Kybernetická a informačná bezpečnosť v organizácii

UIB-3

Daniel Olejár

Univerzita Komenského

Február 2022

Agenda- rýchlokurz pre manažéra KIB

- prečo potrebujeme riešiť kybernetickú a informačnú bezpečnosť v organizácii
- eu a slovenská legislatíva
- systematický prístup ku KIB - ISMS
- zavádzanie ISMS
- správa rizík
- dokumentácia - špeciálne politiky
- ďalší postup pri udržiavaní a rozvoji KIB v organizácii

Úvod

- v tejto prednáške sa budeme zaoberať systematickým riešením kybernetickej a informačnej bezpečnosti (KIB) v organizácii
- na úlohu - riešiť KIB - sa dívame z pozície človeka, ktorý túto úlohu dostal a perspektívne má vykonávať funkciu manažéra KIB
- predpokladáme, že ide o nevýrobnú organizáciu stredného až väčšieho rozsahu, ktorá využíva rôznorodé IKT na činnosti priamo alebo nepriamo spojené s výkonom činností potrebných na plnenie poslania organizácie
- vo výrobnej organizácii by sme sa museli zaoberať aj bezpečnosťou systémov, ktoré riadia výrobné procesy (napr. SCADA), čo si vyžiada špecifické znalosti a možno aj oprávnenia
- predpokladáme, že v organizácii sa zatiaľ KIB nikto systematicky nezaoberal

Podnet pre riešenie KIB

- najčastejšie dôvody, prečo organizácia doteraz neriešila KIB
  - vedenie KIB nerozumie
  - KIB je technická záležitosť, nech to riešia informatici
  - kto by sa už zaujímal o naše údaje a systémy a chcel na nás zaútočiť
  - KIB je drahá, ak sa podarí udržiavať dostatočnú úroveň KIB a nič zlého sa nestane, vedenie organizácie má dojem, že peniaze na KIB boli vynaložené zbytočne
- dva najčastejšie dôvody, prečo sa organizácia začne zaujímať o KIB sú
  - závažný bezpečnostný incident, ktorý organizáciu (alebo podobnú organizáciu) postihol
  - prijatie zákona, ktorý organizácii ukladá povinnosť riešiť KIB a hrozí kontrolou a sankciami

Európska a slovenská legislatíva

- EÚ si je vedomá strategického významu digitálnych IKT (4. a 5. generácia počítačov, Lisabonská stratégia, informatizácia spoločnosti a postindustriálna informačná spoločnosť, znalostná ekonomika, AI, jednotný digitálny trh,...)
- prebieha informatizácia spoločnosti = prispôsobenie tradičných procesov digitálnym IKT
- potrebný je právny rámec aj dôvera ľudí (príklad elektronický podpis)
- veľa právnych aktov (nariadenia, smernice,odporúčania)
- projekty a iniciatívy (napr. FIDIS, Stork, epSOS, sieť superpočítačových centier, centrá excelencie v krypto, AI...)
- u6 teraz digitálne IKT = kritická informačná infraštruktúra
- ENISA

Slovensko

- nariadenia sú priame zákony EÚ a platia aj na Slovensku a majú prednosť pred národnými zákonmi - ak majú veci fungovať na celoeurópskej úrovni, musia existovať všeobecne záväzné pravidlá
- GDPR - ochrana osobných údajov, ochrana kritickej infraštruktúry, e-Government (eIDAS)
- smernice - členské krajiny prijímajú zákony, prostredníctvom ktorých ich implenetujú do národnej legislatívy (ochrana osobných údajov a elektronický podpis boli pôvodne upravené smernicami)
- Smernica NIS (dopĺňajúca prvky kritickej informačnej infraštruktúry, ktoré dostatočne nepokrývalo nariadenie o ochrane kritickej infraštruktúry)
- aj tu - sledovanie účinnosti a revízia smernice (NIS II)

už spomínané zákony a vyhlášky

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (v znení neskorších predpisov).
- Vyhláška Národného bezpečnostného úradu, č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

- hrozba útoku ale skôr obava z kontrol plnenia povinností stanovených zákonmi a sankcií za ich nesplnenie + termíny plnenia úloh = narastajúci záujem o KIB
- typický prístup: vedenie niekoho poverí, aby navrhol riešenie najlepšie také, aby sa splnili minimálne povinnosti vyplývajúce zo zákonov (hrozba sankcií je reálnejšia ako potreba riešiť KIB)
- keďže odborníkov na KIB je málo, môže sa stať, že touto úlohou v organizácii poveria vás
- čo spravíte?

Začíname s KIB

- musíte sa zorientovať a rozhodnúť sa: buď si na to niekoho nájdete (poradcu alebo firmu, ktorá za vás spraví úvodné kroky) alebo sa do toho pustíte sami (aj tak organizácia nebude mať prostriedky na dlhodobé outsourcovanie KIB)
- pozrite sa na zákony a vyhlášky a skúste niečo podľa nich spraviť - pochybujem, že sa vám to podarí;
- ale zákony a vyhlášky vychádzajú z ISO noriem (pozri nasledujúcu tabuľku)
- v KIB sú na rozdiel od zákonov kvalitné medzinárodné normy, ktoré písali odborníci a overovali sa dlhodobo v medzinárodnej praxi
- pozrieme sa na riešenie postavené na medzinárodných normách a na zákony a vyhlášky sa pozrieme na ďalšej prednáške, keď už budeme vedieť, čo a prečo treba spraviť

Oblasti KIB

V nasledujúcej tabuľke porovnávame delenie KIB na oblasti podľa Zákona o KB, Vyhlášky 179/2020 a normy ISO/IEC 27002

ZoKB	vyhláška 179/2020	ISO/IEC 27002
a) organizácia informačnej bezpečnosti,	A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	5 Information security policies 6 Organization of information security
b) riadenia aktív, hrozieb a rizík,	B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	8 Asset management

Oblasti KIB

ZoKB	vyhláška 179/2020	ISO/IEC 27002
c) personálna bezpečnosť,	C. Personálna bezpečnosť	7 Human resource security
d) riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,		14 System acquisition, development, and maintenance 15 Supplier relationships
e) technické zraniteľnosti systémov a zariadení	G. Hodnotenie zraniteľností a bezpečnostné aktualizácie	12.6 Technical vulnerability management

Oblasti KIB

ZoKB	vyhláška 179/2020	ISO/IEC 27002
f) riadenia bezpečnosti sietí a informačných systémov,		13 Communications security 13.1 Network security management
g) riadenia prevádzky,	F. Bezpečnosť pri prevádzke informačných systémov a sietí	12 Operations security
h) riadenia prístupov,	D. Riadenie prístupov	9 Access control

Oblasti KIB

ZoKB	vyhláška 179/2020	ISO/IEC 27002
i) kryptografických opatrení,	N. Kryptografické opatrenia	10 Cryptography
j) riešenia kybernetických bezpečnostných incidentov,	M. Riešenie kybernetických bezpečnostných incidentov	16 Information security incident management
k) monitorovania, testovania bezpečnosti a bezpečnostných auditov,	K. Zaznamenávanie udalostí a monitorovanie P. Audit a kontrolné činnosti	12.4 Logging and monitoring 12.7 Information systems audit considerations

Oblasti KIB

ZoKB	vyhláška 179/2020	ISO/IEC 27002
l) fyzickej bezpečnosti a bezpečnosti prostredia,	L. Fyzická bezpečnosť a bezpečnosť prostredia	11 Physical and environmental security
m) riadenia kontinuity procesov.	O. Kontinuita prevádzky informačných technológií verejnej správy	17 Information security aspects of business continuity management 12.3 Backup

Oblasti KIB

ZoKB	vyhláška 179/2020	ISO/IEC 27002
	E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	15 Supplier relationships
	H. Ochrana proti škodlivému kódu	12.2 Protection from malware
		18 Compliance

Predpoklady a východiská

- KIB v organizácii je potrebné riešiť komplexne (to nutne neznamená, že zložito a draho) a systematicky (nie jednorazovo)
- KIB závisí od všetkých ľudí, ktorí majú prístup k IKT organizácie
- aby sme zaistili potrebnú úroveň KIB v organizácii, každý sa musí zapojiť, ale v miere primeranej jeho úlohe vo vzťahu k IKT a KIB organizácie (podrobnejšie za chvíľu)
- systematické riešenie má podobu ISMS (Information Security Management System), ktorý v nejakej podobe organizácia potrebuje zaviesť (reálne a ukladajú jej to aj zákon o ITVS explicitne a zákon o KB nepriamo)
- ale zavedenie ISMS nedokážeme presadiť z pozície manažéra KIB, potrebujeme explicitnú a jednoznačnú podporu vedenia organizácie

ISMS je virtuálny systém, ktorý pozostáva zo štyroch podstatných zložiek:

- princípov riadenia (informačnej (a kybernetickej) bezpečnosti),
- zdrojov, ktoré sú na zaistenie a udržiavanie informačnej (a kybernetickej) bezpečnosti potrebné,
- ľudí, ktorí pracujú s informáciami, systémami a sieťami a plnia buď špeciálne úlohy v informačnej (a kybernetickej) bezpečnosti, alebo zohľadňujú informačnú (a kybernetickú) bezpečnosť pri plnení svojich pracovných úloh,
- bezpečnostného procesu = aktivity zamerané na dosiahnutie a udržanie potrebnej úrovne KIB v organizácii

Ako zaviesť ISMS v organizácii?

- ISMS je popísaný detailne v medzinárodných normách ISO/IEC [5] [6], z ktorých do značnej miery vychádzali aj oba zákony [1][3] a vyhlášky [2][4].
- ISO normy síce popisujú požiadavky na výsledný ISMS, opatrenia, ktoré je potrebné prijať, ale neuvádzajú postup, ako požadovaný ISMS vytvoriť
- Podrobný návod na vytvorenie ISMS v plnom rozsahu spĺňajúceho požiadavky „certifikačnej“ ISO normy [5] je uvedený v nemeckom štandarde [8] a IT kompendiu Grundschutz [11], z ktorých budeme vychádzať.

Prvá iterácia

- máte poverenie vedenia (úloha, zodpovednosť, termín, právomoci, možno financie)
- vypracujete (sami, alebo so spolupracovníkmi) návrh postupu riešenia KIB (zavedenia ISMS) a predložíte ho vedeniu organizácie (vo forme case study)
  - čo je KIB a prečo by sa organizácia ňou mala zaoberať
  - stav KIB v organizácii
  - čo by organizácia mala mať (stručne ISMS)
  - aké zdroje na to potrebuje
  - postupnosť krokov na zavedenie ISMS
  - prínos ISMS pre organizáciu (ale aj náklady na udržiavanie)
  - alternatívne riešenia (čo sa stane ak sa KIB nebude riešiť)
- ak váš návrh vedenie organizácie schváli, dáte si dokopy oficiálny tím (zamestnanci organizácie, externí špecialisti) a buď si vymyslíte vlastný postup, alebo idete podľa BSI štandardov [7,8]

- **Pozor, začíname!**
- pripomínam: bezpečnostný proces = aktivity zamerané na dosiahnutie a udržanie potrebnej úrovne KIB v organizácii
- vedenie organizácie MUSÍ iniciovať a riadiť bezpečnostný proces v organizácii
- v ďalšom uvedieme kroky, ktoré treba spraviť. Viaceré z nich predstavujú aktivity, ktoré bude potrebné detailnejšie opísať (vypracovanie Politiky KIB, Stratégia KIB, špeciálne bezpečnostné politiky, vysokoúrovňová a podrobná analýza rizík)
- ale, aby sme si uchovali celkový prehľad, nepôjdeme zatiaľ do podrobností

vedenie organizácie MUSÍ

- prijať celkovú zodpovednosť za kybernetickú a informačnú bezpečnosť v organizácii (Politika KIB, Stratégia KIB)
- iniciovať, riadiť a monitorovať bezpečnostný proces
- vymenovať zamestnancov zodpovedných za KIB, poskytnúť im potrebné oprávnenia a zdroje
- pravidelne dostávať a vyhodnocovať informácie o stave KIB v organizácii, najmä informácie o možných rizikách vyplývajúcich z chýbajúcich alebo nedostatočných bezpečnostných opatrení

Definovanie bezpečnostných cieľov a stratégie

- Aby vedenie organizácie mohlo spustiť bezpečnostný proces v organizácii, MUSÍ špecifikovať a dokumentovať bezpečnostné ciele (security objectives) a stanoviť stratégiu KIB.
- Na realizáciu cieľov stanovených v Stratégii KIB musia byť v organizácii vytvorené primerané právne (interné predpisy) organizačné (kompetencie, organizačná štruktúra a roly) a materiálno-technické podmienky.
- Ciele Stratégie KIB sa musia premietnuť do konkrétnych úloh.
- vedenie organizácie MUSÍ riadiť bezpečnostný proces.
- Bezpečnostná stratégia a bezpečnostné ciele sa MUSIA pravidelne revidovať, aby sa zaistilo, že sú stále aktuálne a že sa dajú efektívne implementovať

Vydanie Politiky kybernetickej a informačnej bezpečnosti

- Politika KIB je základný dokument ISMS, ktorý
  - opíše význam KIB pre organizáciu,
  - definuje hlavné bezpečnostné ciele,
  - uvedie najdôležitejšie aspekty Stratégie KIB,
  - špecifikuje organizačnú štruktúru KIB.
- Je to vysokoúrovňový dokument, ktorý vytvára rámec pre ďalšie dokumenty, ktoré popisujú riešenie bezpečnostných problémov detailnejšie.
- V politike KIB MUSÍ byť jasne definovaný rozsah jej pôsobnosti
- MUSIA byť vysvetlené bezpečnostné ciele a ako súvisia s poslaním, úlohami a cieľmi organizácie
- Politika KIB MUSÍ byť dostupná všetkým zamestnancom organizácie, externým spolupracovníkom a iným ľuďom, ktorí sa podľa nej majú riadiť.
- Politika KIB BY MALA BYŤ pravidelne aktualizovaná.

Vymenovanie manažéra KIB

Kľúčovým človekom bezpečnostného procesu v organizácii je manažér KIB, ktorý

- presadzuje KIB v organizácii
- riadi a koordinuje bezpečnostný proces
- zabezpečuje podklady pre rozhodovanie vedenia organizácie v otázkach KIB.
- Mnoho (a veľmi rozmanitých) úloh definovaných vo vyhláškach [2][4] sa priamo alebo nepriamo týka manažéra KIB
- Aby ich bol schopný plniť, mal by mať potrebné znalosti a manažérske schopnosti, kompetencie, nevyhnutné zdroje a podporu vedenia

Vytvorenie vhodnej organizačnej štruktúry pre KIB

- Samotný manažér KIB na zaistenie potrebnej úrovne KIB v organizácii nestačí.
- v organizácii MUSÍ byť vytvorená vhodná organizačná štruktúra pre KIB
- určený člen vedenia, ktorý zodpovedá za KIB (garant KIB)
- výbor pre KIB,
- vytvorený útvar manažéra KIB
- MUSIA byť vytvorené bezpečnostné roly, do ktorých budú zaradení všetci zamestnanci a externí spolupracovníci.
- Zamestnanci MUSIA byť oboznámení s povinnosťami vyplývajúcimi z rôl, do ktorých sú zaradení.
- MUSIA byť naplánované, popísané, vytvorené a oznámené komunikačné kanály, aby sa varovania, informácie o bezpečnostných incidentoch a ďalšie relevantné informácie dostali čo najskôr k ľuďom, ktorí na ich základe majú konať.

Definovanie bezpečnostných opatrení

- Pre všetky aspekty spracovania informácie MUSIA byť definované primerané bezpečnostné opatrenia.
- Všetky bezpečnostné opatrenia musia byť systematicky dokumentované v bezpečnostných projektoch a v pravidelných intervaloch revidované.
- Opatrenia na zavedenie ISMS vytvoria základ, na ktorom sa dá stavať
- na napísanie politiky KIB je potrebné spraviť vysokoúrovňovú analýzu rizík, navrhnúť a implementovať opatrenia (zväčša organizačného alebo právneho charakteru)
- Opatrenia z vysokoúrovňovej analýzy rizík sa čiastočne prekrývajú s opatreniami na zavedenie ISMS a rozširujú/rozvíjajú základné opatrenia

- pri vysokoúrovňovej analýze rizík identifikujeme kľúčové aktíva organizácie a hrozby voči nim
- bude potrebné spraviť analýzu rizík (alebo bezpečnostný projekt) pre kľúčové aktíva
- . Po zavedení ISMS sa naštartuje štandardný cyklus správy rizík:
  - monitorovanie ISVS,
  - vyhodnocovanie účinnosti prijatých opatrení,
  - cielené analýzy rizík (dôležité oblasti a/alebo systémy ktoré dosiaľ neboli analyzované)
  - návrh a zavedenie opatrení.
  - Účinnosť opatrení ako aj fungovanie ISMS organizácie podlieha zo zákona [1] pravidelnému nezávislému auditu,

Zapojenie zamestnancov do bezpečnostného procesu

- Do bezpečnostného procesu MUSIA byť zapojení všetci pracovníci
- každý MUSÍ mať základné informácie o KIB, hrozbách a vedieť, ako používať bezpečnostné opatrenia vo svojej práci.
- Zamestnanci MUSIA mať možnosť zohrávať aktívnu rolu v KIB, MUSIA byť informovaní o príprave bezpečnostných opatrení a organizačných pravidiel.
- Keď sa zavádzajú bezpečnostné politiky, bezpečnostné nástroje, zamestnanci MUSIA byť primerane informovaní o tom, ako by sa mali používať.

Ďalšie kroky ku štandardnej úrovni KIB

- doteraz - najnutnejšie minimum potrebné na dosiahnutie základnej úrovne KIB (baseline)
- chceme sa dostať zo základnej úrovne aspoň na štandardnú (zákony a vyhlášky sú optimistické)
- prehodnotíme niektoré z existujúcich opatrení, doplníme nové
- pripomíname, že postupujeme podľa BSI noriem [7, 8]

Kontinuita KIB

- digitálny ekosystém je dynamický (technológie, hrozby, zraniteľnosti)
- KIB musí reagovať na vývoj aj náhle zmeny
- čo to znamená pre organizáciu:
  - potreba revidovať pravidelne bezpečnostnú dokumentáciu vrátane bezpečnostných cieľov
  - monitorovať účinnosť bezpečnostných opatrení,
  - vykonávať audity zamerané jednak na ISMS, jednak na kompletnosť a účinnosť opatrení,
  - sledovať výskyt hrozieb, objavenie nových zraniteľností,
  - korigovať, prípadne rušiť existujúce a prijímať nové opatrenia.

Riadenie KIB na úrovni organizácie

- zavedenie ISMS bol projekt
- teraz treba ukotviť bezpečnostný proces v štruktúre, plánovaní a procesoch organizácie
- čo máme:
  - základné dokumenty (Stratégia a politika KIB)
  - deklaráciu vedenia organizácie o podpore KIB
  - garanta KIB
  - manažéra KIB
  - možno aj bezpečnostný výbor/bezpečnostné fórum
  - vysokoúrovňovú a pre niektoré systémy možno aj podrobnú analýzu rizík
  - opatrenia

Riadenie KIB na úrovni organizácie

- čo by sme potrebovali
  - rozpracovanie úloh definovaných v politike KIB a všeobecných bezpečnostných opatrení:
  - špeciálne bezpečnostné politiky a ich implementáciu
  - zaradenie manažmentu KIB do manažérskych procesov (pravidelná výročná správa o stave KIB, plán práce a rozpočet KIB, hlásenia o závažných bezpečnostných incidentoch a ich riešení, bezpečnosť v projektoch, dopady legislatívy,...)
  - inventarizáciu aktív, priradenie vlastníkov aktívam, klasifikáciu aktív
  - definovanie bezpečnostných rol, zaradenie ľudí do rol, správa rol
  - systém vzdelávania v KIB (v ideálnom prípade všetkých ľudí podľa pracovného zaradenia, reálne aspoň základy KIB pre používateľov)
  - plány kontinuity činnosti, havarijné plány a ich implementáciu, vrátane cvičení
  - ...

Dokumentácia bezpečnostného procesu

- ak má KIB fungovať, nemôže byť postavená na dobrom slove a neformálnych dohodách
- jasne stanovené pravidlá, zodpovednosti, dokumentované procesy, udalosti
- povinná rozsiahla dokumentácia aj podľa zákonov a vyhlášok:
  - Stratégia KIB
  - Politika KIB
  - čiastkové politiky KIB
  - klasifikácia informácií a kategorizácia sietí a informačných systémov
  - výsledky kontroly zavedenia navrhovaných bezpečnostných opatrení
  - dokumentácia k analýzam rizík
  - správy auditov

Zvyšovanie bezpečnostného povedomia

- školenia (jednorazové, účelové) a vzdelávanie (systematické, na rozličnej odbornej úrovni)
- informácie o bezpečnostne relevantných udalostiach (adresné)
- vzdelávanie špecialistov na KIB (manažér KIB) informatikov, právnikov
- vytvoriť systém vzdelávania (aby sa rozumne využívali zdroje a aby sa na nikoho nezabudlo)
- vstupné školenia, školenia pri zaraďovaní do rôl, preškolenia pri zmenách politík, bezpečnostných mechanizmov, po bezpečnostných incidentoch

Zvyšovanie bezpečnostného povedomia

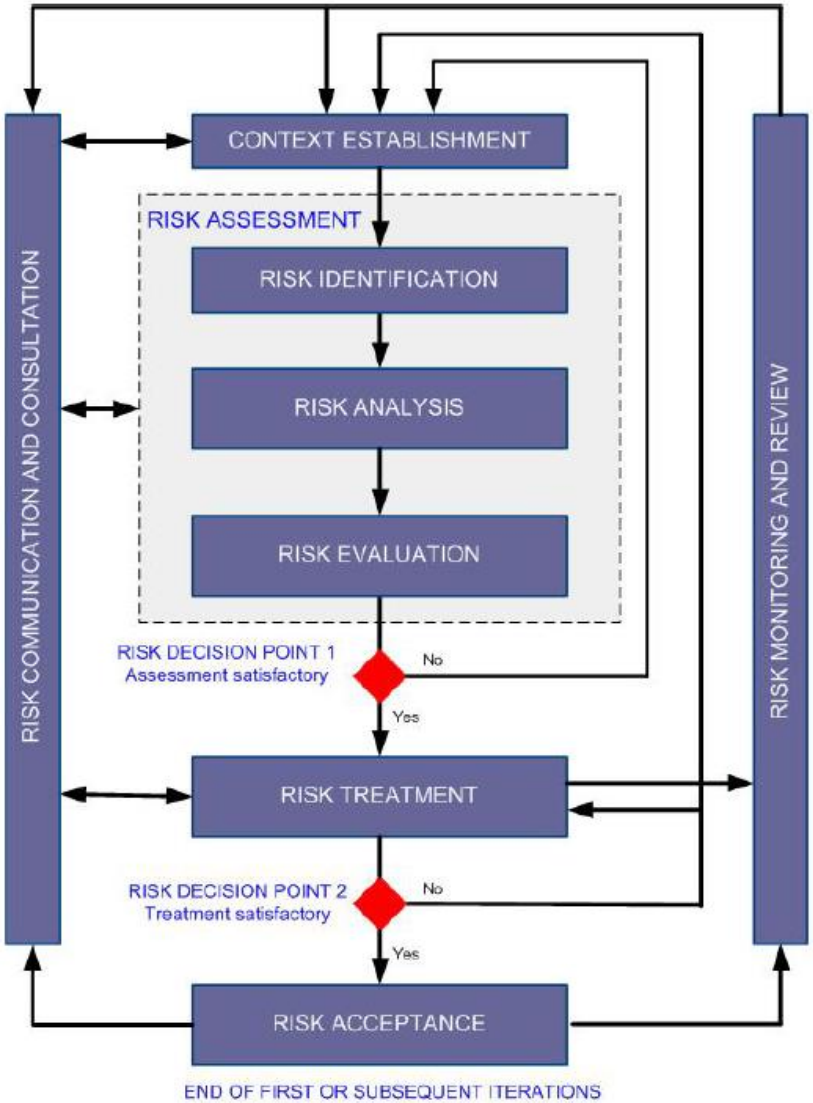
- realizácia - doma v organizácii, kombinácia externých špecialistov a vlastných zamestnancov (poznajú pomery v organizácii), externé vzdelávanie (školenia, kurzy, konferencie, pravidelné semináre na vš a pod.)
- existujú znalostné štandardy pre laikov, vedúcich pracovníkov, informatikov, špecialistov v KIB, lektorov - možno sa inšpirovať, časom budú možno vzdelávacie programy

Efektívne využívanie zdrojov na KIB

- Na zaistenie požadovanej úrovne KIB bude organizácia potrebovať finančné a personálne zdroje a zariadenia.
- Tieto požiadavky predkladá manažér KIB spolu s návrhom opatrení vedeniu organizácie
- Ekonomické aspekty KIB sa musia zohľadniť aj v Stratégii KIB
- Keď sa stanovujú bezpečnostné ciele, musia byť zrejmé aj náklady, ktoré sú s tým spojené a prostriedky potrebné na KIB by mali byť poskytnuté včas
- Rovnako je treba realisticky odhadnúť čas potrebný na plnenie úloh najmä manažéra KIB
- V prípade keď úlohy prevyšujú kapacity, je potrebné do ich riešenia zapojiť ďalších zamestnancov, alebo externých odborníkov

Otvorené otázky

- máme (dúfam) celkový obraz, čo treba a v akom poradí spraviť
- pár úloh ostáva otvorených - ako konkrétne
- pozrieme sa na
  - správu rizík
  - štruktúru bezpečnostných politík druhej úrovne
- pripomíname, že každej z týchto tém by bolo možné venovať minimálne jednu samostatnú prednášku (aj viac)
- podrobnejšie - prednáška manažment KIB a učebnica


CONTEXT ESTABLISHMENT
RISK ASSESSMENT
RISK IDENTIFICATION
RISK ANALYSIS
RISK EVALUATION
RISK DECISION POINT 1
Assessment satisfactory
No
Yes
RISK TREATMENT
RISK DECISION POINT 2
Treatment satisfactory
No
Yes
RISK ACCEPTANCE
END OF FIRST OR SUBSEQUENT ITERATIONS
RISK COMMUNICATION AND CONSULTATION
RISK MONITORING AND REVIEW

- podstatou bezpečnostného procesu je správa rizík a kľúčovým prvkom správy rizík je analýza rizík
- analýzou a správou rizík sa zaoberajú normy ISO/IEC 27005 a BSI-Standard 200-3
- základná schéma činností spadajúcich do správy rizík je uvedená na nasledujúcom obrázku, prevzatom z normy ISO/IEC 27005
- stručne vysvetlíme jednotlivé kroky

Stanovenie kontextu (analýzy rizík)

- na začiatku si treba explicitne povedať, čím sa budeme zaoberať, do akej hĺbky a prečo
- stanovenie rozsahu, teda toho, čoho sa analýza rizík týka (celá organizácia, kľúčový systém, osobné údaje)
- vysokoúrovňová , alebo podrobná analýza rizík
- Zákon o KB, Zákon o ITVS, zavádzame nový systém, zažili sme nepríjemný bezpečnostný incident,...
- prípadne explicitne povedať, akú metodiku budeme používať
- základné parametre - hranice akceptovateľného rizika

Cieľom identifikácie rizík je určiť, čo nežiadúce by pri spracovávaní informácie mohlo nastať a spôsobiť organizácii stratu, kde by k tomu mohlo dôjsť a prečo. Pri identifikácii rizík je potrebné určiť

- aktíva
- zraniteľnosti týchto aktív
- relevantné hrozby voči aktívam
- existujúce bezpečnostné opatrenia chrániace aktíva

Aktíva

- teoreticky by mala organizácia mať a udržiavať zoznam aktív
- nanajvýš bude mať inventárny zoznam fyzických aktív
- identifikácia aktív - zhora nadol
  - poslanie organizácie
  - činnosti, ktoré na naplnenie poslania vykonáva (teoreticky až na úroveň procesov)
  - zdroje, ktoré pri tom používa (informácie, zariadenia, kde sa tieto informácie spracovávajú, ľudia) infraštruktúra a bezpečnostné okolie
  - pre každé aktívum - katalógový list (pozri BSI standard) a stanovenie vlastníka

Identifikácia zraniteľností a hrozieb

- prejsť si cez zoznam aktív a zoznam zraniteľností a určiť, ktoré aktíva majú jednotlivé zraniteľnosti
- toto je dôležité pre posúdenie relevantnosti hrozieb
- potom prejdeme cez zoznam hrozieb a aktív a určíme, ktoré hrozby sa voči danému aktívu môžu naplniť, lebo aktívum má zraniteľnosti, ktoré môže hrozba využiť
- v podstate píšeme scenáre naplnenia hrozieb (bezpečnostných incidentov)
- nasledujúca tabuľka obsahuje zoznam elementárnych hrozieb (katalóg BSI)
- dopady sa posudzujú z hľadiska narušenia dôvernosti (C), integrity (I) a dostupnosti (A)

Zoznam hrozieb

kód	Hrozba	dopad
H.1	Oheň	A
H.2	Nepriaznivé podmienky prostredia	I,A
H.3	Voda	I,A
H.4	Znečistenie/špina, prach, korózia	I,A
H.5	Prírodné katastrofy	A
H.6	Katastrofy v okolitom prostredí	A
H.7	Veľké udalosti v okolitom prostredí	C,I,A
H.8	Prerušenie alebo porucha dodávky energie	I,A
H.9	Zlyhanie alebo porucha komunikačných sietí	I,A
H.10	Zlyhanie alebo porucha dodávateľských reťazcov	A
H.11	Zlyhanie alebo porucha poskytovateľov služieb	C,I,A

kód	Hrozba	dopad
H.12	Elektromagnetická interferencia	I,A
H.13	Zachytávanie kompromitujúceho vyžarovania	C
H.14	Špionáž	C
H.15	Napichnutie komunikačnej linky	C
H.16	Krádež zariadení, pamäťových médií a dokumentov	C,A
H.17	Strata zariadení, pamäťových médií a dokumentov	C,A
H.18	Slabé plánovanie alebo chýbajúce úpravy (plánov)	C,I,A
H.19	Odhalenie informácie, ktorá mala byť chránená	C
H.20	Informácia z nespoľahlivého zdroja	C,I,A
H.21	Manipulácia s hardvérom alebo softvérom	C,I,A
H.22	Manipulácia s informáciou	I
H.23	Neoprávnený vstup do IT systémov	C,I

kód	Hrozba	dopad
H.24	Zničenie zariadení alebo pamäťových médií	A
H.25	Zlyhanie zariadení alebo systémov	A
H.26	Poruchy zariadení alebo systémov	C,I,A
H.27	Nedostatok zdrojov	A
H.28	Zraniteľnosti alebo chyby softvéru	C,I,A
H.29	Porušenie zákonov alebo zmlúv	C,I,A
H.30	Neoprávnené použitie alebo správa zariadení a systémov	C,I,A
H.31	Nesprávne použitie alebo správa zariadení a systémov	C,I,A
H.32	Zneužitie oprávnení	C,I,A
H.33	Strata personálu	A
H.34	Útok	C,I,A
H.35	Nátlak, vydieranie, korupcia C,I,A	
H.36	Krádež identity	C,I,A

kód	Hrozba	dopad
H.37	Popretie konania	C,I
H.38	Zneužitie osobných údajov	C
H.39	Malvér	C,I,A
H.40	Odmietnutie služieb	A
H.41	Sabotáž	A
H.42	Sociálne inžinierstvo	C,I
H.43	Importovanie správ	C,I
H.44	Neoprávnený vstup do priestorov	C,I,A
H.45	Strata údajov	A
H.46	Strata integrity informácie, ktorá mala byť chránená	I
H.47	Škodlivé bočné efekty	C,I,A

Zraniteľnosti

- podobná tabuľka ako je tabuľka hrozieb sa dá spraviť aj pre zraniteľnosti
- na ilustráciu z nej časť uvedieme
- detailnejší popis je v učebnici, BSI štandarde 200-3 a ISO/IEC norme 27005

kód	Zraniteľnosť
Z.1	Koncepčné a organizačné
Z.1.1	chýbajúca alebo nedostatočne rozpracovaná koncepcia kybernetickej a informačnej bezpečnosti organizácie
Z.2	Organizácia KIB
Z.2.1	Chýbajúci alebo nedostatočný organizačný a riadiaci rámec, ktorý by umožňoval iniciovať a riadiť zavedenie a udržiavanie KIB v organizácii
Z.2.2	Chýbajúce pravidlá upravujúce prácu na diaľku a používanie mobilných zariadení a/alebo ich nedostatočné uplatňovanie

kód	Zraniteľnosť
Z.3	Bezpečnosť ľudských zdrojov
Z.3.1	Chýbajúce alebo nedostatočné procedúry na overenie toho, či budúci zamestnanci a potenciálni poskytovatelia služieb rozumejú svojej zodpovednosti za KIB a či sú vhodní na plnenie úloh, o ktorých sa s nimi uvažuje
Z.3.2	Nedostatočná úroveň bezpečnostného povedomia zamestnancov a neplnenie povinností v KIB zamestnancami a tretími stranami kvôli neporozumeniu povinností a nedostatočnej kontrole
Z.3.3	Absencia, neúplnosť alebo nedodržiavanie procedúr pri zmene alebo ukončení pracovného pomeru

Existujúce opatrenia

- organizácia už možno prijala nejaké opatrenia
- tieto možno bude treba prehodnotiť, ale
- potrebujeme o nich vedieť, lebo
- opatrenia znižujú hodnotu rizika (ktoré budeme odhadovať)
- opatrenia musia tvoriť ucelený systém (diery a duplicita)

Analýza rizík-dopad

- najprv nastavíme parametre pre stanovenie hodnoty rizika
- dopad je
  - nízky, ak sú finančné straty pre organizáciu zanedbateľné, nedošlo k ohrozeniu zdravia a ži-vota ľudí, narušeniu zmluvných záväzkov a povinností organizácie a organizácia je schopná plniť úlohy vyplývajúce z jej poslania bez obmedzenia;
  - vysoký, ak (napr.) finančné straty v dôsledku naplnenia hrozby organizácia nie je schopná vykryť z vlastných zdrojov (napr. nie je schopná v dostatočne krátkom čase nahradiť a spus-tiť do prevádzky kľúčový systém organizácie), došlo k vážnemu ohrozeniu zdravia, prípadne smrti ľudí, organizácia nie je schopná dlhodobo (dni, týždne, mesiace) plniť svoje základné úlohy a plniť záväzky;
  - stredný, ak je závažnosť dopadu vyššia ako nízka a nižšia ako vysoká.

- parametre pre stanovenie hodnoty rizika
- Pravdepodobnosť naplnenia hrozby je
  - nízka, ak k naplneniu hrozby ešte nedošlo, alebo došlo raz za niekoľko rokov,
  - stredná, ak k naplneniu hrozby dochádza raz za niekoľko mesiacov,
  - vysoká, ak naplneniu hrozby dochádza každý týždeň.
  - K týmto trom hodnotám pridáme ešte nulovú, aby sme ošetrili prípady, keď sa hrozba na niektoré z aktív nevzťahuje (a teda sa nemôže naplniť).

- pre každé aktívum a relevantnú hrozbu skúmame scenáre naplnenia hrozby (s využitím zraniteľností)
- pravdepodobnosť a dopad hrozby skombinujeme do hodnoty rizika napríklad takto:

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

Table: Výpočet hodnoty rizika

Vyhodnotenie rizika

- pre názornosť: semafórové farby riziko vysoké, stredné,nízke
- dve tabuľky+ katalóg
- katalóg aktív, ku každému aktívu popis a hrozby, zraniteľnosti, riziká, scenáre, opatrenia
- 2D tabuľka hrozby x aktíva, položky = hodnoty rizika
- tabuľka, zoznam rizík usporiadaný podľa hodnoty
- vyhodnotenie rizika: kde spravíme čiaru (akceptovateľné riziko)

Ošetrenie rizík-možnosti

- akceptovať riziko
- prijať opatrenie na elimináciu, alebo zníženie rizika na akceptovateľnú úroveň,
- vyhnúť sa riziku (nahradiť rizikové riešenie iným) alebo
- preniesť riziko (poistenie).

Ďalšie kroky (ktoré už formálne nespadajú do analýzy rizík)

- sú návrh a implementácia opatrení
- potom monitoring systému, aby sa zistilo, či sú opatrenia účinné, či hodnota niektorého zo zostatkových rizík (neošetrených rizík, resp. rizík, ktorých pôvodnú hodnotu znížili prijaté opatrenia) nevzrástla nad akceptovateľnú úroveň, resp. či sa neobjavili nové zraniteľnosti alebo hrozby, ktoré neboli v čase analýzy rizík známe.

Celý tento proces (analýza rizík, prijatie opatrení, monitoring systému, revízia opatrení) prebieha kontinuálne a nazýva sa správa rizík (risk management).

Zoznam bezpečnostných politík 2. úrovne

- Riadenie prístupu
- Klasifikácia informácie a narábanie s informáciou
- Fyzická bezpečnosť a bezpečnosť prostredia
- Bezpečnostné pravidlá pre koncového používateľa
- Zálohovanie
- Manažment bezpečnosti sietí
- Prenos informácie
- Ochrana pred škodlivým kódom
- Manažment technických zraniteľností
- Kryptografické opatrenia
- Ochrana súkromia a osobných údajov
- KIB vo vzťahoch s tretími stranami
- Zaznamenávanie udalostí a monitorovanie
- Organizácia KIB

Riadenie prístupu

- Ide o prierezovú problematiku, bez jej spoľahlivého riešenia nie je možné zaistiť KIB v organizácii.
- Cieľom riadenia prístupu je zaistiť, aby
  - k informačným aktívam organizácie mali prístup (a mohli s nimi pracovať) len oprávnené osoby,
  - mohli s nimi alebo prostredníctvom nich vykonávať len činnosti, na ktoré majú oprávnenie
  - a zabrániť prístupu neoprávnených osôb k aktívam organizácie.
- Politika riadenia prístupu upravuje manažment prístupových práv a prípadne aj spôsob ich uplatňovania
  - kto stanovuje prístupové práva, prideľuje a odoberá ich
  - spôsob a úroveň identifikácie a autentifikácie
  - zásady pri vytváraní, používaní, ochrane a strate autentifikačných prostriedkov a pod.

Klasifikácia informácie a narábanie s informáciou

- Klasifikácia informácie umožňuje štandardizovať úroveň ochrany informačných aktív organizácie, a to tak z hľadiska cieľov ako aj úrovne ochrany.
- Cieľom ochrany je zaistenie dôvernosti, integrity a dostupnosti informačných aktív, úroveň ochrany je nízka, stredná alebo vysoká.
- V prípade verejných informácií je úroveň dôvernosti nulová.
- Kategorizácia systémov je odvodená od klasifikácie informácií, ktoré sa v nich spracovávajú.
- Význam klasifikácie informácie a kategorizácie systémov je v tom, že je možné zoskupiť informácie vzhľadom na potreby ich ochrany do tried s rovnakými bezpečnostnými potrebami a navrhovať riešenia pre triedy a nie pre jednotlivé aktíva.
- pozri FIPS 199 a FIPS 200

Fyzická bezpečnosť a bezpečnosť prostredia

- Informáciu v konečnom dôsledku spracovávajú fyzické zariadenia, ktoré na svoju činnosť potrebujú primerané podmienky.
- Fyzická bezpečnosť a bezpečnosť prostredia sa zaoberá ochranou pred hrozbami fyzického charakteru,
- jej cieľom je zabrániť neoprávnenému fyzickému prístupu k informačným aktívam organizácie, ich fyzickému poškodeniu alebo zasahovaniu do nich.
- politika definuje zabezpečené priestory a pravidlá pre vstup do nich a prácu v nich
- narábanie s IKT zariadeniami v organizácii a mimo nej (vynášnie, práca doma, opravy, vyraďovanie a pod.)

Bezpečnostné pravidlá pre koncového používateľa

- Koncový používateľ je rola s najväčším počtom členov.
- Koncový používateľ má najmenšie privilégiá, najmenšie vedomosti z kybernetickej a informačnej bezpečnosti a informatiky.
- Môže z nevedomosti spraviť chyby, ktoré ohrozia IKT organizácie.
- zároveň je to osoba, kvôli ktorej organizácia prevádzkuje svoje IKT, lebo koncový používateľ pomocou nich vykonáva činnosť, kvôli ktorej bola organizácia zriadená.
- Koncový používateľ nepotrebuje špecializované vedomosti z kybernetickej a informačnej bezpečnosti, potrebuje vedieť,
  - čo má robiť,
  - čo nesmie robiť
  - a na koho sa má obrátiť, keď narazí pri práci s IKS na problém, s ktorým si nevie poradiť.

Zálohovanie

- Zálohovanie je prostriedok na zabránenie straty/dostupnosti údajov.
- Politika zálohovania upravuje
  - stanovenie potrieb organizácie na vytváranie záloh informácie, softvéru a systémov
  - zaistenie dostatočných záložných kapacít na obnovu informácie a softvéru po poškodení alebo zlyhaní
  - plán zálohovania (čo zálohovať, ako a ako často)
  - ukladanie záloh
  - ochrana záloh ekvivalentná ochrane primárnej informácie
  - testovanie kvality pamäťových médií použitých na uchovávanie záloh
  - testovanie procedúr obnovy
  - prípadná ochrana zálohovaných údajov (podľa klasifikácie) šifrovaním

- Organizácia pre svoju činnosť potrebuje zaistiť spoľahlivú komunikáciu svojich systémov navzájom a s externými systémami, na ktorú využíva komunikačné siete.
- Cieľom tejto politiky je zaistiť ochranu informácií v sieťach a informačných systémoch, ktoré prepája

- Toto je druhá, netechnická časť oblasti Bezpečnosti komunikácie.
- Prvá sa zaoberá bezpečnosťou sietí.
- Informácia sa málokedy spracováva a využíva na mieste, kde bola zaznamenaná (zdroj informácie), ale prenáša sa tak medzi rôznymi subjektami v rámci organizácie, ako aj medzi organizáciou a inými externými inštitúciami a jedincami.
- Cieľom tejto špeciálnej politiky je zaistiť bezpečnosť informácie prenášanej v organizácii a medzi organizáciou a externým subjektom.

Ochrana pred škodlivým kódom

- Škodlivý kód (malvér, angl. malware) označuje program, ktorý je tajne vložený do iného programu so zámerom zničiť údaje, spustiť deštruktívne, alebo ďalej sa šíriace programy, alebo inak kompromitovať dôvernosť, integritu alebo dostupnosť údajov, aplikácií alebo operačných systémov obete.
- politika stanovuje zásady znižujúce pravdepodobnosť zanesenia škodlivého kódu do systémov organizácie ako napr.
  - pamäťové médiá prinesené zvonka do organizácie sa musia pred použitím skontrolovať na prítomnosť škodlivého kódu
  - prílohy elektronickej pošty sa pred otvorením musia skontrolovať
  - zákaz posielať mailom súbory, ktoré môžu obsahovať škodlivý kód (napr. exe)
  - obmedzenie alebo úplný zákaz používania vlastných aplikácií a nepotrebného softvéru

Ochrana pred škodlivým kódom

- zákaz používania pamäťových médií v externom prostredí (USB kľúče v internetovej kaviarni)
- špecifikácia, aké sw nástroje na ochranu pred škodlivým kódom sa pre jednotlivé typy zariadení vyžadujú,
- vysokoúrovňové požiadavky na konfiguráciu a udržiavanie sw
- obmedzenie alebo zákaz používania vlastných zariadení v sieti organizácie, alebo pre prácu na diaľku
- zvyšovanie bezpečnostného povedomia koncových používateľov a ľudí zodpovedných za riešenie bezpečnostných incidentov (Ako nezamoriť organizáciu škodlivým kódom)
- redukovanie zraniteľností (včasné identifikovanie nových zraniteľností a inštalácia záplat), konfigurácia systémov, uplatňovanie princípu najmenších privilégií

Ochrana pred škodlivým kódom

- riešenie bezpečnostných incidentov
- príprava reakcie na bezpečnostný incident (infiltráciu škodlivého kódu)
- postup pri identifikácii zasiahnutého systému
- stanovenie priorít pre zásah
- analýza škodlivého kódu
- lokalizácia škodlivého kódu (containment)
- eradikácia škodlivého kódu
- obnova
- vyhodnotenie a závery vyvodené z bezpečnostného incidentu (zmeny bezpečnostnej politiky, zmeny vzdelávacích programov a školení, rekonfigurácia programového vybavenia, inštalácia antivírového sw, prípadne jeho rekonfigurácia)

- Zraniteľnosti svojich aktív bude organizácia skúmať pri analýze rizík a navrhovať opatrenia, ktoré ich odstránia, alebo aspoň zmenšia možnosti ich využitia.
- Niektoré zraniteľnosti organizácia nebude schopná odstrániť a časom sa môžu objaviť nové zraniteľnosti (najčastejšie sú to chyby v programovom vybavení).
- Tvorcovia programového vybavenia reagujú na objavenie sa nových zraniteľností okamžitými riešeniami (záplatami) a z času na čas aj novými verziami (väčších častí) programov.

- Cieľom tejto politiky je zabrániť využitiu technických zraniteľností
  - stanovením zodpovednosti za za úlohy spojené s manažmentom technických zraniteľností (monitorovanie zraniteľností
  - zodpovednosti za identifikáciu a sledovanie zdrojov informácií o zraniteľnostiach, udržiavanie aktuálneho zoznamu informačných aktív organizácie
  - definovaním postupnosti krokov, ktorými organizácia reaguje na informáciu o potenciálnej technickej zraniteľnosti
  - monitorovanie, revízie procesu manažmentu technických zraniteľností
  - definovaním postupu pre prípad, keď nie sú k dispozícii vhodné opatrenia na ošetrenie objavenej technickej zraniteľnosti.

Kryptografické opatrenia

- Kryptografické riešenia sú základom kybernetickej a informačnej bezpečnosti;
- pomocou kryptografických funkcií sa zaisťuje dôvernosť, integrita a dôvernosť informácie/údajov.
- Kryptografické funkcie sú postavené na ťažkých matematických problémoch a modifikácie alebo nesprávne použitie týchto funkcií vytvára takmer isto zraniteľnosti v systéme, v ktorom sa používajú.
- Organizácie používajú štandardné kryptografické riešenia (šifrovanie na ochranu dôvernosti, digitálne odtlačky na zaistenie integrity a elektronické podpisy, pečate na zaistenie autentickosti dokumentov/údajov.

- Politika špecifikuje
  - na čo sa v organizácii používajú kryptografické funkcie
  - algoritmy a ich parametre
  - správu kryptografických kľúčov
  - zodpovednosti za implementáciu politiky a manžmentu kľúčov,
  - a dopad používania šifrovania na iné bezpečnostné opatrenia (detekcia škodlivého kódu), kontrola a audit

Ochrana súkromia a osobných údajov

- organizácia spracováva a je povinné primerane chrániť aj osobné údaje.
- Nemá zmysel vypracovávať paralelné bezpečnostné projekty;
- ochranu osobných údajov je možné zakomponovať do projektu KIB
- politiku ochrany osobných údajov vydať ako špeciálnu bezpečnostnú politiku.

Obsah Politiky

- Zodpovednosť za ochranu osobných údajov v organizácii (kto za čo zodpovedá – vedenie, zodpovedná osoba, osobný úrad, vlastníci a technickí správcovia systémov, v ktorých sa spracovávajú osobné údaje, vedúci pracovníci,...)
- Čo sú osobné údaje, všeobecné dôvody, prečo ich organizácia spracováva, potreba ich ochrany
- Z čoho Politika vychádza (GDPR) a ako súvisí s Politikou KIB, resp. kybernetickou a informačnou bezpečnosťou v organizácii
- Základné zásady pri spracovaní osobných údajov (podľa GDPR)
- Účely spracúvania osobných údajov a právne základy na ktorých je spracúvanie založené
- postupy (treba sa pozrieť na doposiaľ používané štandardné postupy pri spracúvaní osobných údajov a porovnať ich s požiadavkami GDPR a prípadne upraviť)

- vzdelávanie v oblasti ochrany osobných údajov a udeľovanie poverenia a pokynov pre interných príjemcov osobných údajov
- opatrenia – všeobecné (KIB) a špecifické (nahlasovanie bezpečnostných incidentov Úradu na ochranu osobných údajov, oboznamovanie dotknutých osôb, dohody s tretími stranami a pod.)
- postupy v mimoriadnych situáciách (bezpečnostné incidenty)
- analýza rizík (KIB a osobné údaje), audit
- správa Politiky ochrany osobných údajov

KIB vo vzťahoch s tretími stranami

- K informačným aktívam organizácie majú prístup aj dodávatelia, poskytovatelia rôznych informačných služieb a zamestnanci tretích strán.
- Cudzie osoby sú povinné dodržiavať Bezpečnostnú politiku KIB a predpisy KIB, ale organizácia nemá také možnosti presadzovania bezpečnostných politík voči nim , ako voči vlastným zamestnancom
- organizácia zvlášť analyzuje riziká vyplývajúce z prístupu cudzích osôb k jej informačným aktívam, zavádza a udržiava opatrenia na minimalizáciu týchto rizík
- opatrenia a povinnosti pre tretie strany pristupujúce k informačným aktívam organizácie, organizácia prerokováva so zainteresovanými stranami a zahŕňa do zmlúv.
- Tieto povinnosti sa týkajú aj subdodávateľov a v primeranej miere aj ostatných článkov dodávateľského reťazca

Zaznamenávanie udalostí a monitorovanie

- bezpečnostne relevantné aktivity v systémoch organizácie sú kontinuálne monitorované a vytvára sa o nich záznam auditu, aby sa
  - zabezpečilo dodržiavanie bezpečnostnej politiky,
  - umožnilo stanovovať zodpovednosť za aktivity v systémoch organizácie a
  - včas odhalili pokusy o narušenie jej informačných aktív
- politika stanovuje najmä
  - rámcovo čo sa bude zaznamenávať
  - kto o tom rozhodne
  - kto bude zodpovedať za záznam auditu
  - kto bude mať prístup k záznamom auditu
  - ako dlho sa bude záznam auditu uchovávať
  - povinnosť synchronizácie hodín jednotlivých systémov

- Dlhodobé a systematické riešenie KIB v organizácii si vyžaduje koordinovanú činnosť rôznych ľudí.
- Bude potrebné vytvoriť špecializovaný útvar, ktorý sa bude venovať výlučne KIB, pozíciu manažéra KIB, ktorý bude činnosti KIB koordinovať, riadiť a čiastočne aj zabezpečovať.
- Ďalším zamestnancom pribudnú povinnosti v KIB, ktoré budú formalizované v podobe bezpečnostných rôl.
- Tiež bude potrebné prepojiť manažment KIB s manažmentom takých činností, ktoré majú dopad na bezpečnosť ISVS MH SR (obstarávanie systémov, prijímanie a prepúšťanie pracovníkov, zmeny pracovného zaradenia).

Ako ďalej, manažér KIB?

- úloh je veľa, zhrnieme najdôležitejšie
- začiatok systematického bezpečnostného procesu má charakter projektu
- dajú sa využiť externé zdroje, ale
- aby veci fungovali, treba v plnom rozsahu (a primeranej miere) zapojiť vlastných pracovníkov
- asi nebude dobrá stratégia zasypať organizáciu bezpečnostnými politikami, smernicami a vzniesť ultimatívne požiadavky na vedenie - to je cesta k odvolaniu manažéra KIB
- zainteresovať kľúčových ľudí (bezpečnostný výbor: garant, vedúci personálneho, právneho, informatik, správa budov, ochrana osobných údajov)
- prejsť si na výbore výsledky vysokoúrovňovej analýzy rizík

Čo bude ďalej, manažér KIB?

- plán práce
- dávať veci do poriadku postupne (interný web s informáciami pre zamestnancov, bod na porade vedúcich zamestnancov organizácie, inventarizácia aktív, klasifikačná schéma, stanovenie vlastníkov, pomoc vlastníkom aktív pri klasifikácii, bezpečnostné roly, základné školenia nových pracovníkov, priradenie KIB k BOZP školeniam, bezpečnostné projekty kľúčových systémov, audit, zapojenie KIB do nových projektov, informovať o hrozbách, výsledkoch)
- napojenie na rozpočet+pravidelne správa o stave KIB v organizácii
- ďalšie možnosti rozvoja - štandardná úroveň pre celú organizáciu a *core protection* pre kľúčové systémy (BSI štandardy)
- pozor! DO KIB sa dá investovať neobmedzené množstvo peňazí!

Záver

- (z hľadiska predmetu UIB) teraz sa už dá prečítať Zákon o KB, Zákon o ITVS a vyhlášky 362/2018 a 179/2020 lebo už zhruba vieme čo sa od nás (ako manažéra KIB) čaká
- podrobnejšie v učebnici, resp. na prednáške z manažmentu KIB
- aby ste mali predstavu o zložitosti úlohy: robili sme bezpečnostný projekt na ministerstve X, 10 ľudí v tíme, pol roka, cca 2000-3000 hodín, 11 dokumentov 800+ strán a množstvo ďalších pomocných údajov
- a to sme nerobili detailnú analýzu rizík, ani sme nepísali bezpečnostné politiky 2. úrovne

Veľa zdaru, budúci manažéri KIB!

Zdroje

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (v znení neskorších predpisov).

[2] Vyhláška Národného bezpečnostného úradu, č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

[3] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

[4] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

[5] ISO/IEC 27001 — Information security management systems — Requirements.

[6] ISO/IEC 27002 — Code of practice for information security management.

[7] BSI Standard 200-1 Information Security Management Systems (ISMS) www.bsi.bund.de/grundschutz

[8] BSI Standard 200-2 IT Grundschutz Methodology, www.bsi.bund.de/grundschutz

[9] BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz BSI

[10] IT-Grundschutz Compendium, BSI 2019

Zdroje

[11] FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

[12] FIPS 200 Minimum Security Requirements for Federal Information and Information Systems

[13] ISO/IEC 27005 — Information security risk management.