Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.0 | kyberbezpecnost@mirri.gov.sk

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Prvotná orientácia správcu

Úvod

Kybernetická bezpečnosť je v odborných kruhoch často skloňovaný pojem. Ide o veľmi rozsiahlu problematiku, pokrývajúcu viaceré oblasti a ponúkajúcu širokú paletu rôznych produktov, postupov a metodík, sľubujúcich výrazné zlepšenie bezpečnosti Vašej organizácie. Ako si však z tohto mora vybrať, keď ste iba na začiatku cesty? Pomôcť vám v tomto je práve ambíciou týchto metodických dokumentov.
Dozviete sa, čo vlastne je kybernetická bezpečnosť a vysvetlíme vám, prečo si zasluhuje Vašu pozornosť, a čím by ste mali začať, ak ste sa problematike doteraz systematicky nevenovali. Ak ste zástupca organizácie, zodpovieme vám otázku, aké zákonné povinnosti sa na vašu organizáciu vzťahujú a poskytneme vám materiály, ktorých cieľom je pomôcť vám tieto povinnosti naplniť – nielen formálne, ale hlavne tak, aby výsledkom bolo skutočné zlepšenie.

1 Čo je kybernetická a informačná bezpečnosť a prečo by nás mala trápiť?

Výpočtová a komunikačná technika je dnes prakticky neoddeliteľnou súčasťou našej každodennej existencie – máloktorú aktivitu si vieme predstaviť vykonávať bez počítača, mobilu či tabletu. Tieto zariadenia sú veľmi výkonné a spracovávajú obrovské množstvo údajov, preto sú atraktívnym cieľom pre zneužitie. Keď takéto zneužitie nastane, môže mať viacero negatívnych dopadov:

- V najlepšom prípade útočník iba využíva naše zdroje na svoje vlastné účely, čím ich vyťažuje a nám spôsobuje dodatočné náklady (príklad: ťaženie kryptomeny)
- Horšia je situácia, kedy je útočníkova aktivita viditeľná do okolitého sveta, čím prirodzene rozšíri informáciu, že u nás uspel. Toto je nielen strata reputácie a dôvery u klientov, je to taktiež pozvánka pre ďalších útočníkov (príklad: rozosielanie infikovaných súborov z našej elektronickej pošty mnohým adresátom)
- V najzávažnejších prípadoch útočníkove aktivity úplne znemožnia našej organizácii využívať napadnuté zdroje na ich primárny účel (príklad: zničenie serveru alebo kompletné prebratie kontroly nad ním). Podľa toho, nakoľko kritický napadnutý zdroj je, môže takáto situácia viesť až k úplnej neschopnosti organizácie vykonávať svoju činnosť.

S postupujúcim technologickým vývojom sa nielen zvyšuje hodnota dát a závislosť na ich strojovom spracovaní, ale aj dostupnosť metód útokov na organizácie a ich miera sofistikovanosti. Čo je horšie, zlepšovanie nástrojov a dostupnosti globálnej komunikácie znižuje požiadavky na znalosti a schopnosti útočníka. Začiatkom tohto tisícročia musel byť útočník odborníkom, dnes už dokáže nepripravenému cieľu spôsobiť nadmerné až likvidačné škody aj 12-ročné dieťa. Úspešné útoky majú nielen obrovské finančné dopady – správy o úspechu útočníka sa rýchlo šíria, čím spôsobujú nielen veľké reputačné škody, ale taktiež priťahujú pozornosť ďalších útočníkov. Len za prvú polovicu roka 2021 sa udialo viacero vysokoprofilových útokov s veľkými dôsledkami, dá sa spomenúť aj na staršie incidenty s rozsiahlym dopadom – napríklad plošný výpadok britského zdravotníctva spôsobený ransomvérom WannaCry v roku 2017.
Z uvedených dôvodov existuje činnosť, ktorou sa im snažíme predísť, zabrániť, či ich aspoň minimalizovať – **kybernetická a informačná bezpečnosť** (KIB). Je to priebežná a systematická činnosť, zameraná na dosiahnutie a udržiavanie stavu, kedy organizácia vie:

- Čo sú zdroje, ktoré potrebuje na svoju činnosť a/alebo majú pre ňu hodnotu, ktorú chce chrániť (tzv. ***aktíva)***
- Čo sa deje s aktívami a celkovo s dátami, informačnými systémami a používateľmi v organizácii
- Že všetko, z toho čo sa deje sa MÁ DIAŤ
- Že nič z toho, čo sa nemá diať sa NEDEJE

Systematické pokrytie celej organizácie je kritickým aspektom snaženia - útočník sa vždy sústredí na najslabšie miesto, nie nutne na najviditeľnejšiu či najdôležitejšiu časť toho, čo potrebujeme chrániť.
Nedostatočné venovanie sa KIB často nemá okamžité, konkrétne a hmatateľné dopady ako napríklad nezaplatenie účtu za elektrickú energiu. Zvyšuje však pravdepodobnosť, že vznikne problém, a jeho následné dopady. Ak sa dlho žiadna ***hrozba*** nenaplní (obzvlášť po redukcii výdavkov), často má vedenie organizácie tendenciu pristúpiť k ďalším redukciám, čím sa otvoria príležitosti pre útočníkov a následnú diskusiu „Načo míňame všetky tieto peniaze, keď nám to aj tak

nepomohlo?“.
Rovnaká situácia môže veľmi ľahko nastať, keď sa KIB pojme ako nárazová aktivita, nech sú prvotné materiály a procesy zavedené akokoľvek dokonale. Organizácie, ich činnosti a procesy sa prirodzene menia s plynutím času, čo je potrebné zohľadniť.
Z hľadiska vrcholového manažéra je kybernetická a informačná bezpečnosť problematickou záležitosťou:

- Neexistuje obmedzenie na množstvo peňazí, ktoré vyžaduje - vždy sa jej dá venovať viac
- ***Hrozby*** nikdy nie je možné eliminovať kompletne, bez ohľadu na investované množstvo zdrojov
- Výsledkom zdrojov do nej investovaných je **absencia niečoho konkrétneho** (naplnenia hrozieb)
- Je to priebežná činnosť, ktorá stráca zmysel akonáhle nie je systematická a nezohľadňuje zmeny v organizácii

Preto je nevyhnutnou podmienkou úspechu v KIB **pochopenie vedenia organizácie o jej dôležitosti** a **pridelenie dostatočných prostriedkov a kapacít na jej priebežné vykonávanie.** Vedenie organizácie nemusí vedieť detaily, jeho úlohou je byť koordinátorom a sponzorom aktivít, nakoľko sa musia dotýkať celej organizácie.
Niektoré druhy organizácií majú v oblasti KIB zákonné povinnosti. Našim cieľom je pomôcť vám zorientovať sa, čo sa na Vašu organizáciu vzťahuje a ako by mali vyzerať Vaše nasledujúce kroky, ak ste na začiatku cesty k ich plneniu.

1.1 Základ terminológie

Ako každá oblasť odbornosti, aj informačná bezpečnosť má mnoho vlastnej terminológie. Na stránkach MIRRI, v časti Sekcie / Kybernetická bezpečnosť, venovanej tejto problematike nájdete aj Stručný výkladový slovník, nateraz si ale vysvetlíme aspoň základné pojmy:

- **Aktívum** („asset“) je čokoľvek, čo má pre organizáciu hodnotu. Môžu to byť hmotné prostriedky ako je fyzické vybavenie či ľudia, ktorí v organizácii pracujú, ale aj nehmotné prostriedky ako financie, informácie, odbornosť/know-how či dobré meno organizácie. Aktíva sa snažíme v informačnej bezpečnosti chrániť, pretože sú vystavené **hrozbám** a útočníci na ne cielia svoje **útoky**.
- **Hrozba** (angl. „threat“) je existujúca možnosť udalosti, ktorá priamo či nepriamo naruší aktíva organizácie. Narušenie aktív má negatívne dôsledky pre organizáciu, ktorým sa snažíme predísť zavedením **bezpečnostného opatrenia,** čím tieto aktíva chránime.
- **Riziko** („risk“) je veličina na meranie **hrozby**. Závisí od pravdepodobnosti, že sa hrozba naplní a dopadov, ktoré toto naplnenie bude mať. Mieru rizika pre jednotlivé identifikované hrozby potrebujeme vedieť, aby sme dosiahli čo najlepší pomer cena/výkon pri našich snahách. Určenie rizika pre jednotlivé hrozby je predmetom **analýzy rizík**.
- **Zraniteľnosť** („vulnerability“) je okolnosť, ktorej využitím sa môže naplniť **hrozba**. Tá sa môže naplniť prirodzene, alebo v rámci úmyselného **útoku**.
- **Útok** („attack“) je úmyselný a cieľavedomý pokus zneužiť zraniteľnosť aktíva za účelom získania kontroly nad týmto aktívom alebo inými aktívami organizácie.
- **Bezpečnostné opatrenie** („security measure“) je riešenie, ktoré zavádzame, aby sme zredukovali **riziko**. Snažíme sa úplne alebo čiastočne odstrániť zraniteľnosť aktíva, znížiť pravdepodobnosť naplnenia hrozby, alebo redukovať dopad naplnenia tejto hrozby na aktívum či organizáciu.

2 Má naša organizácia zákonné povinnosti súvisiace s kybernetickou bezpečnosťou?

Povinnosti v tejto oblasti primárne určujú dva zákony a k nim prislúchajúce vyhlášky:

- *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov* (link)
    - *Vyhláška Národného bezpečnostného úradu č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení* (link)

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

Okrem týchto predpisov existuje aj ďalšia legislatíva, ktorú je potrebné zohľadniť pri venovaní sa KIB, tá však bude pre nás podstatná až neskôr.

2.1 Kategórie ITVS

Najdôležitejšie kritérium je, či Vaša organizácia prevádzkuje informačné technológie verejnej správy podľa zákona č. 95/2019 Z. z. Ak áno, vzťahujú sa na vás povinnosti. Aké konkrétne, to určuje kategória, do ktorej spadáte. Existujú tri kategórie prevádzkovateľov, I. kategória je najnižšia (najmenej rozsiahle povinnosti), III. kategória najvyššia. Každá kategória má zároveň povinnosti udelené všetkým nižším kategóriám.
Nasleduje prehľad kategórií, ich povinností a rozcestník pre relevantné metodické materiály.

2.2 Ktorá kategória sme?

2.2.1 Kategória I

Ak Vaša organizácia spadá pod nasledujúce kategóriu, ste prevádzkovateľ **I. kategórie**:

- Obec alebo mesto do 6 000 obyvateľov
- Komora regulovanej profesie
- Komora s preneseným výkonom verejnej moci s povinným členstvom
- Právnická osoba nevymenovaná v II. a III. kategórií, ktorá je založená alebo zriadená niektorým z nasledovných orgánov:
    - Kancelária Národnej rady Slovenskej republiky
    - Kancelária prezidenta Slovenskej republiky
    - Kancelária Ústavného súdu Slovenskej republiky
    - Kancelária Najvyššieho súdu Slovenskej republiky
    - Kancelária Najvyššieho správneho súdu Slovenskej republiky
    - Kancelária Súdnej rady Slovenskej republiky
    - Kancelária verejného ochrancu práv
    - Úrad komisára pre deti
    - Úrad komisára pre osoby so zdravotným postihnutím
    - Ústav pamäti národa
    - Sociálna poisťovňa
    - zdravotné poisťovne
    - Tlačová agentúra Slovenskej republiky
    - Rozhlas a televízia Slovenska
    - Rada pre vysielanie a retransmisiu
- Iná osoba, na ktorú je prenesený výkon verejnej moci[1]
- Iná osoba, ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov

V prípade neistoty si môžete skontrolovať presné vymedzenie v právnom predpise na tomto mieste.

[1] Okrem Národnej banky Slovenska

2.2.2 Kategória II

Ak Vaša organizácia spadá pod nasledujúce kategóriu, ste prevádzkovateľ **II. kategórie:**

- Obec alebo mesto nad 6 000 obyvateľov, okrem krajských miest
- Mestská časť s právnou subjektivitou
- Prevádzkovateľ základných služieb podľa Zákona o kybernetickej bezpečnosti, ktorého Vyhláška ku tomuto zákonu kategorizuje do I. alebo II. Kategórie
- Konkrétna organizácia z nasledovného zoznamu:
    - Kancelária verejného ochrancu práv
    - Úrad komisára pre deti
    - Úrad komisára pre osoby so zdravotným postihnutím
    - Rada pre vysielanie a retransmisiu

V prípade neistoty si môžete skontrolovať presné vymedzenie v právnom predpise na tomto mieste.

2.2.3 Kategória III

Ak je Vaša organizácia niečo z nasledovného, ste prevádzkovateľ III. kategórie:

- Krajské mesto
- Samosprávny kraj
- Ministerstvo
- Prevádzkovateľ základných služieb podľa Zákona o kybernetickej bezpečnosti, ktorého Vyhláška ku tomuto zákonu kategorizuje do III. Kategórie
- Konkrétna organizácia z nasledovného zoznamu:
    - Úrad vlády Slovenskej republiky
    - Protimonopolný úrad Slovenskej republiky
    - Štatistický úrad Slovenskej republiky
    - Úrad geodézie, kartografie a katastra Slovenskej republiky
    - Úrad jadrového dozoru Slovenskej republiky
    - Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky
    - Úrad pre verejné obstarávanie
    - Úrad priemyselného vlastníctva Slovenskej republiky
    - Správa štátnych hmotných rezerv Slovenskej republiky
    - Národný bezpečnostný úrad
    - Úrad pre reguláciu sieťových odvetví
    - Úrad pre reguláciu elektronických komunikácií a poštových služieb
    - Najvyšší kontrolný úrad Slovenskej republiky
    - Úrad pre dohľad nad zdravotnou starostlivosťou
    - Úrad na ochranu osobných údajov Slovenskej republiky
    - Generálna prokuratúra Slovenskej republiky
    - Dopravný úrad
    - Ústav pamäti národa
    - Tlačová agentúra Slovenskej republiky
    - Rozhlas a televízia Slovenska
    - Kancelária Súdnej rady Slovenskej republiky
    - Kancelária Najvyššieho súdu Slovenskej republiky
    - Kancelária Ústavného súdu Slovenskej republiky
    - Kancelária prezidenta Slovenskej republiky
    - Kancelária Národnej rady Slovenskej republiky

- Finančné riaditeľstvo Slovenskej republiky
- Národná agentúra pre sieťové a elektronické služby
- Zbor väzenskej a justičnej stráže
- DataCentrum Ministerstva financií Slovenskej republiky
- DataCentrum elektronizácie územnej samosprávy Slovenska
- Sociálna poisťovňa
- zdravotná poisťovňa
- Národné centrum zdravotníckych informácií

V prípade neistoty si môžete skontrolovať presné vymedzenie v právnom predpise na tomto mieste.

2.2.4 Nie sme na žiadnom zozname

Ak nespadáte do žiadnej kategórie, nemáte žiadne priame zákonné povinnosti. To však neznamená, že sa Vaša organizácie nemá zaoberať kybernetickou a informačnou bezpečnosťou. Zvážte, nakoľko by Vašej organizácii prekážali pravidelné týždenné výpadky systému, ktorý na svoju prácu potrebujete najviac. Zároveň keby ste boli raz mesačne predmetom novinového článku o úniku údajov. Ak toto nie je udržateľná predstava, KIB sa vás týka a je podstatná.
V tomto prípade **Vašej organizácii odporúčame splniť povinnosti kategórie I.** Jednotlivé body sú základom z hľadiska náročnosti, zároveň vám prinesú výrazné zlepšenie oproti situácii, kedy organizácia nevenuje vôbec žiadnu pozornosť KIB. Môžete použiť predpripravené šablóny a metodické postupy, ktoré sú zverejnené na tejto web stránke.

3 Zákonné povinnosti podľa kategórií

Povinnosti jednotlivých kategórií určuje Príloha č.2 k Vyhláške č. 179/2020. Nájdete tam špecifický opis jednotlivých povinností. V nasledujúcich kapitolách je vysvetlenie, čo pre Vašu organizáciu reálne znamenajú a akými pripravenými dokumentami vám vieme pomôcť.

3.1 Povinnosti I. kategórie

Ako organizácia I. kategórie máte najmä dve základné povinnosti: určiť koordinátora kybernetickej a informačnej bezpečnosti, a zaviesť interný riadiaci akt, ktorý ustanoví základné zásady a opatrenia KIB, ktoré sa organizácia následne zaviaže nasledovať a napĺňať.
Tento riadiaci akt má isté požadované náležitosti, ktorými vás prevedú naše pripravené materiály pre I. kategóriu, ktoré nájdete na stránkach MIRRI, v časti Sekcie / Kybernetická bezpečnosť.

3.2 Povinnosti II. kategórie

Pre II. kategóriu sú povinnosti komplexnejšie. Ostáva povinnosť zavedenia a napĺňania povinného riadiaceho aktu, tento musí však navyše mať formu Politiky kybernetickej a informačnej bezpečnosti v predpísanej štruktúre. Máme pre vás pripravené metodické postupy, ktoré vás touto štruktúrou prevedú (nájdete ich na stránkach MIRRI v časti Sekcie / Kybernetická bezpečnosť). K tejto politike následne potrebujete implementovať špecifické riadiace akty a zaviesť opatrenia pre Vyhláškou definované oblasti. Bližšie vás týmito povinnosťami prevedie dokument „Povinnosti správcu ISVS v kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní“ (nájdete ich na stránkach MIRRI v časti Sekcie / Kybernetická bezpečnosť).
Ďalej máte povinnosť vytvoriť a obsadiť pracovnú pozíciu Manažéra kybernetickej a informačnej bezpečnosti s pracovnou náplňou stanovenou Vyhláškou (vzorovú pracovnú náplň, ktorú je možné upraviť podľa potreby, so zaradením podľa Katalógu pracovných činností nájdete na stránkach MIRRI v časti Sekcie / Kybernetická bezpečnosť).
V neposlednom rade musíte zabezpečiť priebežný a pravidelný výkon činností, súvisiacich s KIB: pravidelné audity KIB podľa Vyhlášky 436/2019 Z.z. aspoň raz za dva roky a pri každej významnej zmene, monitorovanie a vyhodnocovanie dodržiavania stanovenej Politiky a jej aktualizáciu najmenej raz ročne.

3.3 Povinnosti III. kategórie

Keďže III. kategória je najvyššia, povinnosti pre ňu sú prirodzene najkomplexnejšie. Rovnako ako pri II. kategórií je potrebné vytvoriť a obsadiť pracovnú pozíciu Manažéra kybernetickej a informačnej bezpečnosti s pracovnou náplňou podľa Vyhlášky, tento však musí byť v organizácii situovaný mimo útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy. Pre tohto manažéra musí byť taktiež zabezpečené kontinuálne vzdelávanie. Ďalej je potrebné zriadiť bezpečnostný výbor, ktorý predkladá štatutárovi návrh zodpovednosti za implementáciu a následne rozhoduje o bezpečnostných opatreniach a postupoch. Výbor musí obsahovať:

- Štatutára alebo jeho povereného zástupcu
- Manažéra kybernetickej a informačnej bezpečnosti
- Vedúceho útvaru, zodpovedného za informačno-komunikačné technológie a infraštruktúru
- Vedúceho útvaru zodpovedného za legislatívu
- Zodpovednú osobu v zmysle Zákona o ochrane osobných údajov

V neposlednom rade Vás čaká zavedenie systému riadenia informačnej bezpečnosti, vďaka ktorému bude Vaša organizácia schopná naplniť všetky ďalšie požiadavky Vyhlášky. Týmto procesom Vás, rovnako ako pri II. kategórii, prevedie pripravený materiál „Povinnosti správcu ISVS v kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní“, dostupný na stránkach MIRRI v časti Sekcie / Kybernetická bezpečnosť.

4 Čo mám robiť ako prvé?

Bez ohľadu na kategóriu povinností, ktoré sa na organizáciu vzťahujú, prvé kroky sú vždy rovnaké: Je nutné **získať pochopenie Vedenia** organizácie pre dôležitosť agendy KIB, a treba **zmapovať aktíva** organizácie.
Argumenty pre Vedenie sme už uvádzali, pre prehľadnosť ich však zopakujeme:

- Narušenie kontinuity prevádzky pri probléme
- Reputačné škody (mediálne dopady, strata dôvery) keď sa niečo stane
- Finančné škody (výkupné útočníkovi, náprava škôd) keď sa niečo stane
- Zákonné povinnosti

Mapovanie aktív a ich spísanie do formy katalógu je základný komponent KIB, bez ktorého nie je v organizácii možné pokračovať. V závislosti od veľkosti organizácie môže ísť o veľmi rozsiahlu aktivitu, ktorá si vyžaduje znalosť organizácie a jej fungovania. Preto je najvhodnejšie, aby túto činnosť vykonal interný zamestnanec, aj v prípade že Vaša organizácia zvažuje zabezpečenie systematického riešenia KIB pomocou externého dodávateľa.

5 Často kladené otázky

5.1 Prečo chcem pri plnení povinností postupovať podľa normy?

Je pravda, že legislatívne povinnosti sa teoreticky dajú splniť aj inými spôsobmi ako postupom, ktorý navrhujeme. Máme však za to, že nami navrhovaný postup je realizačne najjednoduchším spôsobom, ako zabezpečiť úplnosť riešenia a jeho dlhodobú udržateľnosť. Zároveň poskytuje výraznú výhodu vo forme medzinárodnej kompatibility – kybernetická a informačná bezpečnosť je globálna problematika a pri jednotlivých incidentoch sa veľmi často stierajú deliace čiary medzi lokálnym a medzinárodným incidentom.

5.2 Aké náklady máme zhruba očakávať?

Nakoľko pri KIB ide o priebežnú agendu, ktorá pokrýva celú organizáciu, náklady veľmi výrazne závisia od jej veľkosti a šírky jej činností. Opätovne však zdôrazníme, že cieľom je zavedenie dlhodobého procesu – radšej si nastavte realistickejšie ciele, ktoré však budete vedieť napĺňať, ako jednorazovo spraviť obrovskú akciu v rozsahu, ktorý nebudete vedieť udržiavať a aktualizovať, a ten následne zastaraním úplne stratí relevanciu.

6 Záver

Úloha KIB je zložitá, lebo musí zväčša s obmedzenými zdrojmi spoľahlivo ošetriť množstvo rôznorodých bezpečnostných problémov organizácie. Navrhované riešenia musia byť navyše praktické, spoľahlivé, ucelené, systematické a dlhodobo prevádzkovateľné. Dosiahnutie želaného stavu ochrany je dlhodobou úlohou v horizonte viacerých rokov, jeho udržiavanie a aktualizácia úlohou priebežnou, vyžadujúcou neprestajnú pozornosť. Predstava náročnosti tejto úlohy môže pôsobiť odstrašujúco, obzvlášť ak sa Vaša organizácia tejto oblasti zatiaľ systematicky nevenovala. Ako však hovorí známa taoistická múdrosť, *„Cesta dlhá tisíc míľ začína prvým krokom“*, a našou ambíciou je byť vám na tejto ceste spoľahlivým sprievodcom.