Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.1 | kyberbezpecnost@mirri.gov.sk

Povinnosti správcu ISVS

v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní

Manažérske zhrnutie

Prevádzka informačného systému verejnej správy (ďalej len „**ISVS**") je podľa zákona o kybernetickej bezpečnosti základnou službou v prípade, ak prekračuje špecifické sektorové kritériá a identifikačné kritériá prevádzkovanej služby. V takom prípade je prevádzkovateľ tejto služby povinný na jeho ochranu prijať bezpečnostné opatrenia uvedené vo vyhláške. ISVS je aj informačnou technológiou verejnej správy (ďalej len „**ITVS**") a zákon o informačných technológiách vo verejnej správe a príslušná vyhláška definujú opatrenia, ktoré jeho správca musí prijať na jeho ochranu. Štát potrebuje na udržanie svojich funkcií zabezpečiť plnenie úloh pomocou štátnych orgánov. Kybernetická a informačná bezpečnosť (ďalej len „**KIB**") slúži ako nástroj na zabezpečenie, že procesy, systémy aj technológie budú dostatočne chránené aj v prípade kybernetického útoku alebo iných neočakávaných udalostí a bezpečnostných incidentov. Oba zákony a vykonávacie predpisy vychádzajú z medzinárodných noriem, predovšetkým z medzinárodnej normy ISO/IEC 27001.

Tento dokument vychádza z vyššie uvedených právnych predpisov, ktoré vyžadujú od správcu ISVS II. a III. kategórie zaviesť v organizácii systém riadenia informačnej bezpečnosti. Úlohou tohto dokumentu je pomôcť vybudovať systém KIB tak, aby bol v súlade s uvedenou legislatívnou a tiež aby bol funkčný, účinný, a dokázal znižovať bezpečnostné riziká na prijateľnú úroveň. Metodický návod, ako implementovať uvedené opatrenia sú predmetom ďalších dokumentov MIRRI určených primárne pre bezpečnostného manažéra a iné poverené osoby.

Prehľad právnych predpisov

- **Zákon 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov**

(ďalej len „zákon 69/2018")

- **Vyhláška Národného bezpečnostného úradu 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení**

(ďalej len „vyhláška 362/2018")

- **Zákon 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov**

(ďalej len „zákon 95/2019")

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

(ďalej len „vyhláška 179/2020")

1 Povinnosti správcu ISVS

Požiadavky na bezpečnosť informačných technológií verejnej správy definuje zákon o ITVS a detailne špecifikuje príslušný vykonávací predpis. Prehľad bezpečnostných požiadaviek je zhrnutý podľa kategórii v dokumente *Legislatívne požiadavky* na webovej stránke MIRRI.

Za ISVS podľa zákona o ITVS zodpovedá jeho správca. Správcu informačnej technológie verejnej správy definuje §2 ods. 5 zákona 95/2019, podrobnejší zoznam a kategorizácia ITVS sú uvedené vo vyhláške 179/2020.

Jednotné riešenie KIB pre ISVS sa zakladá na § 19, ods. (1) zákona 95/2019, ktorý obsahuje požiadavku na správcu

ISVS zaviesť a udržiavať v organizácii **systém riadenia informačnej bezpečnosti**, ktorý sa podľa § 21, ods. (3), písm. b) bod 2. **vzťahuje na <u>všetky</u> informačné systémy, ktoré sú v jej správe**.

Pozn. V oblasti riešenia kybernetickej a informačnej bezpečnosti je potrebné uvedomiť si, že pracujeme s pojmami „Správca" a „Prevádzkovateľ".

*Podľa §2 ods.5 zákona č. 95/2019 Z. z. o ITVS je **Správcom** na účely tohto zákona je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.*

*Podľa §2 ods.6 zákona č. 95/2019 Z. z. o ITVS je **Prevádzkovateľom** na účely tohto zákona správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba. Správcom určený alebo osobitným predpisom ustanovený prevádzkovateľ vykonáva, v rozsahu povinností správcu, činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis; ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu. Určením alebo ustanovením prevádzkovateľa nie je dotknutá zodpovednosť správcu za plnenie povinností podľa tohto zákona.*

Požiadavky oboch zákonov a vyhlášok sa vzťahujú na ISVS a jeho správcu. Našťastie majú veľký spoločný prienik, počet obsahovo rozdielnych požiadaviek je relatívne malý, väčšinou sa dajú zosúladiť a pokiaľ to je potrebné tak sa dajú niektoré z požiadaviek riešiť aj individuálne. Na webovej stránke MIRRI je uvedený dokument *Checklist pre agendu IT a kybernetickú bezpečnosť*, ktorý obsahuje prehľad všetkých bezpečnostných opatrení naprieč platnou legislatívou.

- Na správcu ISVS sa teda vzťahujú požiadavky dvoch rozličných zákonov, zákona 69/2018 a zákona 95/2019.
- **Povinnosti správcu ISVS ako prevádzkovateľa základnej služby** definuje zákon 69/2018 a konkretizuje vyhláška 362/2018.
- **Povinnosti správcu ISVS ako správcu ITVS** stanovuje zákon 95/2019 a kategorizáciu ITVS a bezpečnostné opatrenia na zaistenie ich ochrany stanovuje vyhláška 179/2020.

2 Základné kroky / opatrenia

V tejto časti uvádzame postupnosť krokov na zavedenie KIB podľa platnej legislatívy. Jednotlivé opatrenia sú zoradené podľa dôležitosti, ktorá vyplýva z praxe. Je nevyhnutné zvážiť postupnosť krokov, ktorá sa zakladá na aktuálnej situácii v konkrétnej organizácii. Je možné zavádzať niektoré opatrenia súčasne, prípadne niektoré časti sa dajú riešiť aj externe pomocou dodávateľa. Pri výbere dodávateľa odporúčame preštudovať dokument *Ako si správne vybrať dodávateľa v oblasti KB*, na ktorom spolupracovalo MIRRI s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti.

2.1 Podpora vedenia organizácie

Pre optimálne riadenie procesu zavedenia KIB do organizácie je nevyhnutné prijatie celkovej zodpovednosti za KIB vedením organizácie. Bez dostatočnej podpory vedenia nebude možné zaviesť potrebné procesy a vyčleniť potrebné finančné a personálne zdroje. Keďže vedenie organizácie zodpovedá najmä za to, že organizácia plnohodnotne plní úlohy, pre ktoré bola vytvorená. Pokiaľ je pre plnenie týchto úloh potrebné používanie ISVS, vedenie organizácie zodpovedá za to, že budú spoľahlivo fungovať a tým plniť hlavné úlohy organizácie.

Deklaratívne vyhlásenie záväzku o podpore KIB je v kontexte vyhlášky č. 179/2020 Z. z. súčasťou stratégie KIB, ktorá bude vysvetlená v nasledujúcich krokoch.

Hlavným zmyslom daného vyhlásenia vedenia organizácie je upozornenie zainteresovaných, že vedenie organizácie si plne uvedomuje potrebu a podporuje proces zavedenia bezpečnostných opatrení na dosiahnutie potrebnej úrovne KIB.

Vedenie organizácie musí:

- prijať celkovú zodpovednosť za KIB v organizácii
- iniciovať, riadiť a monitorovať bezpečnostný proces
- byť dobrým príkladom pri dodržiavaní bezpečnostných požiadaviek a opatrení
- vymenovať zamestnancov zodpovedných za KIB a poskytnúť im potrebné oprávnenia a zdroje
- pravidelne dostávať informácie o stave KIB v organizácii, možných rizikách vyplývajúcich z chýbajúcich alebo nedostatočných bezpečnostných opatrení

2.2 Vymenovanie manažéra KIB

Hlavné úlohy manažéra KIB:

- presadzuje KIB v organizácii, riadi a koordinuje bezpečnostný proces
- musí mať primeranú kvalifikáciu a musí mať dostatočné podmienky na jej zvyšovanie
- musí mať k dispozícii dostatočné zdroje
- v prípade potreby musí mať možnosť podávať správy/hlásenia priamo vedeniu organizácie
- musí byť zapojený v počiatočnej fáze rozsiahlych projektov, ako napr. zavedenia novej aplikácie alebo IT systému

Ak na funkciu manažéra KIB organizácia nemá vhodného zamestnanca, organizácia musí nájsť a vymenovať externého manažéra KIB.

Manažér KIB bude zodpovedný za návrh a implementovanie všetkých požiadaviek:

- odborné požiadavky na túto rolu, aké predpoklady by mal napĺňať,
- možnosť preniesť na externú osobu (za akých predpokladov),
- aké bude mať úlohy, zodpovednosti,
- kompetencie.

Zároveň je potrebné zahájiť v organizácii ustanovenie Bezpečnostného výboru.

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. 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.

Povinnosť vymenovať manažéra KIB je definovaná v súlade s legislatívou a má nasledovné zodpovednosti a právomoci.

<table>
<tr><th colspan="3">Vyhláška 179/2020</th><th colspan="4">Vyhláška 362/2018</th></tr>
<tr><td>vypracovať, udržiavať a aktualizovať Politiku kybernetickej bezpečnosti a informačnej bezpečnosti a ďalšie interné riadiace akty</td><td>Kategória I.</td><td rowspan="10">Kategória II.</td><td rowspan="10">Kategória III.</td><td>má možnosť predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby,</td><td rowspan="10">Kategória I. - odporúčané</td><td rowspan="10">Kategória II. - odporúčané</td><td rowspan="10">Kategória III. - POVINNÉ</td></tr>
<tr><td>riadiť a zaisťovať kybernetickú a informačnú bezpečnosť podľa všeobecne záväzných právnych predpisov a interných riadiacich aktov,</td><td rowspan="9"></td><td>zabezpečuje aplikáciu bezpečnostných opatrení v systéme riadenia kybernetickej bezpečnosti,</td></tr>
<tr><td>metodicky viesť správcov informačných technológií verejnej správy, gestorov informačných technológií verejnej správy, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov,</td><td>je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a</td></tr>
<tr><td>v súčinnosti s ostatnými organizačnými útvarmi analyzovať, definovať a monitorovať bezpečnostné hrozby a riziká organizácie,</td><td>spĺňa znalostné štandardy na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu,</td></tr>
<tr><td>navrhovať opatrenia na zamedzenie alebo minimalizáciu rizík a dopadov hrozieb, bezpečnostných udalostí, incidentov, mimoriadnych situácií, monitorovať plnenie a efektivitu týchto opatrení a viesť evidenciu bezpečnostných incidentov,</td><td colspan="3" rowspan="6"></td></tr>
<tr><td>koordinovať vypracovanie plánov kontinuity a obnovy činností organizácie správcu,</td></tr>
<tr><td>predkladať odborné stanoviská, analýzy k procesom, projektom, zmenám a ostatným aktivitám organizácie majúcich vplyv na kybernetickú bezpečnosť a informačnú bezpečnosť organizácie správcu,</td></tr>
<tr><td>zabezpečiť pravidelné – najmenej raz za dva roky – preskúmanie stavu informačnej bezpečnosti a spolupracovať pri realizácii auditov</td></tr>
</table>

vykonávaných internými a externými subjektmi,				
zabezpečovať školenia zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,				
spolupracovať s inými orgánmi verejnej moci.				
navrhuje stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,				
informuje bezpečnostný výbor alebo štatutárny orgán správcu o stave informačnej bezpečnosti v organizácii správcu najmenej raz za rok,				
bezodkladne informuje bezpečnostný výbor alebo štatutárny orgánu správcu o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach,				
zabezpečuje nezávislé preskúmanie stavu informačnej bezpečnosti a spoluprácu pri realizácii auditov vykonávaných internými a externými subjektmi.				

Vedenie organizácie zodpovedá (okrem iného) za KIB organizácie. Definuje ciele, bude rozhodovať v koncepčných otázkach, ale niekto im musí pripravovať odborné podklady a zabezpečovať realizáciu prijatých rozhodnutí (a plniť množstvo ďalších povinností). Týmto človekom je manažér KIB.

Riadenie, organizovanie i koordinácia bezpečnostného procesu vystihuje všetko podstatné – poznať organizáciu a jej bezpečnostné potreby, zdroje, ktoré má k dispozícii, vedieť pripraviť návrh postupu, presvedčiť vedenie organizácie a jednoducho mu vysvetliť, 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.

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.

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.

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).

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.

2.3 Nadefinovanie bezpečnostných cieľov

Bezpečnostné ciele organizácie v KIB možno sformulovať tak, že sa oprú o:

a) potrebu zaistiť hodnovernosť požadovanej informácie, aby sa organizácia mohla na informáciu mohla spoľahnúť,

b) požiadavku, aby informačné systémy a siete organizácie spoľahlivo fungovali,

c) potrebu, aby organizácia preukázateľne plnila všetky právne požiadavky na spracovanie a ochranu údajov,

d) požiadavku efektívneho vynakladania nákladov a zdrojov na KIB.

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.

Možné všeobecné bezpečnostné ciele organizácie sú napríklad:

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) a podobne.

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

Zároveň je potrebné v organizácii zahájiť preverenie bezpečnostných opatrení, a tie, ktoré chýbajú, je potrebné implementovať.

2.4 Vytvorenie bezpečnostnej stratégie a celej koncepcie riadenia kybernetickej bezpečnosti

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 (pozn. nie je potrebné uvádzať čiastkové ciele, aby sa z dôvodu možných budúcich

miernych úprav nemusel prerábať tento vrcholový strategický dokument). Daný dokument je podrobnejšie rozpracovaný na webovej stránke MIRRI v dokumente Stratégia KIB.

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 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 IKT 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?

- Aby vedenie organizácie mohlo spustiť implementáciu bezpečnostných opatrení v organizácii, musí **špecifikovať a zdokumentovať** bezpečnostné ciele a **stanoviť** stratégiu KIB.
- Vedenie organizácie musí zabezpečiť ohodnotenie bezpečnostných požiadaviek na jednotlivé činnosti a musí vytvoriť **všeobecné organizačné podmienky** na to, aby sa umožnilo správne a bezpečné narábanie s informáciou vo všetkých činnostiach organizácie.
- Vedenie organizácie musí **podporovať a prevziať zodpovednosť** za bezpečnostnú stratégiu a bezpečnostné ciele.
- Bezpečnostná stratégia a bezpečnostné ciele sa musia **pravidelne revidovať**, aby sa zaistilo, že sú stále aktuálne a že sa dajú efektívne implementovať.

2.5 Vytvorenie bezpečnostnej politiky

Bezpečnostná politika čosi ako ústava, ktorá má byť doplnená zákonmi upravujúcimi detailnejšie konkrétne oblasti. Bezpečnostná politika je rozpracovaná v špeciálnych bezpečnostných politikách, smerniciach a interných riadiacich aktoch. A tie sú ešte na tretej úrovni detailne rozpracované v podobe bezpečnostných metodík, praktík a postupov. Obvykle je bezpečnostná politika chápaná ako pomerne všeobecný (vysokoúrovňový) dokument, ktorého hlavnou úlohou je prezentovať verejnosti ciele a prístup vedenia ku KIB.

Organizácia upraví existujúce postupy tak, aby zaistila dodržiavanie elementárnych požiadaviek na ochranu informácie, systémov a sietí.

2.6 Vytvorenie interných predpisov alebo smerníc v rozsahu

- riadenie prístupov,
- klasifikácie informácii a kategorizácia sietí a informačných systémov,

- riadenia informačnej bezpečnosti,
- všetky smernice musia pokrývať všetky domény bezpečnosti (sieťová, prístupy, fyzická a objektová bezpečnosť, dodávatelia),
- integrovania procesov KIB do prevádzkových procesov (na úrovni IT aj "biznis" úrovni),
- vytvorenia potrebných zoznamov/evidencií, analýz, plánov, technickej dokumentácie.

2.7 Vybudovanie organizačného útvaru KIB

Zároveň vytvorenie a oficiálne ustanovenie bezpečnostného výboru organizácie.

- V organizácii sa musí vytvoriť **organizačná štruktúra** pre KIB
- Transparentným spôsobom musia byť **definované a pridelené** kompetencie, zodpovednosti a úlohy v manažmente KIB
- V organizácii musia byť definované **bezpečnostné roly** podieľajúce sa na riadení KIB
- Do týchto rolí musia byť zaradení kvalifikovaní ľudia s dostatočnými zdrojmi potrebnými na vykonávanie povinností vyplývajúcich z týchto rolí
- Pre všetky dôležité funkcie v manažmente KIB musí byť definovaný **systém zastupovania**
- Musia byť zjednotené komunikačné kanály a musí byť stanovená **komunikačná matica**

Aby mal úlohy v KIB aj kto plniť, je potrebné v organizácii jasne stanoviť, kto za čo zodpovedá a komu.

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.

Všetky zúčastnené strany musia byť včas informované o 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 tiež oboznámiť zúčastnených, ako má komunikácia prebiehať.

2.8 Zahájenie riadenia rizík

Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému verejnej správy a jeho okolia.

Pre správnu analýzu rizík nestačí iba poznať hrozby, zraniteľnosti a dopady na aktíva. Chýbajúci faktor pri posudzovaní závažnosti nebezpečenstva, pred ktorým je aktíva organizácie potrebné chrániť, je pravdepodobnosť naplnenia hrozby.

Riziko je veličina spájajúca pravdepodobnosť naplnenia hrozby a dopad hrozby. Následne, po vyjadrení hodnoty rizík, je potrebné zamerať sa na ošetrenie rizík s najväčšou hodnotou a optimalizovať využívanie zdrojov.

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z.

o kybernetickej bezpečnosti a taktiež zákona č. 95/2019 Z.z. o ITVS je podrobne spracovaná v materiály, publikovanom Národným bezpečnostným úradom **na tomto mieste**.

V rámci daného metodického materiálu je podrobne popísaná oblasť:

a) procesu a metodiky riadenia rizík,
b) stanovenia kontextu rizika (identifikácia aktív, hrozieb, zraniteľností, dopadov, existujúcich opatrení a závažnosti rizík),
c) kvalitatívnej analýzy rizík,
d) semikvantitatívnej (zmiešanej) analýzy rizík,
e) ošetrovania rizík vrátane návrhu bezpečnostných opatrení,
f) akceptácie zvyškového rizika,
g) komunikácie rizika.

Súčasťou dokumentu sú aj prílohy (Vzor návrhu na akceptáciu rizika, Vzor správy o riziku).

2.9 Implementovať bezpečnostné školenia

Každý človek, ktorý pristupuje k informácii, systémom, alebo sieťam organizácie, môže pozitívne alebo negatívne

- Do bezpečnostného procesu musia byť zapojení **všetci** zamestnanci organizácie; každý musí mať základné informácie o KIB, hrozbách a vedieť, ako implementovať bezpečnostné opatrenia v rámci každodenného pracovného života.
- Zamestnanci musia mať možnosť zohrávať **aktívnu rolu** v KIB, zároveň je vhodné ich informovať o príprave bezpečnostných opatrení a organizačných pravidiel naprieč celou organizáciou.
- Keď sa zavádzajú bezpečnostné politiky, bezpečnostné nástroje, zamestnanci musia byť primerane **informovaní** o tom, ako by sa mali používať.

ovplyvniť ich bezpečnosť. Každý človek nemôže byť odborníkom na KIB, ale potrebuje vedieť minimálne:

a) 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) každý 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.

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).

Podľa toho, aký je rozsah a charakter opatrení, koho sa týkajú treba zvoliť vhodnú formu komunikácie (špecializované školenie, bod na prevádzkovej porade, webová stránka, FAQ, návody...). Je nevyhnutné zamestnancov informovať o tom, čo sa od nich očakáva, prečo, a ako majú nové povinnosti plniť.

2.10 Zahájiť implementáciu bezpečnostných opatrení

- Pre **celý proces** spracovania informácie musia byť definované primerané bezpečnostné opatrenia
- Všetky bezpečnostné opatrenia musia byť systematicky zdokumentované v smerniciach a iných interných riadiacich aktoch a v pravidelných intervaloch **aktualizované**

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). Kľúčovou časťou z ktorej bude organizácia vychádzať je analýza rizík. V organizácii bude potrebné spraviť analýzu rizík, vyhodnotiť ich a navrhnúť opatrenia. 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.

- KIB musí byť primeraným spôsobom integrovaná do **všetkých procesov** v organizácii; t. j. existujúcich aj nových procesoch
- KIB by mala byť **koordinovaná** s inými oblasťami organizácie, ktoré sa zaoberajú bezpečnosťou a manažmentom rizík

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“.

Mnohé opatrenia na ochranu informácie nemajú “technický“ 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.

Manažér KIB by mal byť schopný posúdiť bezpečnostnú stránku navrhovaných riešení a upozorniť na problémy, ktoré by ich prijatie mohlo spôsobiť.