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

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Prvotná orientácia správcu ISVS

1 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*
  - *Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení*
- *Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*
  - *Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy*

Okrem týchto predpisov existuje aj ďalšia legislatíva, ktorú je potrebné zohľadniť pri venovaní sa KIB, tá však bude pre nás podstatná až neskôr. Tento dokument nie je právne záväzný, nejedná sa o náhradu legislatívnych predpisov.

1.1 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 minimálnych bezpečnostných opatrení, do ktorej spadáte. Existujú tri kategórie minimálnych bezpečnostných opatrení, a to:

a) kategória I. minimálnych bezpečnostných opatrení,
b) kategória II. minimálnych bezpečnostných opatrení,
c) kategória III. minimálnych bezpečnostných opatrení.

Nasleduje prehľad kategórií, ich povinností a rozcestník pre relevantné metodické materiály.

1.2 Ktorá kategória sme?

1.2.1 Kategória I minimálnych bezpečnostných opatrení

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

- 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.

1.2.2 Kategória II minimálnych bezpečnostných opatrení

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

- 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 jeho sieť alebo informačný systém do I. alebo II. kategórie v zmysle kategorizácie sietí a informačných systémov
- 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.

1.2.3 Kategória III minimálnych bezpečnostných opatrení

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

- Krajské mesto
- Samosprávny kraj
- Ministerstvo
- Prevádzkovateľ základných služieb podľa Zákona o kybernetickej bezpečnosti, ktorého Vyhláška ku tomuto zákonu kategorizuje jeho sieť alebo informačný systém do III. kategórie v zmysle kategorizácie sietí a informačných systémov
- 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

[1] Okrem Národnej banky Slovenska

- 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 (vyhlášky 179/2020 Z.z.) na tomto mieste.

1.2.4 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 neočakávané výpadky systému, v čase, keď ho na svoju prácu potrebujete najviac (napríklad na konci mesiaca pri povinných uzávierkach). Zároveň keby ste boli 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.** Naplnenie týchto požiadaviek Vám za prijateľné náklady prinesie výrazné zvýšenie úrovne stavu zabezpečenia organizácie. Môžete použiť predpripravené šablóny a metodické postupy, ktoré sú zverejnené na web stránke MIRRI. Vládna jednotka CSIRT.SK vydala metodiku pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, z ktorej je tiež možné čerpať potrebné informácie. Daná metodika je zverejnená na tomto mieste.

2 Zákonné povinnosti podľa kategórií

Povinnosti jednotlivých kategórií určuje Príloha č.2 k Vyhláške č. 179/2020. Nájdete tam špecifický opis jednotlivých povinností. V dokumente *Legislatívne požiadavky* na web stránke MIRRI nájdete prehľadne spísaný zoznam požiadaviek podľa jednotlivých kategórii.

3 Čo mám robiť ako prvé?

Bez ohľadu na kategóriu povinností, ktoré sa na organizáciu vzťahujú, prvé kroky sú vždy rovnaké: Je nutné **získať podporu vedenia** organizácie pre dôležitosť agendy KIB. Výsledkom sú uvoľnené dostatočné zdroje na riadenie, dostatok kompetencií a vôbec aj to, že vedenie sa bude aktívne zúčastňovať na stretnutiach bezpečnostného výboru.

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.

Zjednodušený postup najdôležitejších krokov je možné vyjadriť nasledovne:

- získanie podpory vedenia,
- vymenovanie koordinátora alebo manažéra kybernetickej bezpečnosti,
- vytvorenie bezpečnostného výboru,
- zmapovanie aktív,
- zrealizovanie analýzy rizík,
- popísanie základných procesov,
- zmapovanie kritických dodávateľov
- vytvorenie smerníc a interných riadiacich aktov,
- technické zabezpečenie implementácie bezpečnostných opatrení,
- nastavenie procesov na udržiavanie aktuálnosti prijatých opatrení.

3.1 Aké zdroje potrebujeme?

Nakoľko pri KIB ide o priebežnú agendu, ktorá pokrýva celú organizáciu, zdroje veľmi výrazne závisia od jej veľkosti a rozsahu jej činností. Je potrebné zdôrazniť, že cieľom je zavedenie dlhodobého procesu. Je efektívnejšie mať nastavené realistické ciele, ktoré sa budú dať napĺňať, ako jednorazovo spraviť obrovskú investíciu v rozsahu, ktorý nebude vedieť firma udržiavať a aktualizovať.

4 Záver

Úloha KIB je zložitá, lebo musí zväčša s obmedzenými zdrojmi spoľahlivo ošetriť množstvo rôznorodých bezpečnostných problémov organizácie. Navrhované riešenia musia byť praktické, spoľahlivé, ucelené, efektívne, účinné, transparentné pre používateľov, systematické a dlhodobo prevádzkovateľné. Dosiahnutie želaného stavu ochrany je dlhodobou úlohou v horizonte viacerých rokov, jeho udržiavanie a aktualizácia priebežnou úlohou, vyžadujúcou neustálu 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.