MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Odbor riadenia kybernetickej a informačnej bezpečnosti

Verzia 1.0 | kyberbezpecnost@mirri.gov.sk

Povinnosti správcu ISVS v kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní

Manažérske zhrnutie

Prevádzka informačného systému verejnej správy (ISVS) je podľa zákona o kybernetickej bezpečnosti [1] základnou službou a prevádzkovateľ[1] tejto služby je povinný (podľa dôležitosti systému) na jeho ochranu prijať bezpečnostné opatrenia podrobnejšie uvedené vo vyhláške [2]. ISVS je aj informačnou technológiou verejnej správy a zákon o informačných technológiách vo verejnej správe [3] a vyhláška [4] definujú množstvo opatrení, ktoré jeho správca na jeho ochranu musí prijať. Pritom nejde len o formálnu povinnosť, lebo ochrana ISVS je objektívne potrebná, bez nej by mohlo dôjsť k narušeniu ISVS a bez funkčného ISVS organizácia nebude schopná vykonávať v požadovanom rozsahu a kvalite svoju činnosť. Oba zákony a vykonávacie predpisy vychádzajú z medzinárodných noriem, ktoré popisujú cieľový stav (z čoho všetkého má ochrana ISVS pozostávať), ale nezohľadňujú východiskový stav a zdroje, ktoré má na zaistenie bezpečnosti svojho ISVS správca k dispozícii.

Tento dokument vychádza z vyššie uvedených právnych noriem [1][2][3][4], opiera za o povinnosť správcu ISVS II. a III. kategórie zaviesť v organizácii systém riadenia informačnej bezpečnosti (ISMS[2]) [3] a popisuje postup ako vybudovať ISMS pokrývajúci požiadavky uvedené v právnych normách [1][2][3][4], požiadavky medzinárodných noriem a ktorý je zároveň dostatočne flexibilný na to, aby v rámci neho bolo možné reagovať na zmeny v organizácii aj vo vonkajšom prostredí. Dokument popisuje úlohy v kybernetickej a informačnej bezpečnosti vedenia organizácie, ktorá je správcom ISVS II. alebo III. kategórie podľa kritérií z vyhlášky [4], ktoré majú koncepčný, právny, organizačný, kontrolný a koordinačný charakter, ale nezaťažuje riadiacich pracovníkov realizačnými podrobnosťami, ktoré budú predmetom iných dokumentov určených pre bezpečnostného manažéra a iné osoby poverené konkrétnymi úlohami v KIB. Navrhované riešenie vychádza z noriem [8][9] a Kompendia [10] a výsledný ISMS je plne v súlade s ISO normou [5].

[1] terminológia vychádza zo zákonov [1][3]
[2] Information security management system

1 Úvod

Digitálne informačné a komunikačné technológie (d-IKT) sú kritickou infraštruktúrou spoločnosti a to nielen štátu, ale aj mnohých štátnych a iných organizácií, vrátane súkromných, pretože sa pomocou nich spracováva veľké množstvo informácií, riadia technologické procesy a poskytujú on-line služby; t.j. vykonávajú činnosti, ktoré nie je v dostatočnom rozsahu a kvalite možné vykonávať bez d-IKT.

Existuje veľa faktorov, ktoré môžu spôsobiť narušenie d-IKT organizácie a tým ohroziť až znemožniť plnenie jej povinností; vrátane cielených a úmyselných útokov, technických porúch, ľudských chýb a omylov, organizačných nedostatkov a prírodných vplyvov. Ochrana informácií a d-IKT je preto nutnou podmienkou normálneho fungovania organizácie. Navyše, d-IKT sú tak prepojené, že narušenie d-IKT v jednej organizácii môže vyvolať dominový efekt a zasiahnuť aj iné organizácie a poškodiť spoločnosť ako celok.

Informatizáciu spoločnosti (e-government, e-Health, e-commerce, najnovšie počas pandémie dištančné vzdelávanie a prácu z domu, organizácia testovania a očkovania) sa dá stavať len na spoľahlivo fungujúcich d-IKT a dôveryhodných riešeniach. Preto štát ochranu d-IKT a informácie neponecháva na dobrú voľu organizácií, ale zákonmi im stanovil povinnosť zaistiť potrebnú úroveň ochrany, dôležitých systémov a sietí[3], ktoré spravujú; t.j. zaistiť ich kybernetickú a informačnú bezpečnosť.

Pojem kybernetická a informačná bezpečnosť (KIB) má trojaký význam:

- multiodborová disciplína, zaoberajúca sa skúmaním hrozieb voči d-IKT a hľadaním spôsobov, ako zabrániť naplneniu týchto hrozieb,
- činnosť zameraná zabezpečeniu ochrany d-IKT,
- stav ochrany informácie a d-IKT.

Povinnosti chrániť informáciu, informačné systémy a siete teda rámcovo stanovuje organizáciám viacero zákonov, pre verejnú správu sú najdôležitejšie tie, ktoré sa vzťahujú na organizácie, ktoré spravujú informačné systémy verejnej správy (a definujú konkrétne požiadavky):

1) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, (zákon o KB),
2) Vyhláška Národného bezpečnostného úradu č. 362/2018, 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, (zákon o ITVS),
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.

Okrem týchto právnych noriem treba zobrať do úvahy aj ďalšie zákony a vyhlášky (GDPR, Zákon o e-gov, Zákon o kritickej infraštruktúre, Zákon o ochrane utajovaných skutočností, Nariadenie e-IDAS a i.)

Čiastočná (neúplná) ochrana d-IKT nemá veľký význam, lebo najmä cieľavedomý protivník môže využiť jedno nechránené slabé miesto (zraniteľnosť) a preniknúť do systému organizácie, preto vyššie uvedené zákony stanovujú povinnosť chrániť informáciu, systémy a siete organizácie systematicky a (zákony a vykonávacie predpisy) výslovne uvádzajú množstvo konkrétnych požiadaviek, ktoré musia správcovia týchto systémov splniť.

Zákonné požiadavky na KIB vychádzajú z rokmi vyvíjaných medzinárodných štandardov a ich naplnenie si vyžaduje znalosti KIB, poznanie pomerov v organizácii, zdroje a podporu vedenia. Úzkym miestom je najmä nedostatok odborníkov na KIB a nedostatočná podpora KIB v organizácii, pretože ak by aj organizácia bola schopná zaplatiť externých špecialistov, tí bez spolupráce s pracovníkmi organizácie nebudú schopní preniknúť do pomerov v organizácii a navrhnúť systém účinných a pre organizáciu prijateľných riešení. Navyše, KIB nie je jednorazová záležitosť, lebo niektoré z navrhovaných riešení (právne, organizačné, vzdelávacie) majú trvalý charakter a aj ďalšie (napr. technické) riešenia je potrebné v organizácii nielen navrhnúť, ale aj zaviesť, udržiavať, monitorovať ich účinnosť a podľa potreby meniť, t.j. zavedenie, udržiavanie a rozvoj KIB v organizácii je proces (nazývaný **bezpečnostný proces**), ktorý prebieha počas celej existencie organizácie.[4]

[3] postavených na d-IKT
[4] a "upratovanie" aj po jej zániku

Tento dokument je určený vedúcim pracovníkom organizácií, ktoré sú správcami ISVS, spadajúcich podľa vyhlášky č. 179/2020 do II. a III. kategórie a stručne popisuje, ako naplniť legislatívne požiadavky a zaistiť v organizácii potrebnú úroveň kybernetickej a informačnej bezpečnosti.

Terminologická poznámka. Informačná bezpečnosť (ako oblasť ľudskej činnosti) sa zaoberá hrozbami voči informácii a hľadaním účinných opatrení na zníženie rizika z naplnenia týchto hrozieb. Kybernetická bezpečnosť nemá zatiaľ všeobecne akceptovanú jednotnú definíciu, ale chápe sa ako informačná bezpečnosť kybernetického priestoru (t.j. systémov a sietí). Pre organizáciu je podstatné plnenie jej poslania, t.j. vykonávanie činností potrebných na plneniu účelu, kvôli ktorému bola vytvorená. Informácia je podstatným zdrojom, bez ktorého organizácia nemôže plniť svoje poslanie. Väčšina informácií sa v súčasnosti spracováva pomocou digitálnych IKT a komunikácia organizácie so štátnymi inštitúciami, klientmi prebieha v čoraz väčšej miere elektronicky, pomocou d-IKT. Aby sme zaistili ochranu informácie bez ohľadu na formu, v ktorej sa vyskytuje a mohli využívať dlhoročne budované know-how informačnej bezpečnosti, nebudeme riešiť terminologické rozpory a budeme používať pojem kybernetická a informačná bezpečnosť, na označenie oblasti riešiacej ochranu informácie, s dôrazom na informáciu spracovávanú pomocou d-IKT.

2 Povinnosti správcu ISVS v KIB

Požiadavky na bezpečnosť informačných technológií verejnej správy definuje zákon o ITVS [3] a detailne špecifikuje vykonávací predpis [4]. Špecifickým prípadom informačnej technológie verejnej správy je informačný systém verejnej správy (ISVS), definovaný v §2 zákona o ITVS, pretože správa ISVS je podľa zákona o KB základnou službou[5] a povinnosti prevádzkovateľov základných služieb v KB upravuje zákon o KB.
Za ISVS podľa zákona o ITVS [3] zodpovedá jeho správca. Správcu informačnej technológie verejnej správy definuje §2 ods. 5 zákona o ITVS [3], podrobnejší zoznam a kategorizácia ITVS sú uvedené vo vyhláške [4].
Na správcu ISVS sa teda vzťahujú požiadavky dvoch rozličných zákonov [1][3]. Povinnosti správcu ISVS ako prevádzkovateľa základnej služby definuje Zákon o KB [1] a konkretizuje vyhláška [2], povinnosti správcu ISVS ako správcu ITVS stanovuje zákon [3] kategorizáciu ITVS a bezpečnostné opatrenia na zaistenie ich ochrany stanovuje vyhláška [4]
Požiadavky zákonov [1][3] a vyhlášok [2][4] sa teda vzťahujú na ISVS a jeho správcu. Našťastie majú veľký spoločný prienik, počet obsahovo rozdielnych požiadaviek je relatívne malý, väčšinou sa dajú zosúladiť a pár problematických požiadaviek je potrebné (aj možné) riešiť individuálne.
Jednotné riešenie KIB pre ISVS sa zakladá na § 19, ods. (1) Zákona o ITVS [3], ktorý obsahuje požiadavku na správcu ISVS zaviesť a udržiavať v organizácii **systém riadenia informačnej bezpečnosti**[6], ktorý sa podľa § 21, ods. (3), písm. b) bod 2. **vzťahuje na všetky informačné systémy, ktoré sú v jej správe**.
Zavedením štandardného systému riadenia informačnej bezpečnosti (a doplnením niektorých špecifických opatrení definovaných vo vyhláškach [2][4]) správca splní povinnosti uložené zákonmi [1][3] a vytvorí/získa riešenie, ktoré je podporované početnými normami, pokrýva aj iné požiadavky na ochranu údajov (napr. osobných), je rozšíriteľné o opatrenia, ktoré vyplynú z nových požiadaviek v budúcnosti a je kompatibilné aj v medzinárodnom meradle.

[5] správa konkrétneho ISVS musí byť ešte uvedená v zozname základných služieb
[6] ide o široko používaný technický termín (anglický názov je Information security management system, ISMS), ktorý nebudeme upravovať rozširovaním o pojem kybernetickej bezpečnosti; po vecnej stránke však ISMS pokrýva rovnako oblasť inforrmačnej ako aj kyberntickej bezpečnosti

3 Systém riadenia informačnej bezpečnosti organizácie

Najprv ukážeme problém (dlhodobého zaistenia potrebnej úrovne KIB) a jeho riešenie na abstraktnejšej úrovni, potom sa jeho riešením budeme zaoberať konkrétnejšie. Ciele organizácie v KIB možno sformulovať nasledovne – organizácia požaduje

a) aby mala vždy k dispozícii zaistiť potrebnú informáciu a mohla sa na jej hodnovernosť spoľahnúť,
b) aby informačné systémy a siete organizácie spoľahlivo fungovali,
c) aby preukázateľne plnila všetky právne požiadavky na spracovanie a ochranu údajov,
d) aby náklady na plnenie požiadaviek a) - c) neboli príliš vysoké/boli čo najnižšie.

Tieto prirodzené, ale veľmi všeobecné požiadavky musí vedenie organizácie konkretizovať do podoby cieľov, zohľadňujúcich poslanie organizácie, jej povinnosti a podmienky, v ktorých pôsobí, na čo a ako využíva digitálne IKT, akú informáciu pomocou nich spracováva, aké sú výstupy jej činnosti a pod. Výsledkom je Stratégia informačnej a kybernetickej bezpečnosti, ktorá slúži na orientáciu pri plánovaní aktivít zameraných na dosiahnutie stanovených cieľov.

Stratégia je konkrétnejšie rozpracovaná v Politike kybernetickej a informačnej bezpečnosti a implementovaná pomocou

a) organizácie KIB (pravidlá, procesy, organizačné štruktúry),
b) bezpečnostných projektov (analyzujúcich bezpečnostné problémy, navrhujúcich a implementujúcich ich riešenia).

Zaistenie trvalo udržateľnej, ekonomicky zvládnuteľnej a potrebám organizácie primeranej úrovne KIB je zložitý manažérsky problém, ktorého riešením je systém riadenia informačnej bezpečnosti, ISMS

3.1 Čo vlastne je systém riadenia informačnej bezpečnosti?

Systém manažmentu/riadenia informačnej bezpečnosti (Information security management system, ISMS) je tá súčasť systému riadenia (manažmentu) organizácie, ktorá sa zaoberá informačnou bezpečnosťou. ISMS špecifikuje nástroje a metódy (plánovanie, prijatie, implementácia, kontrola, revízie, korekcie a vylepšenia) ktoré by manažéri mali používať pri riešení úloh a riadení aktivít zameraných na dosiahnutie informačnej bezpečnosti. [8]

ISMS pozostáva zo štyroch podstatných zložiek:

a) princípov riadenia (informačnej bezpečnosti)
b) zdrojov, ktoré sú na zaistenie a udržiavanie informačnej bezpečnosti potrebné
c) ľudí, ktorí pracujú s informáciami, systémami a sieťami a plnia buď špeciálne úlohy v informačnej bezpečnosti, alebo zohľadňujú informačnú bezpečnosť pri plnení svojich pracovných úloh,
d) bezpečnostného procesu (správa rizík)

ISMS je popísané detailne v medzinárodných normách ISO/IEC [5][6], z ktorých do značnej miery vychádzali aj oba zákony [1][3] a vyhlášky [2][4].

Problém je, že 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[7]“ ISO normy [5] je uvedený v nemeckom štandarde [8] a IT kompendiu Grundschutz [10], z ktorých budeme vychádzať.

Iniciatíva na zavedenie ISMS musí vychádzať zhora, rozhodnutie o zavedení ISMS musí prijať vedenie organizácie a podniknúť aj prvé kroky na spustenie celého bezpečnostného procesu (t.j. systematického riešenia KIB v organizácii). To je prirodzená požiadavka, lebo vedenie zodpovedá na chod organizácie a aby nedošlo k narušeniu kritickej informačnej infraštruktúry organizácie, je potrebné primeraným spôsobom zakomponovať KIB do činnosti organizácie. A to bez podpory a výraznej angažovanosti vedenia organizácie nie je možné.

Skôr, ako sa pozrieme na nevyhnutné kroky pre zavedenie IS uvedieme ešte jednu terminologickú poznámku. Nutnú podmienku, bez splnenia ktorej nie je možné dosiahnuť stanovený cieľ, budeme vyjadrovať slovom **MUSÍ** (angl. MUST). Spojenie **MAL BY** (angl. SHOULD) vyjadruje odporúčanie.

[7] organizácia, ktorá zaviedla ISMS, si ho môže dať certifikovať podľa normy ISO/IEC 27001

Teraz uvedieme postupnosť krokov podľa [8][9][10] na zavedenie ISMS v organizácii a v komentároch stručne vysvetlíme jednotlivé kroky, spôsob ich realizácie a korešpondenciu s požiadavkami uvedenými v zákonoch [1][3] a vyhláškach [2][4]. Kroky uvádzame v časovej postupnosti, v akej sa majú vykonávať.
Požiadavky zákonov, vyhlášok a noriem pravdepodobne nebude možné splniť okamžite a v plnom rozsahu. Zavedenie základných opatrení môže výrazne zvýšiť úroveň KIB v organizácii a systematický prístup podľa [8][9][10] k riešeniu KIB umožňuje základné opatrenia postupne dopĺňať a zvyšovať tak úroveň KIB v organizácii. Budeme rozlišovať dve úrovne opatrení smerujúcich k vytvoreniu ISMS – základnú a štandardnú. Kroky/opatrenia základnej úrovne je potrebné vykonať v každom prípade, ďalšie kroky môže organizácia vykonať, keď dosiahne základnú úroveň KIB a bude chcieť KIB pozdvihnúť na kvalitatívne vyššiu úroveň.

3.2 Základné kroky/opatrenia

V tejto časti uvádzame opatrenia, ktoré je podľa štandardov [8][9] a Kompendia [10] potrebné spraviť na zavedenie systematického dlhodobého riešenia KIB v organizácii na základnej úrovni. V rámčeku sú uvedené úlohy, ktoré je potrebné splniť na naplnenie základného opatrenia a kto by tieto úlohy mal riešiť. Tieto úlohy sú prebraté z Kompendia [10] a keď sa na ne budeme odvolávať, budeme o nich hovoriť ako o požiadavkách Štandardu.

3.2.1 Prijatie celkovej zodpovednosti za KIB vedením organizácie[8]

1) Vedenie organizácie MUSÍ prijať celkovú zodpovednosť za kybernetickú a informačnú bezpečnosť v organizácii a to takým spôsobom, aby to bolo jasné všetkým zainteresovaným stranám,
2) Vedenie organizácie MUSÍ iniciovať, riadiť a monitorovať bezpečnostný proces
3) Vedenie organizácie MUSÍ byť dobrým príkladom pri dodržiavaní požiadaviek (neskôr opatrení) KIB
4) Vedenie organizácie MUSÍ vymenovať zamestnancov zodpovedných za KIB, poskytnúť im potrebné oprávnenia a zdroje
5) Vedenie organizácie MUSÍ pravidelne dostávať informácie o stave KIB v organizácii, najmä informácie o stave KIB v organizácii, možných rizikách vyplývajúcich z chýbajúcich alebo nedostatočných bezpečnostných opatrení

Komentár

1) Keďže vedenie organizácie zodpovedá najmä za to za to, že organizácia plní úlohy, pre ktoré bola vytvorená a organizácia pri plnení úloh používa ISVS, vedenie organizácie zodpovedá aj za to, že ich ISVS bude spoľahlivo fungovať. Vedenie by si malo ujasniť, ako bude koncepčne riešiť KIB v organizácii (Stratégia KIB), zverejniť ciele, metódy a dať verejne na vedomie odhodlanie napĺňať ciele stanovené v Stratégii. Táto požiadavka Štandardu sa naplní buď vyhlásením vedenia v úvode Politiky KIB alebo samostatnom deklaratívnom dokumente Bezpečnostný zámer. Zmyslom výslovného prihlásenia sa vedenia organizácie k zodpovednosti za kybernetickú a informačnú bezpečnosť je upozornenie zainteresovaných, že vedenie organizácie hodlá uplatniť svoju autoritu a využiť zdroje organizácie na to, aby v organizácii dosiahla potrebnú úroveň KIB.
2) Bezpečnostný proces v organizácii nemôže spustiť nikto iný ako vedenie, pretože nemá dostatočnú autoritu, aby presadil plnenie potrebných opatrení a spoluprácu zamestnancov organizácie, resp. externých spolupracovníkov a zmluvných partnerov. Vedenie organizácie nemá čas ani vedomosti na to, aby sa detailne zaoberalo KIB, potrebuje zadať úlohy, kontrolovať ich plnenie a na základe pripravených podkladov rozhodovať v kľúčových otázkach KIB. Takýto stav organizácia dosiahne vytvorením organizačnej štruktúry pre KIB, definovaním bezpečnostných rôl

[8] rozumie sa najvyššie vedenie organizácie

a zaradením pracovníkov do týchto rôl. Podrobnejšie budú tieto kroky vedenia organizácie rozpísané v ďalších opatreniach.

3) Bezpečnostné opatrenia zasahujú často do pohodlia používateľov informačných systémov organizácie. Ak by tieto opatrenia samotné vedenie nedodržiavalo, sotva by mohlo očakávať, že ich budú dodržiavať zamestnanci organizácie. (To je síce podmienka nutná, ale nie postačujúca).
4) Na zaistenie KIB v organizácii bude potrebné vykonávať rôzne činnosti, ktoré sa dosiaľ nevykonávali systematicky, alebo vôbec. (Základné sú známe ihneď, ďalšie sa objavia, keď sa organizácia začne zaoberať KIB detailnejšie.) Organizácia spravujúca ISVS II. alebo II. kategórie má v KIB toľko povinností, že na ich plnenie bude potrebovať niekoľko ľudí, ktorí sa budú KIB zaoberať profesionálne, aspoň na čiastočný úväzok. Minimum je manažér KIB a garant KIB, t.j. člen vedenia organizácie, ktorý zodpovedá za KIB a spolupracuje s hlavným[9] manažérom KIB. Vedenie bude musieť rozhodnúť, čo organizácia potrebuje, na čo má dostatočné zdroje a podľa toho prijímať nových ľudí a/alebo rozširovať pracovnú náplň existujúcim zamestnancom.
5) Keď bude ustanovený hlavný manažér KIB v organizácii, jeho povinnosťou bude o.i. aj vypracovávať výročné správy o stave KIB v organizácii, plány práce a na podnet vedenia organizácie aj správy o čiastkových bezpečnostných problémoch a ich riešení.

3.2.2 Definovanie bezpečnostných cieľov a stratégie

1) aby vedenie organizácie mohlo spustiť bezpečnostný proces v organizácii, MUSÍ špecifikovať a zdokumentovať bezpečnostné ciele (security objectives) a stanoviť stratégiu KIB
2) vedenie organizácie MUSÍ zabezpečiť ohodnotenie bezpečnostných požiadaviek na jednotlivé činnosti (business processes) a MUSÍ vytvoriť všeobecné organizačné podmienky na to, aby sa umožnilo správne a bezpečné nakladanie s informáciou vo všetkých činnostiach (business processes) organizácie
3) vedenie organizácie MUSÍ podporovať a prevziať zodpovednosť za bezpečnostnú stratégiu a bezpečnostné ciele
4) bezpečnostná stratégia a bezpečnostné ciele sa MUSIA pravidelne revidovať, aby sa zaistilo, že sú stále aktuálne a že sa dajú efektívne implementovať.

Komentár

1) Vedenie organizácie musí stanoviť všeobecné ciele KIB. Všeobecné ciele KIB sú odvodené od poslania organizácie, prostredia a podmienok, v ktorých organizácia pôsobí. Všeobecné ciele KIB sú základom, z ktorého sa budú odvodzovať bezpečnostné požiadavky na spracovanie informácie, IT operácie neskôr, keď budú vytvorené organizačné podmienky KIB a organizácia bude pracovať na bezpečnostnom projekte. Možné všeobecné bezpečnostné ciele organizácie sú napríklad [9]
    a) vysoká spoľahlivosť činností, zvlášť spracovania informácií (dostupnosť, integrita, dôvernosť)
    b) zaistenie dobrej reputácie organizácie v očiach verejnosti,
    c) ochrana vysokej a potenciálne nenahraditeľnej hodnoty spracovávanej informácie
    d) splnenie požiadaviek vyplývajúcich zo zákonov, štandardov a vnútornej legislatívy organizácie,
    e) ochrana fyzických osôb (zdravie, osobné údaje)
    f) iné

Aby z týchto všeobecných cieľov bolo možné odvodiť konkrétnejšie bezpečnostné ciele, bude potrebné zistiť, ktoré činnosti organizácie (business processes), sú kľúčové pre napĺňania poslania organizácie (bez ktorých to organizácia

[9] organizácia môže mať viacero manažérov KIB, ale jeden musí byť hlavný a riadiť tých ostatných

nedokáže robiť), aké informácie sa pri tom používajú a aké sú požiadavky na ochranu dôvernosti, integrity a dostupnosti informácií. V tejto fáze sa nevyžaduje detailná analýza, ale len stanovenie, čo je pre organizáciu obzvlášť dôležité a prečo.

V Stratégii KIB sa na vysokej úrovni popíše poslanie organizácie, význam KIB pre plnenie poslania, všeobecné bezpečnostné ciele, ktoré z poslania vyplývajú, aktuálny a cieľový stav a spôsob, akým chce vedenie organizácie stanovené ciele naplniť.

2) V tejto fáze (ešte pred analýzou rizík) je potrebné identifikovať/odhadnúť bezpečnostné požiadavky na činnosti, ktoré organizácia vykonáva. Tie sú odvodené od bezpečnostných požiadaviek na informácie, ktoré sa pri činnostiach spracovávajú (dôvernosť, integrita, dostupnosť) a vyjadrené na škále nízka, stredná a vysoká úroveň. Organizácia by mala byť schopná odpovedať na nasledujúce otázky:
    a) ktoré informácie sú pre organizáciu kritické z hľadiska dôvernosti, integrity a dostupnosti?
    b) ktoré kritické činnosti organizácia nedokáže bez podpory d-IKT vykonávať vôbec, vykonávať len vo veľmi redukovanom rozsahu (na veľmi nízkej úrovni) alebo s veľkými dodatočnými nákladmi?
    c) aké efekty môžu mať neúmyselne alebo úmyselne vyvolané bezpečnostné problémy?
    d) používajú sa d-IT na spracovanie informácie, ktorá má špecifické požiadavky na ochranu napr. z hľadiska dôvernosti (utajované skutočnosti, citlivá informácia)?
    e) ktoré podstatné rozhodnutia, ktoré organizácia prijíma, závisia od dôvernosti, integrity, dostupnosti informácie a informačných systémov?
    f) z ktorých právnych požiadaviek, interných predpisov vyplývajú požiadavky na konkrétne bezpečnostné opatrenia?

Organizácia upraví existujúce postupy tak, aby zaistila dodržiavanie elementárnych požiadaviek na ochranu informácie, systémov a sietí. (Častokrát pôjde len o dôsledné dodržiavanie existujúcich pravidiel pre správu systémov, prácu koncových používateľov a narábanie s informáciami).

3) Stratégia KIB bude schválená vedením organizácie a na jej základe vytvorená a vedením organizácie schválená Politika KIB, ktorá bude obsahovať aj vyhlásenie vedenia organizácie o význame KIB pre organizáciu a záväzok vedenia organizácie podporovať zaistenie a udržiavanie potrebnej úrovne KIB v organizácii.
4) Bezpečnostné ciele organizácie sú sformulované v dvoch dokumentoch Stratégia KIVB a Politika KIB. Stratégia KIB, Politika KIB (aj ďalšie dokumenty tvoriace bezpečnostnú dokumentáciu organizácie) majú svojich vlastníkov a definované pravidlá pre správu (pravidelné revízie a revízie v prípade mimoriadnych udalostí); revízie sa v prípade potreby (cieľ bol dosiahnutý alebo už nie je aktuálny) môžu týkať aj cieľov a iných koncepčných otázok KIB organizácie, návrhy na zmeny prerokováva a schvaľuje vedenie organizácie.

3.2.3 Napísanie a vydanie Politiky kybernetickej a informačnej bezpečnosti

1) vedenie organizácie MUSÍ zabezpečiť vypracovanie vysokoúrovňovej politiky KIB, ktorá
   a) opíše význam KIB pre organizáciu
   b) bezpečnostné ciele
   c) najdôležitejšie aspekty stratégie KIB
   d) organizačnú štruktúru KIB
2) v politike KIB MUSÍ byť jasne definovaný rozsah jej pôsobnosti a
   a) MUSIA byť vysvetlené bezpečnostné ciele a ako súvisia s poslaním, úlohami a cieľmi organizácie
   b) Politika KIB MUSÍ byť dostupná všetkým zamestnancom organizácie, externým spolupracovníkom a iným ľuďom, ktorí sa podľa nej majú riadiť
3) Politika KIB BY MALA BYŤ pravidelne aktualizovaná

Komentár

1) Organizácia potrebuje okrem koncepčne postavenej Stratégie KIB aj základný dokument pre praktické použitie. Tým je v chápaní noriem Bezpečnostná politika (plný názov Politika informačnej bezpečnosti). Okrem základných ustanovení je jej obsah v normách stanovený len veľmi voľne. Na druhej strane je Bezpečnostná politika čosi ako ústava, ktorá má byť doplnená zákonmi upravujúcimi detailnejšie konkrétne oblasti. Bezpečnostná politika je vrcholom trojúrovňovej hierarchickej štruktúry bezpečnostnej dokumentácie, je rozpracovaná v špeciálnych bezpečnostných politikách a tie sú ešte na tretej úrovni detailne rozpracované v podobe bezpečnostných praktík. (Súčasťou povinnej bezpečnostnej dokumentácie organizácie sú aj iné dokumenty, ktorými sa teraz nebudeme zaoberať).Štandardy BSI, normy ISO a vyhlášky [2][4] sa v obsahu a chápaní Politiky KIB dosť výrazne líšia. Štandardy BSI chápu Politiku KIB (Bezpečnostnú politiku) ako pomerne všeobecný (vysokoúrovňový) dokument, ktorého hlavnou úlohou je prezentovať verejnosti ciele a prístup vedenia ku KIB, ktorý je sformulovaný v zrejme neverejnej Stratégii. ISO normy sú konkrétnejšie a rozširujú povinný obsah Politiky KIB. Vyhláška [2] za hlavný koncepčný dokument KIB považuje Bezpečnostnú stratégiu kybernetickej bezpečnosti, ale definuje jej obsah a a spôsob použitia tak, že zodpovedá skôr štandardnej Politike KIB ako Stratégii KIB. Bezpečnostnú politiku (Bezpečnostná politika kybernetickej bezpečnosti) chápe ako súbor deviatich čiastkových bezpečnostných politík (Príloha 1B) zodpovedajúci štandardným bezpečnostným politikám 2. úrovne. Keďže podľa § 3 ods. (2) je možné Bezpečnostnú stratégiu kybernetickej bezpečnosti vydať *aj ako jednu z bezpečnostných politík kybernetickej bezpečnosti*, dá sa vytvoriť hierarchicky usporiadaný systém bezpečnostnej dokumentácie, ktorý bude spĺňať aj požiadavky vyhlášky [2]. Vyhláška [4] nemení hierarchiu bezpečnostných politík, ale podstatne rozširuje obsah Politiky KIB Príloha 2, časť A, Kategória II. písm. a), bod 2 tým že požaduje aby Politika KIB *obsahovala najmenej... základné zásady a opatrenia kybernetickej a informačnej bezpečnosti v štruktúre oblastí definovaných touto vyhláškou.* Taktiež požaduje vypracovanie interných riadiacich aktov pre vybrané oblasti KIB, čo zodpovedá vypracovaniu bezpečnostných politík 2. úrovne.
   Implementácia Vytvoriť hierarchický systém bezpečnostných politík (Stratégia KIB, Politika KIB, špeciálna politika KIB pre oblasť xxx, perspektívne bezpečnostné praktiky) Politiku KIB upraviť obsahovo tak, aby spĺňala požiadavky noriem, vyhlášky [2] na Bezpečnostnú stratégiu kybernetickej bezpečnosti a požiadavky vyhlášky [4]. Postupne vypracovať špeciálne politiky (Bezpečnostné politiky 2. úrovne) pre tie oblasti, kde je potrebné všeobecné opatrenia bližšie špecifikovať.
   Poznámka. Politike KIB je venovaný samostatný materiál (Politika KIB)
2) Čiastočne sme vysvetlili v predchádzajúcej časti. Politika KIB je verejný materiál, ktorý je určený osobám pristupujúcim k informáciám, sieťam a systémom organizácie. Rámcovo im vysvetľuje, aké sú ciele organizácie v

KIB, ako ich organizácia hodlá dosiahnuť a že sú povinní dodržiavať pri práci isté pravidlá, s ktorými budú podrobnejšie oboznámení. Nemá zmysel ísť do veľkých detailov, ktorým väčšina ľudí nebude rozumieť, ale vzhľadom na požiadavku vyhlášky [4] bude Politika KIB pomerne rozsiahla.

3) Správcom Politiky KIB je manažér KIB a jeho úlohou budú jednak pravidelné revízie Politiky KIB (v ročných intervaloch) a mimoriadne revízie ak dôjde ku zmenám, ktoré si vyžiadajú aj zmenu Politiky KIB. Manažér KIB predloží navrhované zmeny Politiky KIB vedeniu organizácie pri výročnom hodnotení stavu KIB, alebo v správe o závažnej bezpečnostne relevantnej udalosti (organizačná zmena v organizácii, závažný bezpečnostný incident, novelizácia zákona a pod.) Správa Politiky KIB je rozobratá v dokumente Politika KIB

3.2.4 Vymenovanie manažéra KIB

1) vedenie organizácie MUSÍ vymenovať manažéra KIB organizácie
2) manažér KIB organizácie
   a) presadzuje KIB v organizácii, riadi a koordinuje bezpečnostný proces
   b) MUSÍ mať primeranú kvalifikáciu a musí mať dostatočné podmienky na jej zvyšovanie
   c) MUSÍ mať k dispozícii dostatočné zdroje
   d) v prípade potreby MUSÍ mať možnosť podávať správy/hlásenia priamo vedeniu organizácie
   e) MUSÍ byť zapojený v počiatočnej fáze rozsiahlych projektov, ako napr. zavedenia novej aplikácie alebo IT systému
3) ak na funkciu manažéra KIB organizácia nemá vhodného vlastného zamestnanca, organizácia MUSÍ nájsť a vedenie organizácie vymenovať externého manažéra KIB
4) externý manažér KIB MUSÍ mať na túto funkciu potrebnú kvalifikáciu
5) zmluva s externým manažérom MUSÍ
   a) pokrývať všetky úlohy, ktoré má manažér KIB; zároveň aj s nimi spojené práva a povinnosti
   b) obsahovať záväzok o zachovaní mlčanlivosti
   c) zaistiť riadený postup pri ukončení zmluvného vzťahu, vrátane odovzdanie úloh

Komentár

1) Vedenie organizácie zodpovedá (okrem iného) za KIB organizácie. Definuje ciele, bude rozhodovať v koncepčných otázkach, ale niekto mu musí pripravovať odborné podklady a zabezpečovať realizáciu prijatých rozhodnutí (a plniť množstvo ďalších povinností). Týmto človekom je manažér KIB. Organizácia môže mať viacero manažérov KIB, v tomto prípade je jeden z nich hlavný a riadi ostatných manažérov. Keď budeme hovoriť o manažérovi KIB, máme na mysli hlavného manažéra KIB v organizácii.
2) Štandardy a ešte vo väčšej miere vyhlášky [2][4] kladú na manažéra KIB (obsahovo oprávnené) požiadavky, ktoré však výrazne prevyšujú možnosti jedného človeka. Na pozíciu manažéra KIB bude preto potrebné vymenovať človeka, ktorý potrebné veci dokáže skôr zorganizovať, ako ich sám spraviť.
   a) riadenie a koordinácia bezpečnostného procesu vystihuje všetko podstatné – poznať organizáciu a jej bezpečnostné potreby, zdroje, ktoré má k dispozícii, vedieť pripraviť návrh postupu, presvedčiť vedenie organizácie, aby sa s ním (po stanovení priorít a ďalších úpravách) stotožnilo a podporovalo ho; vypracovať projekty na riešenie čiastkových problémov, získať na ne zdroje, zapojiť ľudí do riešenia, koordinovať ich súčinnosť, atď.
   b) Problém je v odborných požiadavkách kladených na manažéra KIB ktoré budú sotva spĺňať vlastní zamestnanci organizácie a nedostatku prostriedkov na zaplatenie externého špecialistu. (Špecialistov na KIB je málo a sú mimoriadne dobre ohodnotení v súkromnej sfére). Riešením bude poverenie vlastného zamestnanca a to buď informatika, alebo právnika s organizačnými a komunikačnými schopnosťami, znalosťou organizácie a ochotou

učiť sa. Obaja, právnik aj informatik budú potrebovať podporu personálneho, právneho oddelenia, informatiky, správy budov a určite aj externých špecialistov.

c) Na reálne plnenie úloh bude potrebovať manažér KIB dostatočné právomoci a zdroje – najmä ľudí a peniaze. Niektoré bezpečnostne relevantné činnosti v organizácii môžu vykonávať existujúci zamestnanci organizácie, ak sa im – rozšíri pracovná náplň, budú na nové úlohy patrične vyškolení, budú mať na ich plnenie potrebné podmienky a za prácu naviac budú finančne motivovaní. Niektoré činnosti si budú vyžadovať vytvorenie a obsadenie nových pozícií, jednorazové úlohy využitie externých špecialistov.

d) Manažér KIB bude priamo komunikovať s garantom KIB (členom vedenia organizácie, zodpovedným za KIB). Pri spustení bezpečnostného procesu v organizácii, bude potrebné vo vedení organizácie prerokovať niekoľko základných dokumentov (Stratégia KIB, Politika KIB, možno špeciálne politiky KIB), neskôr to raz do roka bude správa o stave KIB a plány práce na ďalší rok (vrátane rozpočtu na KIB na ďalší rok). Okrem výročnej správy by vedenie malo byť informované o závažných bezpečnostných incidentoch, výsledkoch auditov, analýz rizík, zmenách, ktoré majú veľký dopad na KIB organizácie a vyžadujú si pozornosť vedenia.

e) aby sa KIB neriešila ex-post, čo môže byť drahé a menej účinné, manažér KIB bude zapojený do prípravy nových projektov, kde bude jeho úlohou najmä posúdiť bezpečnostné riziká, sformulovať bezpečnostné požiadavky na ich ošetrenie ešte vo fáze návrhu a skontrolovať, či ich výsledné riešenie spĺňa. a za akých podmienok

3) Organizácia potrebuje manažéra KIB a keď nenájde vhodného interného zamestnanca, ktorý sa dovzdeláva a bude schopný túto funkciu kvalifikovane zastávať, musí nájsť vhodného kandidáta v externom prostredí. (Takýto externý špecialista bude potrebovať spolupracovať s ľuďmi z organizácie, možno mu prideliť zamestnanca organizácie, ktorý mu bude pomáhať a pripraví sa na funkciu manažéra KIB)
4) toto je prirodzená požiadavka, od externého manažéra KIB organizácia očakáva prinesenie know-how, ktoré v organizácii nie je. Problém môže byť v tom, že
   - skutočných špecialistov na KIB nie je veľa
   - sú drahí
5) Povinnosti manažéra KIB bude v prípade externistu presne sformulovať (čo a v akom rozsahu bude od neho požadovať) a za akých podmienok. Oproti internému manažérovi KIB, ktorý má tieto povinnosti upravené v štandardnej pracovnej zmluve – doplniť povinnosť zachovať mlčanlivosť (o čom a ako dlho po ukončení pracovného pomeru) a postup pri ukončení pracovného pomeru, pretože niekto bude musieť v práci manažéra KIB pokračovať a prebrať od neho najmä rozpracované úlohy.

Poznámka. Vyhlášky (implicitne aj explicitne) obsahujú množstvo povinností, ktoré by mal manažér KIB plniť. Rozsah úloh prevyšuje časové kapacity jedného človeka a ak sa nestanovia priority a do riešenia najdôležitejších úloh nezapoja aj ďalší ľudia, tak bude manažér KIB písať politiky, metodické materiály, správy, organizovať školenia, ale nebude mať čas pracovať na KIB organizácie a po prvom závažnom bezpečnostnom incidente bude odvolaný pre neschopnosť. Tým sa však stav KIB v organizácii nijako nezlepší.

3.2.5 Vytvorenie vhodnej organizačnej štruktúry pre KIB

1) v organizácii sa MUSÍ vytvoriť vhodná organizačná štruktúra pre KIB
2) MUSIA byť definované bezpečnostné roly
3) do týchto rôl MUSIA byť zaradení kvalifikovaní ľudia s dostatočnými zdrojmi potrebnými na vykonávanie povinností vyplývajúcich z týchto rôl
4) transparentným spôsobom MUSIA byť definované a pridelené/prideľované kompetencie, zodpovednosti a úlohy v manažmente KIB
5) pre všetky dôležité funkcie v manažmente KIB MUSIA byť definovaní náhradníci a systém zastupovania
6) MUSIA byť naplánované, popísané, vytvorené a oznámené komunikačné kanály
7) pre všetky úlohy a bezpečnostné roly MUSÍ byť stanovené kto koho informuje, kto a o akých akciách má byť informovaný a rozsah informácie, ktorú mu je potrebné poskytnúť

1) aby mal úlohy v KIB aj kto plniť, je potrebné v organizácii jasne stanoviť, kto za čo zodpovedá a komu
2) väčšina ľudí plní v KIB podobné, dlhodobé úlohy, ktoré vyplývajú z ich pracovného zaradenia. Preto má zmysel zaviesť bezpečnostné roly (vedúci pracovník, informatik, manažér KIB, informatik, koncový používateľ, technický správca systému) definovať oprávnenia a povinnosti viažúce sa na konkrétne roly a zaraďovať ľudí do bezpečnostných rôl. Je to podstatne jednoduchšie a prehľadnejšie, ako stanovovať povinnosti pre každého človeka jednotlivo a kontrolovať ich dodržiavanie. (Ďalšie úlohy možno zadávať nad rámec povinností definovaných v rolách; ak sa ukáže, že by to bolo užitočné, možno upraviť obsah bezpečnostnej roly, alebo vytvoriť novú bezpečnostnú rolu).
3) ak sa jedná o špecifické bezpečnostné roly, od ktorých podstatne závisí KIB organizácie, ľudia, ktorí sú do nich zaradení, musia vedieť, čo majú robiť a musia mať vytvorené podmienky na to, aby to mohli aj skutočne robiť.
4) zaradenie do roly nie je statické, ale môže sa meniť v súvislosti so zmenami postavenia človeka v organizácii, ale aj podmienok v organizácii (prístupové práva k novému systému). Organizácia musí mať stanovené pravidlá pre správu rôl: kto rozhoduje o zadelení človeka do roly, kto mu nastaví príslušné oprávnenia v systémoch, čo sa stane, ak je človeka zaradiť doďalšiej roly, ktorej kompetencie sú v konflikte záujmov s jeho predchádzajúcimi; čo robiť pri zmene pracovného zaradenia, ukončení pracovného pomeru a pod. Takisto v prípade mimoriadnych úloh (vypracovania koncepčných materiálov, riešenia bezpečnostných incidentov) musí byť jasná úloha, ktorú má človek plniť, aby sa on aj jeho kolegovia vedeli zorientovať a skoordinovať.
5) problémy nezaniknú dočasným výpadkom človeka, ktorý ich mal riešiť, ani nepočkajú, kým sa vráti. Pre kľúčové pozície musí byť definovaný náhradník, ktorý okamžite preberie povinnosti svojho neprítomného kolegu a potom po jeho príchode mu odovzdá agendu. V opačnom prípade by sa mohlo stať, že v neprítomnosti zodpovedného človeka vznikne problém, ktorý si ostatní všimnú až vtedy, keď narastie do nepriehľadnuteľného rozsahu a jeho riešenie si vyžiada podstatne väčšie úsilie a viac prostriedkov, ako keby ho zastupujúci pracovník odhalil a riešil v zárodku.
6) a súčasne 7) všetky zúčastnené strany musia byť včas informované o rozličných aktivitách, ktoré v rámci manažmentu KIB prebiehajú, aby vedeli primerane reagovať. To znamená, že pre všetky aktivity KIB, začínajúc najdôležitejšími, organizácia (manažér KIB) musí identifikovať účastníkov aktivity, zistiť, aké informácie kto kedy komu má poslať a dohodnúť spôsob (webová stránka pri oznámeniach, e-mali, telefonát,...) a oboznámiť zúčastnených, ako má komunikácia prebiehať Interná komunikácia je na organizácii, ako si ju nastaví, ale okrem toho komunikuje aj s tretími stranami, kde je obsah a spôsob komunikácie daný zákonom, alebo ho treba

nastaviť zmluvne. aby organizácia splnila podmienky zákona, zákon o KB [1] §19 ods. (4), ods. (6), písm. b). ods. (7), § 20, ods. (4), písm. e). § 24.

3.2.6 Definovanie bezpečnostných opatrení

1) Pre všetky aspekty spracovania informácie MUSIA byť definované primerané bezpečnostné opatrenia
2) všetky bezpečnostné opatrenia musia byť systematicky dokumentované v bezpečnostných projektoch a v pravidelných intervaloch revidované

Komentár

1) Aby v ochrane informácie, systémov a sietí organizácia neboli diery, je potrebné zistiť, čo treba chrániť (aktíva), pred čím (hrozby) , na akej úrovni a ako (opatrenia). Na tieto otázky dáva odpoveď bezpečnostný projekt, ktorého kľúčovou časťou je analýza rizík. V organizácii bude potrebné spraviť analýzu rizík, vyhodnotiť riziká a navrhnúť opatrenia. Bezpečnostný projekt je možné škálovať: možno ho spraviť pre celú organizáciu, alebo sa zamerať na kľúčový systém organizácie, je možné voliť úroveň podrobnosti. V každom prípade bude organizácia potrebovať identifikovať svoje kľúčové aktíva, zraniteľnosti, ktoré majú, hrozby, ktoré sa voči nim môžu uplatniť, existujúce opatrenia, aby zistila aké sú najväčšie riziká a prijala na ich ošetrenie potrebné opatrenia. Potom sa môže zamerať na vybrané oblasti alebo systémy a pre tie spraviť detailnú analýzu rizík. Správa rizík je podstatou zaistenia KIB v organizácii.
2) Bezpečnostná situácia v organizácii sa mení, objavujú sa nové hrozby, zraniteľnosti; zavedené opatrenia môžu strácať na účinnosti. Preto je potrebná dokumentácia opatrení a kontrola ich dodržiavania a posudzovanie ich účinnosti, aby ich v prípade potreby bolo možné doplniť, alebo nahradiť účinnejšími.

3.2.7 Zapojenie zamestnancov do bezpečnostného procesu

1) do bezpečnostného procesu MUSIA byť zapojení všetci pracovníci organizácie; každý MUSÍ mať základné informácie o KIB, hrozbách a vedieť, ako používať bezpečnostné opatrenia vo svojej práci
2) zamestnanci MUSIA mať možnosť zohrávať aktívnu rolu v KIB, MUSIA byť informovaní o príprave bezpečnostných opatrení a organizačných pravidiel
3) keď sa zavádzajú bezpečnostné politiky, bezpečnostné nástroje, zamestnanci MUSIA byť primerane informovaní o tom, ako by sa mali používať

Komentár

1) každý človek, ktorý pristupuje k informácii, systémom, alebo sieťam organizácie, môže pozitívne alebo negatívne ovplyvniť ich bezpečnosť. Každý človek nemôže byť odborníkom na KIB, ale potrebuje vedieť základné veci
   a) chápať význam KIB pre organizáciu a vedieť, že sa KIB týka aj jeho (že existujú povinnosti, ktoré musí plniť a sankcie, ak ich plniť nebude)
   b) čo má robiť, ako, čo nesmie robiť (prečo), na koho sa má obrátiť, keď narazí na problém, s ktorým si nevie rady
   c) kde nájde základné dokumenty KIB organizácie, informácie o bezpečnostných problémoch, varovania, upozornenia, návody

d) Nový zamestnanec prejde základným školením KIB a pre existujúcich bude potrebné preškoliť v základoch a organizovať školenia k aktuálnym bezpečnostným problémom pre tých zamestnancov, ktorých sa problém týka.

2) súčasťou povinností zamestnanca je aj upozorňovanie na bezpečnostné problémy, na ktoré narazí – odhalenie zraniteľností, bezpečnostných incidentov. Zamestnanci musia vedieť, komu zistené problémy nahlasovať (čo je dôležité najmä v prípade, keď sa jedná o útok, alebo začínajúci bezpečnostný incident, kde včasná reakcia môže minimalizovať škody[10]). Keď sa pripravujú nové opatrenia, ktoré sa týkajú zamestnancov, je potrebné prebrať ich s nimi alebo ich zástupcami[11] (manažér KIB), aby sa našiel postup, ako ich zaviesť, aby ich zamestnanci prijali a používali.
3) podľa toho, aký je rozsah a charakter opatrení, koho sa týkajú treba zvoliť vhodnú formu (špecializované školenie, bod na prevádzkovej porade, webová stránka, FAQ, návody...) a zamestnancov informovať o tom, čo sa od nich očakáva, prečo, ako majú nové povinnosti plniť.

3.2.8 Integrovanie KIB do procedúr a procesov organizácie

1) KIB **MUSÍ** byť primeraným spôsobom integrovaná do všetkých procesov v organizácii; t.j. aj existujúcich aj nových
2) KIB **BY MALA** byť koordinovaná s inými oblasťami organizácie, ktoré sa zaoberajú bezpečnosťou a manažmentom rizík
3) hlavný manažér KIB **MUSÍ** byť primeraným spôsobom zapojený do prijímania bezpečnostne relevantných rozhodnutí

Komentár

1) Najprv bude potrebné určiť činnosti, ktoré organizácia vykonáva na plnenie svojich úloh aj zabezpečenie vlastného chodu a ľudí, ktorí za ne zodpovedajú. To by mali vedieť vedúci organizačných útvarov organizácie. Manažér KIB spolu s ľuďmi zodpovednými za jednotlivé činnosti zistí, aká informácia sa v týchto činnostiach používa, aké sú na ňu kladené bezpečnostné požiadavky (akú ochranu si vyžaduje), v akých systémoch sa spracováva, kto má k nej prístup, čo ju ohrozuje a aké opatrenia je potrebné prijať, aby sa hrozby nenaplnili. Týka sa to existujúcich činností, pri nových činnostiach je situácia jednoduchšia, lebo je ich možné navrhovať tak, aby v nich boli bezpečnostné opatrenia už „zabudované“
2) mnohé opatrenia na ochranu informácie nemajú “informatický“ charakter. Manažér KIB bude potrebovať pomoc právneho oddelenia pri príprave zmlúv s dodávateľmi, osobného oddelenia pri výbere pracovníkov, zmenách pracovného zaradenia, správy budov pri implementácii opatrení na ochranu pred prírodnými vplyvmi, fyzickým prístupom k systémom a pod.
3) Manažér KIB by mal byť schopný posúdiť bezpečnostnú stránku navrhovaných riešení a upozorniť na problémy, ktoré by ich prijatie mohlo spôsobiť.

3.3 Vypracovanie bezpečnostného projektu

Vyššie uvedené základné opatrenia viedli k spusteniu dobre nastaveného bezpečnostného procesu a vytvoreniu systému riadenia informačnej bezpečnosti v organizácii. Tým vytvorili základ pre ďalšiu fázu bezpečnostného procesu, ktorým je vypracovanie bezpečnostného projektu organizácie. To je úloha, ktorá je stanovená v § 19, ods. (1), písm. c) , § 23 ods. (1) a (2) zákona o ITVS [3]. Obsah a štruktúra bezpečnostného projektu je popísaná vo vyhláške [4].

[10] niečo podobné ako včasná lokalizácia požiaru
[11] ľuďmi, ktorí budú vedieť posúdiť, či ich kolegovia na podobných pozíciách budú schopní opatreniam rozumieť a aplikovať ich

Bezpečnostný projekt sa môže vzťahovať na celú organizáciu, jej časť, alebo na konkrétny systém. Jeho cieľom je zistiť bezpečnostné potreby entity (= celá organizácia, časť organizácie, konkrétny systém), na ktorú sa vzťahuje, navrhnúť a zaviesť opatrenia. Okrem rozsahu (na čo sa projekt vzťahuje) je možné pri návrhu projektu voliť aj granularitu (úroveň podrobnosti danú napríklad tým, čo sa považuje za aktívum, ako detailne sa rozlišujú hrozby a pod.
Na zistenie celkových bezpečnostných potrieb organizácie bude potrebné vypracovať bezpečnostný projekt pre celú organizáciu, t.j. vykonať vysokoúrovňovú analýzu rizík (menej podrobnú, ale vzťahujúcu sa na celú organizáciu), pri ktorej sa jednak identifikujú riziká, ktoré je možné ošetriť pomocou spoločných opatrení a tie, ktoré si vyžadujú podrobnejšiu analýzu, resp. užšie, ale na konkrétny systém alebo problém zameraný bezpečnostný projekt.
Analýza rizík je základom pre správu rizík a správa rizík je podstatou KIB v organizácii. Na základe analýzy rizík navrhuje (manažér KIB) ktoré riziká je optrebné ošetriť a bezpečnostné opatrenia pomocou ktorých sa to má spraviť. Opatrenia si buď vyžadujú zásah do fungovania organizácie, alebo implementáciu nejakého technického riešenia, nové povinnosti pre ľudí a pod., preto podliehajú schvaľovaniu vedením organizácie. To nemusí mať vedomosti potrebné na vykonanie analýzy rizík, ale malo by byť schopné posúdiť dopad nejakej hrozby na organizáciu a náklady na zavedenie nejakého opatrenia. Potrebné poznatky o analýze rizík možno nájsť v materiáli [11].
Pri analýze rizík sa dajú uplatniť rôzne postupy (kvantitatívna alebo kvalitatívna analýza rizík), vedenie organizácie (v politike KIB) bude musieť rozhodnúť, ako sa v organizácii pri analýze rizík bude postupovať a aké riziká sú pre organizáciu neprijateľné a ktoré si bude môcť, resp. s ohľadom na svoje možnosti musieť dovoliť akceptovať (stanovenie hranice akceptovateľného rizika).

3.4 Ďalšie kroky ku štandardnej úrovni

Nasledujúce opatrenia nie sú ničím novým, čiastočne sa už objavili aj medzi riešeniami potrebnými na zavedenie základných opatrení, ale keď bude dosiahnutá základná úroveň KIB, stojí za to sa k nim vrátiť a riešiť problémy systematicky. Pre úplnosť ich uvedieme a stručne popíšeme, aby tí, ktorí zavádzajú riešenia na základnej úrovni vedeli, na čo sa bude potrebné pripraviť pri posune zo základnej na štandardnú úroveň KIB v organizácii.

3.4.1 Kontinuita KIB

Aj dokumenty, aj zavedené riešenia vychádzali zo situácie, ktorá bola v čase ich vytvárania/zavedenia. Okolnosti sa však mohli odvtedy zmeniť a dokumenty (Politika KIB, Stratégia KIB. špeciálne politiky, metodiky,...) nemusia byť aktuálne a opatrenia dostatočne účinné. Navyše sa mohli objaviť nové zraniteľnosti, hrozby, mohli sa zmeniť podmienky, pri ktorých niektoré riziká boli ešte akceptovateľné, zmeniť organizačná štruktúra organizácie, narásť rozsah povinností manažéra KIB do rozsahu prevyšujúceho jeho kapacity. Organizácia bude

5) potrebovať revidovať pravidelne bezpečnostnú dokumentáciu vrátane bezpečnostných cieľov (čo je, ostatne, aj požiadavka §20, ods. (5) Zákona o KB [1]),
6) monitorovať účinnosť bezpečnostných opatrení,
7) vykonávať audity zamerané jednak na ISMS, jednak na kompletnosť a účinnosť opatrení,
8) sledovať výskyt hrozieb, objavenie nových zraniteľností

korigovať, prípadne rušiť existujúce a prijímať nové opatrenia

3.4.2 Správy a hlásenia vedeniu organizácie

Po počiatočnom informačnom nápore na vedenie organizácie súvisiacom so spustením bezpečnostného procesu v organizácii sa KIB dostane do štandardnej agendy vedenia organizácie. Okrem štandardných výročných správ o stave a plánoch KIB sa vedenie organizácie bude musieť zaoberať mimoriadnymi problémami a častokrát prijímať rozhodnutia o opatreniach. To predpokladá, že manažér KIB pripraví hlásenia/správy pre vedenie s informáciami potrebnými pre

prijatie rozhodnutia, vrátane priorít možných riešení, nákladov a času potrebného na implementáciu navrhovaných riešení. Rozhodnutia vedenia budú zachytené v zápisniciach, ale rovnako by mali byť zachytené a dlhodobo uchovávané manažérske rozhodnutia týkajúce sa bezpečnostne relevantných udalostí a to v takej podobe, aby sa dali podrobiť auditu.

3.4.3 Dokumentácia bezpečnostného procesu

Explicitné požiadavky na bezpečnostnú dokumentáciu definuje § 2 vyhlášky [2]. Tento zoznam bude potrebné doplniť o dokumenty, ktoré má organizácia vytvoriť na základe požiadaviek vyhlášky [4] a ktoré vzniknú pri činnostiach súvisiacich s KIB v organizácii. V súčasnosti ide o "veľké" dokumenty, ako

9) Stratégia KIB
10) Politika KIB
11) čiastkové politiky KIB
12) klasifikácia informácií a kategorizácia sietí a informačných systémov
13) výsledky kontroly zavedenia navrhovaných bezpečnostných opatrení
14) dokumentácia k analýzam rizík
15) správy auditov

3.4.4 Zvyšovanie bezpečnostného povedomia

Jednotlivé školenia (vstupné školenia, školenia pri zaraďovaní do rôl, preškolenia pri zmenách politík, bezpečnostných mechanizmov, po bezpečnostných incidentoch a pod.) by organizácia mala spojiť do systému zvyšovania bezpečnostného povedomia, čím bude spĺňať požiadavky §7 písm. b), d) vyhlášky [2] a časti C Prílohy 2 vyhlášky [4].

3.4.5 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 bezpečnostného manažéra. V prípade keď úlohy prevyšujú kapacity, je potrebné do ich riešenia zapojiť ďalších zamestnancov, alebo externých odborníkov.

4 Záver

Organizácie, ktoré sú správcami ISVS II. a II. kategórie majú zákonmi a vykonávacími predpismi stanovené množstvo úloh v kybernetickej a informačnej bezpečnosti. Aj objektívne, ISVS a ďalšie d-IKT, ktoré organizácie používajú sú kritickou infraštruktúrou organizácie; ich výpadok s veľkou pravdepodobnosťou znemožní alebo aspoň výrazne obmedzí činnosť organizácie. Hrozby voči informácii, informačným systémom sú reálne a nikto si nemôže byť istý tým, že sa jeho ISVS alebo iné d-IKT nestanú cieľom nejakého útoku. Kybernetická a informačná bezpečnosť je však rozsiahla a komplikovaná oblasť a riešenia, ktoré je potrebné v organizácii na ochranu informácie a systémov zaviesť, si vyžadujú zdroje: peniaze, odborníkov, znalosti a čas. Organizácia nemá zdrojov nazvyš, vedenie organizácie má množstvo iných povinností, ako je KIB; preto sme v tomto dokumente popísali postup, ktorý vedie k systematickému riešeniu KIB v organizácii a úlohy, ktoré v tomto riešení pripadajú vedeniu organizácie. Ďalšie dokumenty by mali byť zamerané na špecifické oblasti a poskytovať manažérom KIB a ďalším špecialistom na KIB v organizáciách návody na riešenie konkrétnych úloh, ktoré im ukladajú zákony, spracované na základe medzinárodných štandardov.

5 Referencie

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
[2] Vyhláška Národného bezpečnostného úradu č. 362/2018, 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] ISO/IEC 27005 — Information security risk management.
[8] BSI Standard 200-1 Information Security Management Systems (ISMS) www.bsi.bund.de/grundschutz
[9] BSI Standard 200-2 IT Grundschutz Methodology, www.bsi.bund.de/grundschutz
[10] IT-Grundschutz Compendium, BSI 2019
[11] Olejár D., Krátky úvod do kybernetickej a informačnej bezpečnosti

6 Zoznam skratiek

BSI Bundesamt für Sicherheit in der Informationstechnik
d-IKT digitálne informačné a komunikačné technológie
FAQ frequently asked questions
GDPR General Data Protection Regulation
e-IDAS Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
IB informačná bezpečnosť
IKT informačné a komunikačné technológie
ISMS Information security management system
ISO International Organization for Standardization
ISVS informačný systém verejnej správy
IT informačné technológie
ITVS informačné technológie verejnej správy
KB kybernetická bezpečnosť
KIB kybernetická a informačná bezpečnosť