia
  - Analýza existujúceho stavu
  - Možné riešenia
  - Výber a implementácia riešenia
  - Monitoring, kontrola a udržiavanie/zmeny riešenia
- Poznámka:
  - BSI – bezpečnostný proces
  - Bezpečnostný projekt

Bezpečnostná politika

- Stratégia IB v organizácii má podobu dokumentu Politika informačnej bezpečnosti (Bezpečnostná politika) organizácie
- **Úlohou Bezpečnostnej politiky** je povedať každému zamestnancovi organizácie čo môže, čo nesmie, čo musí a za čo je zodpovedný
- Bezpečnostná politika
  - Pracovná skupina na vypracovanie
  - Posúdená, pripomienkovaná a schválená vedením
- Musí byť dostupná každému zamestnancovi, prípadne externým spolupracovníkom

Obsah bezpečnostnej politiky (1)

- Deklarácia vedenia organizácie
  - O význame ochrany informácií
  - Identifikácia hlavných aktív
  - Stanovenie cieľov IB v organizácii
  - Podpora vedenia organizácie pri ich napĺňaní
- Oblasť použiteľnosti bezpečnostnej politiky
- Štruktúra a obsah bezpečnostnej dokumentácie nadväzujúcej na bezpečnostnú politiku
- Stanovenie zodpovednosti zamestnancov za presadzovanie a dodržiavanie bezpečnostnej politiky
- Klasifikácia informácie (klasifikačná schéma)
- Spôsob analýzy rizík a hranica akceptovateľného rizika

Obsah bezpečnostnej politiky (2)

- Monitoring, kontrola a audit informačných a komunikačných systémov (IKS) organizácie
- Riešenie bezpečnostných incidentov
- Zaistenie kontinuity činnosti organizácie
- Správa bezpečnostnej politiky organizácie (riadne a mimoriadne revízie bezpečnostnej politiky)

* * *

Poznámky k Bezpečnostnej politike

- Bezpečnostná politika nerieši všetko – spravidla vysokoúrovňový dokument (1. úroveň)
- Podrobnosti v špecializovaných bezpečnostných politikách alebo bezpečnostných štandardoch (2. úroveň)
- Pravidlá na uplatňovanie bezpečnostnej politiky: bezpečnostné praktiky (3. úroveň)
- Pojmy Bezpečnostná politika, Bezpečnostný zámer, Bezpečnostný projekt, Bezpečnostný plán a iné sa (ani v legislatíve) nepoužívajú konzistentne

Analýza rizík (1)

- potrebujeme poznať skutočné bezpečnostné potreby systému alebo organizácie
- Nástroje
  - Analýza rizík (ISO/IEC 27005)
  - Gap analysis (porovnanie so želaným stavom)
- Kto ju bude robiť
  - Vlastní zamestnanci (asi nie)
  - Externí špecialisti (účasť vlastných zamestnancov je aj tak nevyhnutná)
- Plán: rozsah analýzy (čoho sa bude týkať)

Analýza rizík (2)

- Popis systému a všetkých bezpečnostne relevantných skutočností
- Identifikácia
  - aktív (vlastníci, umiestnenie)
  - (relevantných) hrozieb
  - bezpečnostných požiadaviek (legislatíva)
  - existujúcich opatrení
  - Zraniteľností
  - Dopadov hrozieb

Analýza rizík (3)

- **Odhad rizík**
- Dva základné prístupy:
  - Kvantitatívny (číselné vyjadrenie)
  - Kvalitatívny (slovné vyjadrenie: {pravdepodobnosť, dopad, riziko} → {vysoké, stredne vysoké, nízke}
- riziko = pravdepodobnosť * dopad hrozby
- Výsledok odhadu rizík = zoznam riziko + odhad; napr. (prezradenie prístupových hesiel; vysoké riziko)

Analýza rizík (4)

- Pri ohodnotení dopadov sa zohľadňuje (ISO/IEC 27005)
  - úroveň klasifikácie postihnutých informačných aktív,
  - 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 a
  - Život a zdravie ľudí

Analýza rizík (5)

- Úroveň dopadov: nízka, stredná a vysoká
- Napr. dopad je **vysoký** (katastrofický) ak strata dôvernosti, integrity alebo dostupnosti má veľmi závažný až katastrofický negatívny vplyv na činnosť organizácie, jej aktíva alebo osoby.
- 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,
  - veľkú až katastrofickú ujmu osobám (vrátane život ohrozujúcich zranení až smrti osôb).
- Podrobnosti v učebnici

Analýza rizík (6)
pravdepodobnosť

Označenie	pomenovanie	poznámka
0	nulová	Udalosť nenastane
1	nízka	Udalosť ešte nenastala, alebo nastala raz za niekoľko rokov
2	stredná	Raz za rok
3	vysoká	Niekoľkokrát mesačne/týždenne

Analýza rizík (7)

dopad→ pravdepodobnosť ↓	nízky	stredný	vysoký
nulová	nulové	nulové	nulové
nízka	nízke	nízke	stredné
stredná	nízke	stredné	vysoké
vysoká	stredné	vysoké	vysoké

Analýza rizík (8)

- **Vyhodnotenie/ohodnotenie rizík**
  - Porovnanie odhadnutej rizík s kritériami na ohodnotenie rizík
  - Potrebná súčinnosť majiteľov aktív
- Výsledok
  - Ktorými rizikami sa organizácia zaoberať (stanovenie priorít)
  - Ktoré riziká akceptuje (ale bude spravovať)

Ošetrenie rizík

- Máme zoznam rizík podľa závažnosti
- 4 možnosti:
  - Redukcia rizika (prijatie opatrení na zníženie pravdepodobnosti a/alebo dopadu hrozby na aktívum)
  - Prijatie rizika (ak jeho úroveň nepresahuje úroveň akceptovateľného rizika)
  - Vyhnutie sa riziku (iné riešenie, napr. presťahovanie výpočtových kapacít na bezpečnejšie miesto)
  - Prenesenie rizika (zapojenie tretej strany – poistenie, outsourcing bezpečnostných služieb, zmluvné podmienky – zásah do x hodín)

Po analýze rizík

- Analýzu rizík robia odborní pracovníci, ale návrh na ošetrenie rizík sa týka chodu organizácie (opatrenia) – schvaľuje vedenie (v norme = akceptovanie rizík)
- Informovanie o rizikách (všetky zainteresované strany)
- Implementácia opatrení
- Monitorovanie rizík a revízie odhadu/ohodnotenia rizík (zmeny)
- Celý proces = spravovanie rizík (podstata zaistenia IB v organizácii)
- Metaúroveň: posudzovanie a vylepšovanie samotného systému spravovania rizík

Systematický prístup k IB

- Zaistenie potrebnej úrovne IB v organizácii – trvalý proces
- Opatrenia na zaistenie IB zasahujú do činnosti (procesov) organizácie
- Potreba súčinnosti všetkých zamestnancov a tretích strán (nedá sa uplatniť uniformný prístup, lebo majú rôzne práva aj povinnosti)
- Nie je zadarmo (náklady na IB sa pritom ťažko zdôvodňujú)
- V malých systémoch/organizáciách sa možno dá uplatňovať *ad hoc* prístup (problém – riešenie), v ostatných je potrebné zaviesť nejaký systém manažmentu IB
- ISO rad noriem 27000 venovaných manažmentu IB (budeme o nich ešte hovoriť)
- Bezpečnostné štandardy Výnosu o štandardoch pre ISVS vychádzajú z normy ISO/IEC 27002
- Rozdiel: mať v organizácii systém manažmentu IB a mať certifikovaný systém manažmentu IB v súlade s ISO 27001-2
- Výnos MF SR nepožaduje certifikáciu

Požiadavky na ISMS

- ISO/IEC 27001 požiadavky na
  - Vytvorenie
  - Implementáciu,
  - Prevádzku
  - Monitoring
  - Revízie
  - Údržbu
  - Vylepšovanie ISMS
- Stručný (14 strán) a všeobecný štandard, na ilustráciu
- The organization shall determine the need for internal and external communications relevant to the information security management system including:
  - what to communicate;
  - when to communicate;
  - to whom it will communicate.
- Zaujímavý z hľadiska certifikácie ISMS

Prehľad systému manažmentu IB

- Budeme vychádzať z ISO noriem radu 27000, najmä ISO/IEC 27002
  - Bezpečnostná politika
  - Organizácia IB
  - Správa aktív
  - Personálna bezpečnosť
  - Fyzická bezpečnosť
  - Manažment vzťahov s dodávateľmi/poskytovateľmi služieb
  - Prevádzka systémov a komunikácie
  - Manažment aplikačných sieťových služieb
  - Riadenie prístupu
  - Obstarávanie, vývoj a údržba systémov
  - Riešenie bezpečnostných incidentov
  - Manažment kontinuity činnosti
  - Súlad s legislatívou

Prehľad systému manažmentu IB (2)

- Bezpečnostná politika
- O obsahu a význame sme už hovorili
- Vedenie Bezpečnostnou politikou
  - definuje smerovanie IB v organizácii
  - Deklaruje záväzok/odhodlanie presadzovať ju

Prehľad systému manažmentu IB (3)
Organizácia IB

- Cieľ: vytvoriť organizačné podmienky pre zavedenie (ak nie je) a riadenie IB v organizácii
- Vedenie:
  - Schvaľuje politiku IB
  - Zaraďuje zamestnancov do bezpečnostných rolí (zriaďuje bezpečnostný manažment a schvaľuje štruktúru bezpečnostných rolí)
  - Posudzuje a reviduje implementáciu IB v organizácii
  - Presadzuje IB v organizácii (napr. zohľadnenie bezpečnostných aspektov v projektovom manažmente)
- Organizácia nadväzuje a udržuje kontakty na štátne inštitúcie, relevantné organizácie, dodávateľov a poskytovateľov služieb pre prípad mimoriadnych udalostí

Prehľad systému manažmentu IB (4)
Správa aktív

- Cieľ: adekvátna ochrana aktív organizácie
- Inventarizácia aktív
  - každé aktívum musí mať vlastníka, zodpovedného za jeho správu a ochranu
  - Pre informačné aktíva: pravidlá používania (vlastník)
- Klasifikácia informácie
  - Úroveň ochrany
  - Spôsob nakladania s klasifikovanými údajmi
- Vedenie organizácie:
  - Schvaľuje klasifikačnú schému
  - Iniciuje inventarizáciu aktív

Prehľad systému manažmentu IB (4)

Personálna bezpečnosť

- Cieľ: aby zamestnanci, externí spolupracovníci a tretie strany
  - Rozumeli svojim povinnostiam a vedeli, za čo nesú zodpovednosť
  - Stačili na rolu, do ktorej sú zaradení
  - A tým sa redukovalo riziko podvodu a krádeže
- Pred zamestnaním
  - Výber zamestnancov
  - Povinnosti v IB zaradené do pracovnej zmluvy (rámcovo)
- Počas zamestnania
  - Informovať zamestnancov o povinnostiach vyplývajúcich z roly
  - Úvodné školenie
  - Priebežné vzdelávanie v IB (adekvátne prac. zaradeniu)
  - Segregácia povinností
  - Formálny disciplinárny proces pri porušení povinností v IB

Prehľad systému manažmentu IB (5)
Personálna bezpečnosť

- Ukončenie zamestnania alebo zmena pracovného zaradenia
  - Spolupráca personálneho oddelenia a útvaru IT
  - Vrátenie zariadení
  - Odňatie/zmena prístupových práv
- Poznámka. Nespokojný zamestnanec je jedným z najčastejších príčin bezpečnostných incidentov
- Vedenie: schválenie a presadzovanie bezpečnostných opatrení v personálnej bezpečnosti

Prehľad systému manažmentu IB (6)
Fyzická bezpečnosť

- Cieľ: zabrániť neoprávnenému fyzickému prístupu k aktívam organizácie; ochrana aktív pred prírodnými vplyvmi a technickými poruchami
- Bezpečné priestory (perimeter, kontrola prístupu, zabezpečené priestory, iné prístupové možnosti)
- Bezpečnosť vybavenia
  - Umiestnenie a ochrana zariadení
  - Podporná infraštruktúra
  - Ochrana káblov (vnútorných sietí)
  - Údržba zariadení
  - Odnášanie zariadení z priestorov organizácie
  - Používanie zariadení mimo priestorov organizácie
  - Vyraďovanie zariadení

Prehľad systému manažmentu IB (7)

Manažment vzťahov s dodávateľmi a poskytovateľmi služieb

- Cieľ: nastaviť a udržiavať vzťahy s dodávateľmi a poskytovateľmi služieb tak, aby nebola narušená IB organizácie
- Externé subjekty majú prístup k zariadeniam, informáciám organizácie a môžu ovplyvniť jej činnosť
- Bezpečnostná politika upravujúca vzťahy s externými subjektmi
- Bezpečnostné požiadavky v zmluvách
- Kontrola dodržiavania zmlúv
- Vedenie
  - Politika a jej premietnutie do zmlúv

Prehľad systému manažmentu IB (8)
Prevádzka systémov a komunikácie

- Táto (a nasledujúce časti) majú technický charakter, uvedieme len prehľad a upozorníme na vybrané otázky
  - Dokumentácia procedúr a zodpovedností
  - Ochrana proti škodlivému softvéru
  - Zálohovanie
  - Redundancia hardvéru
  - Manažment bezpečnosti sietí
  - Narábanie s pamäťovými médiami
  - Prenos informácie
  - Monitorovanie a logovanie
  - Kryptografické prostriedky
  - Mobilné zariadenia a práca na diaľku

Prehľad systému manažmentu IB (9)
Manažment aplikačných služieb na sieti

- integrita a dostupnosť zverejnenej informácie
- Podstatne komplikovanejšie: Bezpečnosť aplikačných služieb ponúkaných prostredníctvom počítačových sietí
  - Autentifikácia zúčastnených strán
  - Požiadavky na dôvernosť, nepopretie pôvodu, prijatia, záväznosť dohodnutých podmienok
  - Integrita a dôvernosť prenášanej informácie
  - Atď.
- Vedenie:
  - Aké informácie organizácia bude zverejňovať prostredníctvom sietí a akú úroveň ochrany im zaručí
  - Aké služby bude organizácia poskytovať pomocou sietí a bezpečnostné požiadavky na ne kladené

Prehľad systému manažmentu IB (10)
Riadenie prístupu

- **cieľ:** zamedziť /obmedziť neoprávnený prístup k (informačným) zdrojom organizácie
- Riadenie prístupu na základe pracovných potrieb a bezpečnostných požiadaviek (roly, bezpečnostná politika)
- Správa prístupových práv používateľov
- Zodpovednosť používateľov (dodržiavanie politiky riadenia prístupu, ochrana autentizačných prostriedkov)
- Riadenie prístupu do systémov a aplikácií
- Vedenie:
  - Klasifikačná schéma
  - Bezpečnostná politika (zásady politiky riadenia prístupu)

Prehľad systému manažmentu IB (11)

Obstarávanie, vývoj a údržba systémov

- Bezpečnosť počas celého životného cyklu
- Bezpečnostné požiadavky na informačné systémy (súčasť celkových požiadaviek na systémy)
- Bezpečnosť pri vývoji a podporných procesoch (vývoj, zmeny, zmeny platforiem, procedúry vývoja systému, bezpečnostné vývojové prostredie, vývoj tretími stranami), schvaľovanie systému
- Bezpečnosť systémových súborov (pravidlá/procedúry pre inštalovanie sw na bežiace systémy, ochrana testovacích dát, prístup k zdrojovým kódom)
- Manažment technických zraniteľností

Prehľad systému manažmentu IB (12)

Manažment bezpečnostných incidentov

- Cieľ: konzistentné a účinné riešenie bezpečnostných incidentov
- Stanovenie zodpovednosti a vypracovanie/zavednie postupov riešenia incidentov v organizácii
- Oznamovanie bezpečnostných incidentov (rýchle, v súlade s postupmi)
- Oznamovanie odhalených/možných zraniteľností
- Vyhodnotenie a rozhodnutie o nahlásenom bezpečnostnom incidente
- Reakcia na bezpečnostný incident
- Poučenie z bezpečnostných incidentov
- Zber forenzných dôkazov

Prehľad systému manažmentu IB (13)

Manažment kontinuity činnosti

- Organizácia má/mala by riešiť udržanie kontinuity svojej činnosti
- bezpečnostné požiadavky na ochranu informácie zostávajú nemenné za každej situácie
- Plánovanie kontinuity IB
- Implementácia opatrení na zachovanie kontinuity IB
- Vývoj a zavedenie plánov kontinuity činnosti vrátane IB
- Testovanie, údržba a prehodnocovanie plánov kontinuity činnosti

Prehľad systému manažmentu IB (14)
Súlad

- Legislatíva a zmluvné záväzky
  - Identifikácia relevantných zákonov a z nich vyplývajúcich požiadaviek
  - Ochrana duševného vlastníctva
  - Ochrana klasifikovanej informácie
  - Ochrana osobných údajov
  - Kryptografické prostriedky
- Štandardy
  - Bezpečnostná politika a štandardy
- audit

Klasifikácia informácie a systémov

Podstata klasifikácie

- Neriešiť bezpečnosť jednotlivých aktív, ale
- Zoskupiť aktíva s podobnými bezpečnostnými požiadavkami do tried
- Navrhnúť bezpečnostné opatrenia pre triedy
- Zaradiť aktívum do klasifikačnej triedy je jednoduchšie, ako analyzovať jeho bezpečnostné potreby individuálne

Klasifikačné kritériá

- Klasifikačné kritériá (aktuálne používané)
  - Charakter, resp. účel použitia (údajov a systémov)
  - Bezpečnostné požiadavky na ochranu aktív
- Problém: veľa a rôznych
- Riešenie (USA, Nemecko)
  - Klasifikačné kritériá = bezpečnostné požiadavky (neutrálne)
  - Definovať úroveň ochrany pre typy informácie
- Kritériá
  - Dôvernosť
  - Integrita (aj autentickosť a non repudiation of origin)
  - Dostupnosť
- Rozšírenie integrity je umelé, pridáme autentickosť

Klasifikácia informácie (1)

- Tri úrovne významnosti: nízka, stredná, vysoká + n.a.
- nízka: malé finančné straty, lokálny dopad, neohrozuje činnosť organizácie
- stredný: významné ale zvládnuteľné straty, obmedzenie činnosti organizácie, vplyv na iné organizácie, zdravie ľudí, právne dôsledky
- vysoký: straty ohrozujúce existenciu organizácie, neschopnosť plniť základné funkcie, významný vplyv na iné organizácie, život a zdravie ľudí, ohrozenie mena a záujmov SR
- N.a. – kritérium sa v danom prípade nedá použiť

Klasifikácia informácie (2)

- Klasifikujeme typy a nie jednotlivé položky informácie
- Napr. informácie zverejnené na webovej stránke, osobné údaje, utajované skutočnosti, zdravotné záznamy, kryptografické kľúče
- Štvorica:
  - Vážnosť dopadu pri poušení dôvernosti
  - Vážnosť dopadu pri poušení integrity
  - Vážnosť dopadu pri poušení dostupnosti
  - Vážnosť dopadu pri poušení autentickosti
- Napr. verejná informácia (webová stránka)
  - Dôvernosť : n.a.
  - integrita: stredná
  - Dostupnosť : nízka
  - Autentickosť : stredná

Klasifikácia systémov

- Na základe klasifikácie všetkých typov informácie, ktoré sa v systéme vyskytujú
- Najprv maximá z úrovne jednotlivých požiadaviek (výnimka n.a.) = úrovne ochrany info v systéme vzhľadom na dôvernosť, integritu, dostupnosť a autentickosť (stĺpce tabuľky)
- Klasifikácia systému = maximum z úrovní jednotlivých požiadaviek na ochranu info v systéme (posledný riadok tabuľky)

info	dôvernosť	integrita	dostup.	autentic.
Typ1	n.a.	nízka	vysoká	nízka
Typ2	n.a.	stredná	nízka	n.a.
Typ3	n.a.	nízka	n.a.	nízka
systém	nízka	stredná	vysoká	nízka

Bezpečnostné požiadavky na ochranu systému

- Tri úrovne (USA) nízka, stredná, vysoká
- Pre každú úroveň minimálny súbor opatrení
- Úprava súboru opatrení (znižovanie podľa úrovne jednotlivých požiadaviek platnej pre systém) systém: vysoká, ale dôvernosť stredná
- Potom implementácia opatrení a štandardná správa rizík
- Nemecko: zdola nahor, základný súbor opatrení, analýza rizík pre informácie a systémy, kde základná úroveň nestačí

* * *

Prehľad štandardov informačnej bezpečnosti

Štandardizácia v informačnej bezpečnosti

- Význam
  - Nemusíme objavovať to, čo je známe a overené
  - Kompatibilita metód a úrovne ochrany systémov
- Zdroje použiteľných noriem
  - Medzinárodné štandardizačné organizácie ISO, IEC, CEN, ETSI,...
  - Národné štandardizačné orgány
    - NIST (USA)
    - BSI (Nemecko)
  - Príležitostne medzinárodné organizácie (OECD)
  - Aktivizuje sa ENISA
  - Národné a medzinárodné organizácie (IETF, SANS Institute, ISACA, RSA laboratories a i.)
  - STN – preberáme medzinárodné normy (ISO)

Ako funguje ISO?

- Pomaly a dôkladne
- Zložitá organizačná štruktúra, pre jednotlivé oblasti technické výbory
- Informatika JTC 1 (spolu s IEC)
- Bezpečnosť – podvýbor, pracovné skupiny, v nich najmä zástupcovia národných štandardizačných organizácií, odborných organizácií podobného zamerania
- Príprava novej normy 3-5 rokov (WD,CD,DIS,FDIS IS)
- Typy noriem
  - Slovníková norma (Vocabulary standard)
  - Certifikačná norma (Requirement standard)
  - Návodová norma (Guidence standard)
  - Technická správa (Technical report)
  - Technická špecifikácia (Technical specification)

ISO normy pre informačnú bezpečnosť

- Sústredíme sa na najdôležitejšie ISO normy, potom spomenieme užitočné normy NIST a BSI
- ISO normy pre oblasť IB cca 80, z nich niektoré vo vývoji
- Stručné delenie:
  1. Manažment IB
  2. Kryptológia
  3. Evaluácia a certifikácia systémov
  4. Bezpečnostné riešenia (Security controls)
  5. Identifikácia a autentizácia
- Z praktického hľadiska najzaujímavejšia je prvá skupina
- Prebieha systematizácia noriem, zosúlaďovanie IB s manažmentom, a manažmentom kvality
- Prečíslovanie noriem, rad 27000 vyhradený pre manažment IB

ISO/IEC normy radu 27000 (1)
základné

- 4 základné:
- **ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary**
  - Úvod do ISMS (information security management systems, systémov manažmentu informačnej bezpečnosti)
  - Základné pojmy a definície pre oblasť ISMS
  - Prehľad rodiny noriem 27000
- **ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements**
  - Relatívne stručný štandard
  - Definuje požiadavky na zriadenie, implementáciu, prevádzku, monitorovanie, revíziu, údržbu a zlepšovanie systému riadenia informačnej bezpečnosti
  - Zohľadňuje činnosť, ktorú organizácia vykonáva a hrozby, ktorým čelí
  - Požiadavky sú definované všeobecne a preto je štandard všeobecne použiteľný
  - Väčšina požiadaviek je povinných, ak chce organizácia certifikovať ISMS podľa ISO 27001

ISO/IEC normy radu 27000 (2)
základné

- ISO/IEC 27002 **Information technology — Security techniques — Code of practice for information security management**
- Definuje ciele pre jednotlivé oblasti IB a uvádza zoznam bezpečnostných funkcií/opatrení na dosiahnutie stanovených cieľov
- Pokrýva nasledujúce oblasti IB:
  - Bezpečnostná politika
  - Organizácia IB
  - Správa aktív
  - Personálna bezpečnosť
  - Fyzická bezpečnosť
  - Manažment vzťahov s dodávateľmi/poskytovateľmi služieb
  - Prevádzka systémov a komunikácie
  - Manažment aplikačných sieťových služieb
  - Riadenie prístupu
  - Obstarávanie, vývoj a údržba systémov
  - Riešenie bezpečnostných incidentov
  - Manažment kontinuity činnosti
  - Súlad s legislatívou

ISO/IEC normy radu 27000 (3)
základné

- ISO/IEC 27005 **Information technology — Security techniques — Information security risk management**
- Užitočný štandard, kompletná správa rizík
- Praktické návody
  - identifikácia aktív
  - Identifikácia hrozieb
  - Identifikácia a ohodnotenie zraniteľností
  - Ohodnotenie rizík

ISO/IEC normy radu 27000 (4)
implementácia ISMS

- Normy zamerané na zavedenie a posudzovanie účinnosti ISMS:
- **ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance**
- Rozsiahly štandard
- Návod na praktickú implementáciu ISMS podľa ISO 27001
  - Iniciovanie projektu ISMS
  - Definovanie pôsobnosti ISMS
  - Analýza bezpečnostných požiadaviek
  - Odhad rizík a plánovanie ošetrenia rizík
  - Návrh ISMS
- Podrobne sa rozpisujú aj samozrejmé veci

ISO/IEC normy radu 27000 (5)
meranie účinnosti a audit

- **ISO/IEC 27004 Information technology — Security techniques — Information security management — Measurement**
  - Vychádza z požiadavky ISO/IEC 27001 na pravidelné revízie účinnosti ISMS
  - Obsahuje návod na vývoj a používanie mier, ktoré umožňujú posúdiť účinnosť ISMS a bezpečnostných opatrení
  - Zavedenie Programu/programov merania bezpečnosti
- **ISO/IEC 27007 Information technology — Security techniques — Guidelines for information security management systems auditing**
- Stručná norma poskytujúca návody na
  - na manažment programov auditu a
  - Vykonanie interných a externých auditov ISMS podľa normy ISO 27001
  - Posúdenie kompetentnosti a ohodnotenie audítorov
- Vychádza zo všeobecnejšej normy ISO 19011 Guidelines for auditing management systems, ktorú upravuje na potreby auditu ISMS

ISO/IEC normy radu 27000 (6)
audit

- **ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems**
  - štandard by bol zaujímavý v prípade, keby MF SR, alebo iný štátny orgán požadoval audit a certifikáciu ISMS podľa ISO 27001
  - Základné požiadavky na organizácie vykonávajúce audit a certifikáciu sú v norme ISO/IEC 17021, táto norma stanovuje dodatočné požiadavky (kompetentnosť a spoľahlivosť) a návod pre takéto organizácie ako splniť požiadavky
  - Pre organizáciu prevádzkujúcu prvok CRITIS je zaujímavá keď dostane ponuku na certifikáciu svojho ISMS

ISO/IEC normy radu 27000 (7)
audit

- **ISO/IEC TR 27008 Information technology — Security techniques — Guidelines for information security management systems auditing**
  - TR poskytuje návod na audit vhodnosti a účinnosti bezpečnostných funkcií ISMS

ISO/IEC normy radu 27000 (8)
ISMS pre špecifické oblasti

- ISO/IEC 27010 – Information technology – Security techniques -- Information security management for inter-sector communications
- ISO/IEC 27011 -- Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations
- ISO/IEC 27015 Information technology — Security techniques – Information security management guidelines for financial services
- ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002

ISO/IEC normy radu 27000 (9)
rôzne

- ISO/IEC 27013 Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC TR 27016 Information technology — Security techniques — Information security management – Organizational economics
- ISO/IEC 27014 Information technology — Security techniques — Governance of information security

Ďalšie ISO normy

ISO/IEC 13335 Management of Information and Communications Technology Security

- Všeobecný návod na inicializáciu a implementovanie procesu riadenia IB
- Inštrukcie, ale nie riešenia ako riadiť IB
- Klasika – základ riadenia IB
- V súčasnosti už len 3 časti
  - 1. Koncepty a modely pre riadenie bezpečnosti IKT
  - 2. techniky pre manažment IB rizík
  - 5. Manažérsky návod na sieťovú bezpečnosť
- **ISO/IEC 15408 Common Criteria**
  - Rozsiahly, voľne dostupný štandard pre certifikáciu systémov
  - Bezpečnostné požiadavky na systémy sa formulujú v podobe ST a PP podľa Common Criteria

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Vydáva dobre spracované, zrozumiteľné, voľne dostupné a použiteľné materiály
- Prepracovaný systém základných požiadaviek na IB : IT Grundschutz, podporený rozsiahlym manuálom a štandardami
- Momentálne 4 BSI štandardy, obsahujúce odporúčania BSI týkajúce sa metód, procesov, procedúr, prístupov a opatrení týkajúcich sa informačnej bezpečnosti
- Sú určené štátnym inštitúciám aj súkromným spoločnostiam
- Zohľadňujú medzinárodné normy
- Okrem štandardov – viacero špecializovaných publikácií, analýz, správ
- https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html

Štandardy BSI (1)

- **BSI Standard 100-1 Information Security Management Systems (ISMS)**
  - definuje všeobecné požiadavky na ISMS
  - Kompatibilný s ISO/IEC 27001
  - Zohľadňuje aj odporúčania ostatných noriem radu 27000
  - Detailnejšie a metodicky lepšie spracovaný dokument ako ISO normy
  - Kompatibilný s IT-Grundschutz prístupom
- **BSI-Standard 100-2: IT-Grundschutz Methodology**
  - Popisuje, ako zaviesť a prevádzkovať ISMS v praxi
  - Ako vytvoriť bezpečnostnú koncepciu, vybrať vhodné bezpečnostné opatrenia a realizovať bezpečnostnú koncepciu v praxi
  - Kompatibilný s ISO normami radu 27000

Štandardy BSI (2)

- **BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz**
  - Používajú sa štandardné („konfekčné“) bezpečnostné riešenia pre typické systémy so štandardnými nárokmi na IB (založené na katalógu IT-Grundschutz opatrení BSI)
  - Zvýšené/špecifické požiadavky – individuálny prístup
  - Analýza rizík (a návrh opatrení)
  - Štandard obsahuje metodiku pre analýzu rizík
  - Príloha: Katalóg elementárnych hrozieb
- **BSI-Standard 100-4: Business Continuity Management**
  - Systematicky popisuje, ako vyvinúť, zaviesť a udržiavať v organizácii systém na riadenie kontinuity činnosti

National Institute of Standards and Technology, NIST

- Americký štandardizačný inštitút
- V rezorte Ministerstva obchodu
- o.i. zodpovedný za štandardizáciu IB pre oblasť neklasifikovanej informácie
- Od konca 80-tych rokov
- Vydáva štandardy a metodické materiály
- Primárne určené pre americké štátne organizácie a americké firmy, môžu byť užitočné aj v našich podmienkach
- Do pozornosti
  - NIST Special Publications 800
  - FIPS (Federal Information Processing Standard)
- Menovite SP 800-100 Information Security Handbook: A Guide for Managers

Medzinárodné inštitúcie

- OECD:
  - **The promotion of a culture of security for information systems and Networks in OECD countries**
  - **OECD Recommendation of the Council on the Protection of Critical Information Infrastructures**
- ENISA
  - Zatiaľ skôr prehľady a štúdie
  - http://www.enisa.europa.eu/publications#c2=publicationDate&reversed=on&c5=all&c0=10&b_start=0
- IETF: Vydávajú de facto štandardy pre Internet (RFC)
- ISACA, SANS Institute – de facto štandardy pre vzdelávanie odborníkov v IB
- Iné – napr. RSA laboratories: spravuje štandardy pre PKI (PKCS)

Slovensko

- SÚTN, technická komisia pre IB
- Na dobrovoľnej báze
- Preberáme štandardy do STN
- problémy:
  - Terminologické
  - Kapacitné
  - Ekonomické
- Rozumnejšie je používať medzinárodné štandardy, resp. preberať ich do STN v origináli
- Využitie v štandardoch vydávaných št. orgánmi (Výnos o štandardoch ISVS)

* * *

Právne požiadavky na ochranu informácie a systémov

Ochrana prvku kritickej (informačnej) infraštruktúry (CRITIS)

- Zákon č. 45/2011 o kritickej infraštruktúre
- Všeobecný a veľmi stručný zákon
- Prvky kritickej infraštruktúry sú systémy rôzneho charakteru a určenia
- Je ťažké stanoviť spoločné požiadavky a pritom vyhovieť špecifikám rôznych systémov
- V zákone – dôraz na fyzickú a organizačnú bezpečnosť, špecifiká informačnej bezpečnosti sa uvádzajú minimálne
- Cieľ: nie je kritika zákona, ale analýza ako sa rozumne dajú interpretovať jeho požiadavky a zabezpečiť primeraná úroveň informačnej bezpečnosti prvku CRITIS
- Využijeme poznatky, ktoré sme prezentovali v predchádzajúcich prednáškach
- Najprv uvedieme požiadavky zákona, potom ich vyjadríme vo forme štandardnej pre IB a popíšeme postup na ich naplnenie a nakoniec sa pozrieme na požiadavky ďalších zákonov relevantné pre prvok CRITIS

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (1)

- Zákon č. 45/2011 o kritickej infraštruktúre, §9 Povinnosti prevádzkovateľa

(1) Prevádzkovateľ je povinný ochraňovať prvok pred narušením alebo zničením. Na ten účel prevádzkovateľ je povinný

a) uplatniť pri modernizácii prvku technológiu, ktorá zabezpečuje jeho ochranu,

- Všeobecná požiadavka, ktorá sa bez bližšej špecifikácie nedá naplniť
- Požiadavka
  - sa uplatňuje pri zmenách prvku, ktoré znamenajú jeho technologický upgrade (čo dovtedy?)
  - Predpokladá, že na zabezpečenie ochrany prvku budú stačiť samotné technológie (nestačia)
- V záujme adekvátneho zaistenia bezpečnosti prvku budeme hľadať iné riešenia

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (2)

§9 ods 1) písm b) zaviesť bezpečnostný plán po predchádzajúcom vyjadrení príslušného ústredného orgánu do šiestich mesiacov od doručenia oznámenia o určení prvku a o jeho zaradení do sektora, ak sa vo výnimočnom odôvodnenom prípade nedohodne s príslušným ústredným orgánom na predĺžení tejto lehoty; lehotu je možné predĺžiť iba jedenkrát, maximálne o tri mesiace,

- Zákon podrobnejšie špecifikuje požiadavky na bezpečnostný plán a spôsob jeho vytvárania v § 10 a prílohe 2:

Bezpečnostný plán (§ 10)

(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.

(3) Rozsah bezpečnostných opatrení na ochranu prvku sa určuje na základe posúdenia hrozby narušenia alebo zničenia prvku.

(4) Minimálny postup pri vypracúvaní bezpečnostného plánu je uvedený v prílohe č. 2.

Príloha č. 2 k zákonu č. 45/2011 Z. z. (1)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

Pri vypracúvaní bezpečnostného plánu sa postupuje takto:

A. Určujú sa dôležité zariadenia prvku.

B. Vyhodnocuje sa riziko hrozby narušenia alebo zničenia jednotlivých zariadení prvku, ich zraniteľné miesta, predpokladané dôsledky ich narušenia alebo zničenia na funkčnosť, integritu a kontinuitu činnosti prvku.

Príloha č. 2 k zákonu č. 45/2011 Z. z. (2)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

C. Uskutočňuje sa výber hlavných bezpečnostných opatrení na ochranu prvku, ktoré sa členia na

a) trvalé bezpečnostné opatrenia, ktorými sú investície a postupy na zabezpečenie ochrany prvku, a to

1. mechanické zábranné prostriedky,
2. technické zabezpečovacie prostriedky,
3. bezpečnostné prvky informačných systémov,
4. organizačné opatrenia s dôrazom na postup pri vyrozumení a varovaní, ako aj na krízové riadenie,
5. odborná príprava osôb, ktoré zabezpečujú ochranu prvku,
6. kontrolné opatrenia na dodržiavanie trvalých bezpečnostných opatrení,

b) mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.

Príloha č. 2 k zákonu č. 45/2011 Z. z. (3)

MINIMÁLNY POSTUP PRI VYPRACÚVANÍ BEZPEČNOSTNÉHO PLÁNU

D. Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku.

E. Bezpečnostný plán sa počas jeho tvorby konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.

Bezpečnostný plán/projekt prvku CRITIS

Zákon o kritickej infraštruktúre	Štrandardné postupy IB
Určujú sa dôležité zariadenia prvku	Inventarizácia aktív systému
Vyhodnocuje sa riziko hrozby	Inventarizácia hrozieb
zraniteľné miesta	Zoznam zraniteľností
	Zoznam bezpečnostných požiadaviek
predpokladané dôsledky ich narušenia alebo zničenia	Dopady hrozieb na aktíva
	Analýza rizík (chýba)
výber hlavných bezpečnostných opatrení	Návrh opatrení
mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v závislosti od intenzity hrozby narušenia alebo zničenia prvku.	Správa rizík
D. Určujú sa hlavné bezpečnostné opatrenia na ochranu prvku	Implementácia opatrení
BP ... konzultuje s orgánmi, ktorých súčinnosť sa predpokladá pri ochrane prvku.	ISMS

Kritériá informačnej bezpečnosti zákona o kritickej infraštruktúre

- V prílohe 2: predpokladané dôsledky ich narušenia alebo zničenia (*aktív*) na funkčnosť, integritu a kontinuitu činnosti prvku.
- Postačuje nám požiadavka na funkčnosť, ak ju budeme chápať v širšom zmysle, t.j. tak, že požadujeme, aby systém fungoval v súlade s bezpečnostnou politikou.
- *Funkčnosť* v chápaní Zákona je ekvivalentná spoľahlivosti a čiastočne dostupnosti, *integrita* zariadenia znamená jeho neporušenosť a v podstate je už obsiahnutá v požiadavke na funkčnosť, *kontinuita činnosti* znamená dostupnosť služieb a zdrojov systému; t.j. jednu zo základných bezpečnostných požiadaviek na ochranu informácie
- **Záver:** štandardné bezpečnostné požiadavky na dôvernosť, integritu a dostupnosť informácie postačujú na pokrytie požiadaviek Zákona

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (3)

c) prehodnocovať priebežne bezpečnostný plán, a ak je to potrebné, zaviesť po predchádzajúcom vyjadrení príslušného ústredného orgánu aktualizovaný bezpečnostný plán,

d) oboznámiť svojich zamestnancov v nevyhnutnom rozsahu s bezpečnostným plánom,

e) precvičiť podľa bezpečnostného plánu aspoň raz za tri roky modelovú situáciu hrozby narušenia alebo zničenia prvku,

f) určiť oprávnenú osobu, ktorá je zároveň kontaktná osoba, ak ide o prvok európskej kritickej infraštruktúry,

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (4)

g) poskytnúť príslušnému ústrednému orgánu súčinnosť ,najmä údaje, doklady a vysvetlenia potrebné na

1. určenie prvku a jeho zaradenie do sektora, ako aj vyradenie prvku zo sektora,
2. posúdenie ochrany prvku vrátane zabezpečenia ochrany prvku prevádzkovate-

ľom strážnej služby alebo ozbrojeným bezpečnostným zborom,

3. vypracovanie analýzy rizík sektora,
4. správu registra prvkov,

h) postupovať podľa bezpečnostného plánu v prípade hrozby narušenia alebo zničenia prvku.

Výnimky

(3) Na prevádzkovateľa, ktorý vypracúva havarijný plán alebo obdobný bezpečnostný dokument podľa osobitného predpisu,4) sa nevzťahuje odsek 1 písm. b), c), d) e) a h).

- Napríklad zákon č. 261/2002 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Z logického hľadiska by mohlo ísť o akýkoľvek zákon, ktorý na ochranu prvku CRITIS kladie rovnaké alebo vyššie požiadavky ako zákon o kritickej infraštruktúre
  - Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
  - Zákon č. 215/2004 Z.Z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
  - Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení zákona č. 602/2003 Z. z., zákona č. 576/2004 Z. z. a zákona č. 90/2005 Z. z.
- Kto rozhoduje o výnimke – implicitne pravdepodobne MF SR
- MF SR pripravuje zákon o IB

Povinnosti prevádzkovateľa prvku kritickej infraštruktúry (4)

§2, písm k) citlivou informáciou o kritickej infraštruktúre (ďalej len „citlivá informácia“) neverejná informácia, ktorej zverejnenie by sa mohlo zneužiť na činnosť smerujúcu k narušeniu alebo zničeniu prvku,

§ 12 Citlivá informácia

(1) Písomnosť alebo iný hmotný nosič, ktorý obsahuje citlivú informáciu, sa označuje slovami „Kritická infraštruktúra – nezverejňovať“.

(2) Oprávnená osoba je povinná zachovávať mlčanlivosť o citlivej informácii, a to aj po zániku jej oprávnenia oboznamovať sa s citlivou informáciou.

(3) Citlivá informácia sa nesprístupňuje podľa osobitného predpisu. (Infozákon)

Sankcie

- Fyzická osoba za prezradenie citlivých informácií (§ 14)
- prevádzkovateľ za nesplnenie povinností pri ochrane prvku CRITIS (správny delikt, § 15)

Ochrana prvku CRITIS

- Ako zosúladiť požiadavky Zákona o kritickej infraštruktúre s potrebami ochrany prvku CRITIS?
- Požiadavky Zákona
  - Sú neúplné
  - Používajú neštandardný jazyk
  - Ale nekladú prekážky adekvátnej ochrane prvkov CRITIS
- Ideálne riešenie: výnimka podľa § 9, ods. 3) a Zákon 275/2006 o ISVS, ak má organizácia zavedený Systém riadenia informačnej bezpečnosti podľa Výnosu č. 312/2010 Z.z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
- Ak by aj prvok nebol ISVS, ale má zavedený ISMS podľa Výnosu č. 312/2010 Z.z., spĺňa všetky požiadavky Zakona č. 45/2011

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (1)

Súlad bezpečnostných štandardov ISVS so Zákonom o kritickej infraštruktúre:

(§ 28 Výnosu) Štandardom pre riadenie informačnej bezpečnosti je

a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby, ktorej obsahom je (o.i.)

   6. zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi,

   7. určenie požiadaviek na informačné systémy verejnej správy, vyplývajúcich zo všeobecne záväzných právnych predpisov,

b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby,

Porovnanie bezpečnostných funkcií ISMS a požiadaviek na ochranu prvku CRITIS (2)

Z 45/2011	požiadavka	Výnos
§9 ods. 1	Ochrana prvku pred narušením alebo zničením	§28-42
Písm. a)	Modernizácia prvku	§ 41
Písm. b)	Zavedenie bezpečnostného plánu	Najmä § 28, § 30
Písm. c)	Aktualizácia bezpečnostného plánu	Najmä §28, §31
Písm. d)	Oboznamovanie zamestnancov s BP	§ 29
Písm. e)	Cvičenia	§ 30, f) § 36
Písm. f)	Stanovenie oprávnenej osoby	§ 28 písm. c), d)
Písm. h)	Dodržiavanie BP	§28 písm. b)
§ 10	Bezpečnostný plán	
§ 12	Citlivá informácia	§ 28 a) body 7,8,13

Čo treba dopracovať?

- Všeobecnými ustanoveniami bezpečnostných štandardov sú pokryté všetky požiadavky Zákona o kritickej infraštruktúre
- Najmä ustanovenia § 28, písm. a) body 6,7,8 (požiadavky vyplývajúce zo zákonov, súlad s legislatívou, stanovenie rozsahu a úrovne ochrany) a 13 – rozpracovanie bezpečnostnej dokumentácie
- Bude potrebné konkretizovať
  - Opatrenia na zachovanie/obnovenie Kontinuity činnosti (explicitne uviesť cvičenia v havarijných plánoch)
  - Klasifikácia informácie (doplniť citlivú informáciu a požiadavky na jej ochranu), do bezpečnostných štandardov doplniť klasifikačnú schému (pripravuje sa v zákone o IB)

Iné zákony

428/2002 Z. z. o ochrane osobných údajov

- Len informatívne, pretože existuje novela vrátená prezidentom
- Ochrane osobných údajov je venovaná Hlava II
- Trocha nekonzistentný:
  - Chápanie bezpečnosti
  - Rozsah pôsobnosti
  - Veľa odkazov na iné zákony
- Požiadavky na ochranu údajov sa však dajú splniť bez väčšieho dodatočného úsilia
- Bezpečnosť sa chápe ako zachovanie dôvernosti, integrity, dostupnosti a zamedzenie neprípustného spracovávania (osobných údajov)
- Pod posledný pojem sa zmestí všetko

Iné zákony

428/2002 Z. z. o ochrane osobných údajov (2)

- Osobné údaje je prevádzkovateľ/spracovateľ povinný chrániť v každom prípade (§ 15, ods. (1)), navyše
- Ak sa v systéme spracovávajú osobitné kategórie osobných údajov
  - pripojený na verejnú sieť – bezpečnostný projekt
  - Nepripojený – len zdokumentovanie bezpečnostných opatrení
- Výnimka – bezpečnostný projekt podľa Zákona o ochrane utajovaných skutočností
- Kľúčová otázka: čo všetko spadá do osobitnej kategórie osobných údajov (rodné číslo? rodinné pomery, obmedzená pracovná schopnosť,...)
- Technické a organizačné požiadavky na ochranu prvkov CRITIS, v ktorých sa spracovávajú (aj) osobné údaje sa dajú riešiť v rámci ISMS podľa Výnosu MF SR č. 312/2010 z.z.

Iné zákony

428/2002 Z. z. o ochrane osobných údajov (3)

- Nekonzistentnosti (hrozby-riziká, bezpečnostné ciele, bezpečnostný zámer-bezpečnostná politika)
- Zaradenie osobných údajov do klasifikačnej schémy
- Splnenie administratívnych povinností (zodpovedná osoba, školenia, nahlasovanie na ÚOOÚ)
- Odporúčanie: ak sa dá, redukovať počet systémov, v ktorých sa spracovávajú osobné údaje (teoreticky – práca off-line, prakticky ???)

Iné zákony

Zákon č. 215/2004 Z. z.

- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Najvyššia priorita, ale vzťahuje sa len na vymedzený okruh systémov
- Ak sa na prvok, alebo jeho subsystém vzťahuje Zákon č. 215/2004 Z. z. treba pri ochrane prvku postupovať podľa neho (predpoklad: uplatní sa výnimka podľa § 9, ods. 3 Zákona 45/2011)
- Minimalizovať rozsah systému, kde sa spracovávajú utajované skutočnosti (kvôli zjednodušeniu prevádzky a optimalizácii nákladov na ochranu)
- Prípadné nejasnosti MF-MV-NBÚ

Záver

- Informačná bezpečnosť – nutná podmienka fungovania (kritickej) informačnej infraštruktúry spoločnosti
- Súčasný stav (kompetencie, legislatíva, štandardy, prax) je neuspokojivý; dôsledok historického vývoja
- Živelný vývoj nebude konvergovať dostatočne rýchlo do požadovaného stavu
- O IB sme sa za vyše 40 rokov niečo naučili, vieme ochraňovať jednotlivé IKS, potrebujeme však chrániť globálny digitálny priestor
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union
- V SR pripravovaný Zákon o IB, potrebné by bolo zosúladenie legislatívy a koordinovaný systematický prístup k IB na lokálnej aj globálnej úrovni

* * *