

# Analýza súčasného stavu metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy

Komponent 17  
Reforma č. 4

## Obsah

<b>1 Zoznam použitých skratiek a pojmov .....</b>	<b>4</b>
<b>1.1 Vymedzenie základných pojmov.....</b>	<b>5</b>
<b>2 Manažérske zhrnutie.....</b>	<b>7</b>
<b>3 Súčasný stav metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy .....</b>	<b>9</b>
<b>3.1 Zákon o informačných technológiách vo verejnej správe.....</b>	<b>9</b>
<b>3.1.1 Orgán vedenia a orgán riadenia.....</b>	<b>10</b>
<b>3.1.2 Správca.....</b>	<b>11</b>
<b>3.2 Vyhláška č. 179/2020 Z. z. ....</b>	<b>12</b>
<b>3.3 Zákon o kybernetickej bezpečnosti.....</b>	<b>14</b>
<b>3.3.1 Prevádzkovateľ základnej služby .....</b>	<b>15</b>
<b>3.4 Prehľad dostupných metodík a štandardov .....</b>	<b>17</b>
<b>3.4.1 Metodiky a štandardy vydané MIRRI .....</b>	<b>17</b>
<b>3.4.1.1 Popis zverejnených metodík a štandardov na webovom sídle MIRRI .....</b>	<b>18</b>
<b>3.4.1.2 Čiastkový záver .....</b>	<b>29</b>
<b>3.4.2 Metodiky a štandardy vydané Národným bezpečnostným úradom .....</b>	<b>30</b>
<b>3.4.2.1 Popis zverejnených metodík a štandardov na webovom sídle Národného bezpečnostného úradu .....</b>	<b>32</b>
<b>3.4.2.2 Čiastkový záver .....</b>	<b>32</b>
<b>3.5 Vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike .....</b>	<b>33</b>
<b>3.5.1 Popis zverejnených metodík a štandardov na webovom sídle jednotky CSIRT.SK. ....</b>	<b>35</b>
<b>3.5.2 Čiastkový záver .....</b>	<b>38</b>
<b>3.6 Agentúra Európskej únie pre kybernetickú bezpečnosť .....</b>	<b>38</b>
<b>3.6.1 Čiastkový záver .....</b>	<b>39</b>
<b>3.7 Komparácia legislatívnych požiadaviek s poskytnutými a zverejneným súborom materiálov.....</b>	<b>40</b>
<b>4 Vlastný prieskum metodík a štandardov v oblasti kybernetickej bezpečnosti v prostredí verejnej správy .....</b>	<b>43</b>
<b>4.1 Realizácia vlastného prieskumu.....</b>	<b>43</b>
<b>4.2 Metodika zberu údajov formou online dotazníka.....</b>	<b>44</b>
<b>4.3 Vyhodnotenie vlastného prieskumu.....</b>	<b>45</b>
<b>5 Záver.....</b>	<b>54</b>
<b>5.1 Návrhy a odporúčania .....</b>	<b>56</b>
<b>Zoznam použitých zdrojov.....</b>	<b>58</b>

Detail dokumentu	
Názov dokumentu	Analýza súčasného stavu metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy
Autor dokumentu	KPMG MIRRI (Michal Bartók, Ivan Kopáček, Michal Ďorda, Vladimír Fecko)
Popis dokumentu	Dokument popisuje súčasný stav dokumentov, metodík, štandardov a vzorov dostupných na webových sídlach Ministerstva investícií, regionálneho rozvoja a informatizácie SR, Národného bezpečnostného úradu a Vládnej jednotky CSIRT.SK. Súčasťou tohto dokumentu je vyhodnotenie vlastného prieskumu vykonaného medzi orgánmi verejnej moci s cieľom zistiť rozsah využiteľnosti dostupných materiálov na uvedených webových sídlach. V závere dokumentu je zhrnutie získaných výstupov z analýzy, vlastného prieskumu, na základe ktorých autori tohto dokumentu uvádzajú návrhy a odporúčania na zlepšenie súčasného stavu.
Zodpovedná osoba	Michal Bartók

Verzia	Zmeny	Autor	Dátum
V1.0	N/A – prvá verzia dokumentu na pripomienkovanie	MIRRI, KPMG	12.8.2022
V2.0	Zpracovanie aktuálnych pripomienok MIRRI, drobné štylistické zmeny	KPMG, MIRRI	20.08.2022
V3.0	Zpracovanie dodatočných pripomienok MIRRI a výsledkov dotazníkového prieskumu	KPMG, MIRRI	13.09.2022

## 1 Zoznam použitých skratiek a pojmov

Skratka / Pojem	Vysvetlenie
CSIRT	(Computer Security Incident Response Team Slovakia) je vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike
ENISA	European Network and Information Security Agency
GDPR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
IKT	informačno-komunikačné technológie
IS	Informačný systém
ISVS	informačný systém verejnej správy
IT	informačné technológie
ITVS	informačné technológie vo verejnej správe
JISKB	jednotný informačný systém kybernetickej bezpečnosti
KB	kybernetická bezpečnosť
KCKKB	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
KIB	kybernetická a informačná bezpečnosť
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Nariadenie eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
NBÚ	Národný bezpečnostný úrad
OVM	orgán verejnej moci
SKB	Sekcia kybernetickej bezpečnosti
Smernica NIS	Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
VS	verejná správa
Vyhláška č. 179/2020 Z. z.	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
Vyhláška č. 362/2018 Z. z.	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 o ITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Zákon o KB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

## 1.1 Vymedzenie základných pojmov

*Orgán vedenia* je Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

*Orgán riadenia* je

- a) ministerstvo a ostatný ústredný orgán štátnej správy,
- b) Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán,
- c) obec a vyšší územný celok,
- d) 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 retransmisiiu,
- e) právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),
- f) komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,
- g) osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,
- h) záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.

*Správca* 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.

*Informačná technológia* je prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.

*Informačný systém* je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

*Informačná technológia verejnej správy* je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Povinnosti v rámci správy informačných technológií verejnej správy sa vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe.

*Prevádzkovateľ* je 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.

## 2 Manažérske zhrnutie

Cieľom tejto analýzy je zistenie skutkového stavu momentálne dostupných metodík, ktoré zodpovedajú plneniu požiadaviek legislatívy na implementáciu bezpečnostných opatrení v oblasti kybernetickej a informačnej bezpečnosti, ako aj zavádzanie procesov v oblasti riadenia kybernetickej bezpečnosti. Tieto súbory dokumentov, metodík by mali byť pomôckou pri rozhodovaní, navrhovaní a implementácii procesov riadenia KB a súvisiacich bezpečnostných opatrení.

MIRRI sa ako orgán vedenia (po kapitola 1.3.1) má podieľať a sprístupniť sadu vzorových dokumentov a metodík (viď. Vyhláška č. 179/2020, § 1 Základné ustanovenia, ods. (4):

*„Na splnenie požiadaviek zákona a tejto vyhlášky sa poskytne správcovi súbor materiálov, ktorý obsahuje šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návody, školiace materiály a ukážky.“*

Celková koncepcia legislatívy SR reflektuje na požiadavky EÚ, ktorá prostredníctvom organizácie ENISA a jej nariadení, najmä Smernice NIS (v príprave je smernica NIS2) interpretuje požiadavky na jednotnej úrovne kybernetickej odolnosti jednotlivých členských štátov EÚ ako aj EÚ samotnej.

Ako vyplýva aj z Právnej analýzy súčasného stavu právnej úpravy kybernetickej bezpečnosti v slovenskej republike [6] (samostatný dokument), tieto sú v súčasnosti rozložené na dve hlavné časti – zákon o KB a zákon o ITVS, ktoré svojimi výkonnými vyhláškami definujú požiadavky na tvorbu procesov riadenia KB ako aj implementáciu bezpečnostných opatrení. Pre prevádzkovateľa základnej služby alebo správcu z pohľadu zákona o ITVS je situácia komplikovaná a plnenie požiadaviek kladie zbytočne vysoké nároky na pochopenie a orientáciu v tom, ktoré z požiadaviek a ako je potrebné implementovať. Vyhláška 362 stavia na opatrení na základe kategorizácii informačných systémov a sietí (§ 4 a Príloha č. 2 Vyhlášky č. 362/2018), teda posúdenia dopadových kritérií identifikovaných IS a sietí a určenej kritickosti (najmä na základe dostupnosti, dôvernosti a integrity a ďalších parametrov), pričom vyhláška č. 179/2020 Z. z. zas priamo určuje, ktoré organizácie patria do ktorej z definovaných kategórií (§ 3 Minimálne bezpečnostné opatrenia).

Súčasný stav v implementácii je možné analyzovať aj prostredníctvom Správy o stave KB v SR za 2021 vydanéj NBÚ. Táto sa však zameriava primárne a logicky na plnenie požiadaviek zákona o KB a súvisiacich vyhlášok. Taktiež hovorí iba o stave tých organizácií, ktoré audit KB absolvovali (certifikovaným audítorom, niektoré samohodnotením).

Stav implementácie bezpečnostných opatrení interpretuje celkovú alebo čiastkovú mieru kybernetickej odolnosti, ale taktiež v určitej miere napovedá o miere pochopenia a využitia sprístupnených metodík a vzorových dokumentov.

Taktiež Nariadenie GDPR zaoberajúce sa právnou úpravou ochrany osobných údajov v EÚ priamo nariaďuje prevádzkovateľovi (z pohľadu GDPR) prijať špecifické bezpečnostné opatrenia na ochranu informácií, ktoré sú klasifikované ako osobný údaj, napríklad recitál (78) nariadenia č. 2016/679 GDPR:

*„Na to, aby mohol prevádzkovateľ preukázať súlad s týmto nariadením, by mal prijať interné pravidlá a prijať opatrenia, ktoré budú predovšetkým spĺňať zásady špecificky navrhutej ochrany údajov a štandardnej ochrany údajov. Takéto opatrenia by mohli okrem iného pozostávať z minimalizácie spracúvania osobných údajov, čo najskoršej pseudonymizácie osobných údajov, transparentnosti v súvislosti s funkciami a spracúvaním osobných údajov, umožnenia dotknutým osobám monitorovať spracúvanie údajov, umožnenia prevádzkovateľovi vypracovať a zlepšiť bezpečnostné prvky.“*

Kombinácia týchto prístupov predstavuje z pohľadu zástupcov OVM zodpovedných za riešenie súladu a zabezpečenie plnenia legislatívnych požiadaviek ako aj implementácie bezpečnostných opatrení vyplývajúcich z požiadaviek bežnej praxe, bezpečnostných analýz, analýz rizík a rôznych typov bezpečnostných testov veľmi komplikovanú situáciu, v ktorej sa priamo pýta potreba štruktúrovania a sprehľadnenia legislatívnych požiadaviek sumarizovaných do jednotlivých kategórií OVM.



### 3 Súčasný stav metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy

Informatizácia verejnej správy je riadený proces, ktorý sa realizuje v rámci celej štruktúry verejnej správy. Je to proces vytvárania spoločenských, legislatívnych, metodických, technologických a organizačno-personálnych podmienok pre efektívnu aplikáciu informačných technológií (ďalej len „IT“) vo výkone verejnej správy, ako aj riadený proces vlastnej aplikácie IT.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“) a Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB“) a ich vykonávacie predpisy ukladajú tak správcom informačných systémov verejnej správy (ďalej len „ISVS“) ako aj prevádzkovateľom základnej služby povinnosť prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov, resp. prijať a dodržiavať primerané bezpečnostné opatrenia s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovania vplyvov kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné určené pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifik kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

Za účelom splnenia požiadaviek uvedených zákonov a ich vykonávacích predpisov, ako aj správnej implementácie bezpečnostných opatrení sa má poskytnúť správcom ISVS či prevádzkovateľom základnej služby súbor materiálov obsahujúci šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy či štandardy a metodiky. Táto povinnosť je určená orgánu vedenia, ktorým je podľa zákona o ITVS Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (ďalej len „MIRRI“) a Národný bezpečnostný úrad (ďalej len „NBÚ“) podľa zákona o KB.

#### 3.1 Zákon o informačných technológiách vo verejnej správe

Zákon o ITVS je všeobecným právnym predpisom, ktorý upravuje organizáciu správy ITVS, práva a povinnosti orgánu vedenia a orgánu riadenia a stanovuje základné požiadavky kladené na ITVS a ich správu.

Cieľom zákona o ITVS je zvýšenie miery informatizácie spoločnosti, zefektívnenie výkonu verejnej správy a zabezpečenie jej sprístupnenia verejnosti prostredníctvom moderných technológií a metód. Zavádza systémovú zmenu, ktorá sa týka hlavne rozšírenia povinností pre jednotlivé inštitúcie verejnej správy v oblasti správy, t. j. vedenia a riadenia IT, a to od samotného plánovania, obstarania, implementáciu IT, až po monitoring a hodnotenie IT.

### 3.1.1 Orgán vedenia a orgán riadenia

Podľa zákona o ITVS správu informačných technológií vo verejnej správe (ďalej len „ITVS“ vykonávajú

- a) orgán vedenia, ktorým je MIRRI,
- b) orgán riadenia vo vzťahu k ITVS v jeho pôsobnosti.

Orgán vedenia a orgán riadenia sú v správe ITVS povinné

- a) dodržiavať princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti,
- b) postupovať tak, aby vynaložené náklady na IT boli primerané ich kvalite,
- c) prednostne využívať už existujúce IT, alebo IT určené na spoločné využitie viacerých orgánov riadenia, ak to nie je v rozpore s povinnosťami podľa písmena a) alebo písmena b) a ak to umožňujú technické možnosti a bezpečnostné požiadavky,
- d) dbať na vytvorenie integrovaného prostredia ITVS na základe spoločných princípov definovaných v štandardoch a Národnej koncepcii informatizácie verejnej správy Slovenskej republiky, s cieľom jednotného výkonu úloh podľa osobitných predpisov.

Orgán vedenia a orgán riadenia využívajú v správe ITVS podnety a poznatky odbornej verejnosti a prihládajú na spoločenské potreby používateľov služieb verejnej správy (ďalej len „VS“), služieb vo verejnom záujme alebo verejných služieb.

MIRRI ako orgán vedenia, vykonáva, okrem iných, aj tieto činnosti

- a) monitoruje výkon riadenia v správe ITVS na účely sledovania aktuálneho stavu v správe ITVS a ich vývoji a sledovania spôsobov a postupov pri vykonávaní tejto správy,
- b) vyhodnocuje informácie získané z monitorovania, kontroly a z iných podnetov na účely identifikácie rizík a nedostatkov v ITVS,
- c) vydáva metodické usmernenia, usmerňuje a koordinuje orgány riadenia na účely jednotného spôsobu výkonu riadenia v správe ITVS a centrálného riadenia informatizácie spoločnosti,
- d) vydáva štandardy a výkladové stanoviská,
- e) zverejňuje na ústrednom portáli rozhodnutia, iné dokumenty a informácie týkajúce sa ITVS a informatizácie VS.

Orgán riadenia je povinný poskytovať orgánu vedenia súčinnosť potrebnú na riadny výkon vedenia v správe ITVS a poskytovať mu prostredníctvom elektronickej služby VS údaje o ITVS na účely štatistických analýz.

MIRRI vyplýva zo zákona o ITVS povinnosť:

- vydávať metodické usmernenia, usmerňovať a koordinovať orgány riadenia na účely jednotného spôsobu výkonu riadenia v správe informačných technológií verejnej správy a centrálneho riadenia informatizácie spoločnosti,
- vydávať štandardy a výkladové stanoviská,
- zverejňovať na ústrednom portáli rozhodnutia, iné dokumenty a informácie týkajúce sa informačných technológií verejnej správy a informatizácie verejnej správy.

### 3.1.2 Správca

Správca je na úseku plánovania a organizácie ITVS povinný

- a) nastaviť systém riadenia,
- b) určiť stratégiu rozvoja a riadenia,
- c) zabezpečiť riadenie správy architektúry,
- d) nastaviť organizačnú štruktúru, procesy a nástroje potrebné na riadenie,
- e) zabezpečiť riadenie kľúčových zdrojov, ktorými sú ľudské zdroje, finančné prostriedky alebo zdroje poskytované inými osobami,
- f) riadiť nastavenie zmluvných vzťahov pre poskytovanie služieb,
- g) zabezpečiť riadenie kvality,
- h) zabezpečiť riadenie rizík,
- i) zabezpečiť riadenie bezpečnosti.

V rámci nastavenia systému riadenia je správca povinný vydať vnútorný predpis pre systém riadenia ITVS.

V rámci nastavenia organizačnej štruktúry, procesov a nástrojov potrebných na riadenie je správca povinný zabezpečiť také organizačné podmienky a procesné podmienky, aby zabezpečil riadny výkon povinností pri riadení ITVS a realizoval určené strategické ciele.

V rámci zabezpečenia riadenia kvality je správca povinný vydať vnútorný predpis pre riadenie kvality a v rámci zabezpečenia riadenia rizík je správca povinný vydať vnútorný predpis pre riadenie rizík.

Podľa zákona o ITVS je správca povinný plniť úlohy na úsekoch:

- a) plánovania a organizácie ITVS,
- b) obstarávania a implementácie ITVS,
- c) prevádzky, servisu a podpory ITVS,
- d) monitoringu a hodnotenia ITVS.

V prípade, že je správca prevádzkovateľom základnej služby podľa zákona o KB je ďalej povinný prijať a realizovať bezpečnostné opatrenia vo vzťahu k ISVS v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov.

Správca je ďalej povinný ďalej zabezpečiť

- a) bezpečnosť ITVS v oblasti plánovania a organizácie,
- b) bezpečnosť ITVS v oblasti obstarávania a implementácie,
- c) bezpečnosť ITVS v oblasti prevádzky, servisu a podpory,
- d) bezpečnosť ITVS v oblasti monitoringu a hodnotenia.

Medzi ďalšie povinnosti správcu patrí aj vypracúvanie bezpečnostného projektu ISVS. Vypracovanie bezpečnostného projektu ISVS zabezpečí správca, vychádzajúc:

- a) z bezpečnostnej stratégie kybernetickej bezpečnosti a bezpečnostných politík,
- b) zo všeobecne akceptovaných štandardov riadenia IT, ktoré vychádzajú z uznaných technických noriem,
- c) z metodických usmernení orgánu vedenia.

Podrobnosti o obsahu a štruktúre bezpečnostného projektu upravuje 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 (ďalej len „vyhláška č. 179/2020 Z. z.“).

### 3.2 Vyhláška č. 179/2020 Z. z.

Vyhláška č. 179/2020 Z. z. upravuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu. Upravuje tiež podrobnosti o bezpečnosti ITVS rozpracované v zákone o ITVS a v zákone o KB a povinnosti správcu vo vzťahu k ITVS. Správca je povinný identifikovať a udržiavať svoj zoznam aktív a je povinný realizovať bezpečnostné opatrenia aspoň na úrovni minimálnych požadovaných bezpečnostných opatrení danej kategórie.

Bezpečnostné opatrenia ITVS sú tvorené minimálnymi bezpečnostnými opatreniami troch úrovní, a to Kategóriou I, Kategóriou II a Kategóriou III. Minimálne bezpečnostné opatrenia troch úrovní z jednotlivých oblastí kybernetickej a informačnej bezpečnosti sú bližšie špecifikované v prílohe č. 2 vyhlášky č. 179/2020 Z. z. V prípade, keď dôjde k duplicite či redundancii bez stanoveného účelu, alebo k nekompatibilite minimálnych bezpečnostných opatrení rôznych úrovní, ktoré majú byť aplikované na konkrétne ITVS, majú prednosť ustanovenia, ktoré upravujú opatrenia vyššej úrovne (§ 2 ods. 2 vyhlášky č. 179/2020 Z. z.).

Vyhláška č. 179/2020 Z. z. ustanovuje

- a) kategórie ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov,

- b) podrobnosti o bezpečnosti ITVS, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsahu bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov.

Aktíva ITVS sa identifikujú a udržiavajú podľa prílohy č. 1 vyhlášky č. 179/2020 Z. z. so zreteľom na ich nedostupnosť alebo zníženú kvalitu, ktoré môžu mať zásadný vplyv na poskytovanie služieb VS, služieb vo verejnom záujme alebo verejných služieb.

Vo vzťahu k ITVS sú realizované bezpečnostné opatrenia aspoň na úrovni minimálnych bezpečnostných opatrení danej kategórie.

V zmysle ustanovenia §1, ods. 4 Vyhlášky č. 179/2020 Z. z. MIRRI ako príslušný ústredný orgán „na splnenie požiadaviek zákona a tejto vyhlášky poskytne správcovi súbor materiálov, ktorý obsahuje šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návody, školiace materiály a ukážky“.

### ***Bezpečnostný projekt pre informačné systémy verejnej správy***

Medzi ďalšie povinnosti správcu patrí aj vypracúvanie bezpečnostného projektu informačné systémy verejnej správy (ďalej len „ISVS“), a to v súlade s vyhláškou č. 179/2020 Z. z. a tvorí súčasť bezpečnostnej dokumentácie.

Správca vypracuje bezpečnostný projekt pre ISVS, ktorý:

- a) pri narušení bezpečnosti môže spôsobiť závažný kybernetický bezpečnostný incident,
- b) tvorí základné registre alebo referenčné registre alebo je ich súčasťou,
- c) je agendový informačný systém,
- d) je nevyhnutný na rozhodovanie orgánu verejnej moci (ďalej len „OVM“),
- e) je špecializovaný portál,
- f) spracúva osobitné kategórie osobných údajov podľa osobitného predpisu,
- g) je zaradený do kategórie III. podľa vyhlášky č. 179/2020 Z. z.

Rozsah vypracovania a implementácie bezpečnostného projektu pre ISVS je upravený v prílohe č. 3 vyhlášky č. 179/2020 Z. z. Príloha č. 3 predpisuje obsah a štruktúru tohto bezpečnostného projektu. Bezpečnostný projekt ISVS pozostáva z dvoch hlavných výstupov:

- bezpečnostného zámeru a
- analýzy bezpečnosti.

Jednotlivé výstupy vznikajú v určenom poradí a sú priebežne aktualizované počas celého projektu ISVS realizovaného v súlade so zákonom o ITVS. Samotná finalizácia dokumentácie bezpečnostného projektu ISVS je realizovaná v etape implementácie a testovania podľa zákona o ITVS.

Prvým výstupom bezpečnostného projektu ISVS je dokument Bezpečnostný zámer. Hlavným výstupom bezpečnostného projektu ISVS je dokument Analýza bezpečnosti, ktorého súčasťou je kvalitatívna analýza rizík. Analýza rizík je zameraná na získanie poznatkov o pravdepodobných rizikách týkajúcich sa aktív ISVS a jeho okolia.

### 3.3 Zákon o kybernetickej bezpečnosti

Dňa 1. apríla 2018 nadobudol účinnosť zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB“), ktorý komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NIS).

Podľa zákona o KB NBÚ, okrem iných, plní aj tieto úlohy

- a) riadi a koordinuje výkon štátnej správy,
- b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,
- c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,
- d) vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,
- e) je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy,
- f) plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
- g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,
- h) v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie Severoatlantickej zmluvy,
- i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,
- j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti (ďalej len „JISKB) atď.



Na účely zabezpečenia plnenia úloh podľa zákona môže NBÚ na účel zabezpečenia KB uzatvoriť písomnú dohodu o spolupráci a o výmene informácií a podkladov s OVM alebo s inou právnickou osobou. Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.

JISKB obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. JISKB pozostáva z verejnej časti a neverejnej časti a prístup k nemu je bezodplatný. Verejná časť jednotného informačného systému kybernetickej bezpečnosti (ďalej len „JISKB“) obsahuje

- a) register ústredných orgánov,
- b) zoznam základných služieb,
- c) register prevádzkovateľov základných služieb,
- d) zoznam digitálnych služieb,
- e) register poskytovateľov digitálnych služieb,
- f) register kybernetických bezpečnostných incidentov,
- g) zoznam akreditovaných jednotiek CSIRT,
- h) metodiky, usmernenia, štandardy, politiky a oznamy,
- i) informácie a údaje potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,
- j) výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu.

Medzi činnosti NBÚ patrí:

- určovanie štandardov, operačných postupov, vydávanie metodiky a politiky správania sa v kybernetickom priestore,
- zverejňuje metodiky, usmernenia, štandardy, politiky a oznamy vo verejnej časti jednotného informačného systému kybernetickej bezpečnosti.

### 3.3.1 Prevádzkovateľ základnej služby

Podľa zákona o KB je Prevádzkovateľ základnej služby povinný

- do 12 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia, ak sú prijaté,
- pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík; povinnosť uzatvoriť zmluvu neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí

s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke,

- informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným, ak NBÚ nerozhodne inak; povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, NBÚ v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov.

Prevádzkovateľ základnej služby je ďalej povinný

- riešiť kybernetický bezpečnostný incident,
- bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
- spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
- v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
- oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosť, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,
- hlásiť zmeny v údajoch do 30 dní odo dňa ich vzniku prostredníctvom JISKB.

Prevádzkovateľ základnej služby, ako už bolo uvedené, je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 zákona o KB a sektorové bezpečnostné opatrenia, ak sú prijaté. Bezpečnostnými opatreniami sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia sú spresnené vyhláškou NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, a to

- Obsah a štruktúra bezpečnostnej dokumentácie;
- Bezpečnostná stratégia kybernetickej bezpečnosti;
- Klasifikácia informácií a kategorizácia sietí a informačných systémov;
- Bezpečnostné opatrenia pre oblasť
  - organizácie kybernetickej bezpečnosti a informačnej bezpečnosti;
  - riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti;
  - personálnej bezpečnosti;
  - riadenia prístupov;



- riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami;
- bezpečnosti pri prevádzke informačných systémov a sietí;
- hodnotenia zraniteľností a bezpečnostných aktualizácií;
- ochrany proti škodlivému kódu;
- sieťovej a komunikačnej bezpečnosti;
- akvizície, vývoja a údržby informačných sietí a informačných systémov;
- zaznamenávania udalostí a monitorovania;
- fyzickej bezpečnosti a bezpečnosti prostredia;
- riešenia kybernetických bezpečnostných incidentov;
- kryptografických opatrení;
- kontinuity prevádzky;
- auditu, riadenia súladu a kontrolných činností.

### 3.4 Prehľad dostupných metodík a štandardov

Cieľom tejto časti dokumentu je poskytnúť prehľad dostupného súboru materiálov pre správcov a prevádzkovateľov základnej služby.

#### 3.4.1 Metodiky a štandardy vydané MIRRI

MIRRI na pomoc správcovi ISVS, ale aj ostatným záujemcom, vydalo sériu metodických materiálov, ktoré vypracovali odborníci dlhodobo pôsobiaci v oblasti informačnej a kybernetickej bezpečnosti a zverejnilo ich na svojom webovom sídle, časť Informatizácia – Kybernetická bezpečnosť, metodiky, ktorých cieľom je usmerniť OVM pri vypracúvaní bezpečnostnej dokumentácie.

Podľa informácií uvedených na webovom sídle MIRRI, na tvorbe týchto dokumentov spolupracovali pracovníci Sekcie kybernetickej bezpečnosti (ďalej len „SKB“) MIRRI vrátane externých expertov SKB MIRRI a pracovníkov z akademickej sféry. Pri tvorbe predmetnej dokumentácie autori vychádzali z best practices, legislatívnych materiálov a medzinárodných noriem v oblasti informačnej a kybernetickej bezpečnosti.

Špecifickou oblasťou bola tvorba dokumentácie pre subjekty spadajúce do kategórie I minimálnych bezpečnostných opatrení. Súčasťou prác bola úzka spolupráca so starostom obce Bánov, okr. Nové Zámky, ktorý paralelne koordinoval spoluprácu so starostami ďalších obcí v okolí s cieľom priebežne overovať zrozumiteľnosť a použiteľnosť vytváraných materiálov. Spoločným cieľom bolo vytvoriť dokumentáciu, ktorá bude pre malé obce a organizácie nápomocná, nekomplikovaná a bude ich podporovať pri plnení legislatívnych požiadaviek v oblasti kybernetickej a informačnej bezpečnosti.

Ďalej sa uvádza, že Vytvorené vzory a šablóny nie sú povinné na ich použitie, ani nie sú záväzné. Sú poskytnuté voľne a bezplatne, na využitie podľa potrieb konkrétnej organizácie. Vytvorené dokumenty majú aj svoj metodický rozmer, takže je ich možné použiť i

pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Všetky dokumenty sú očíslované podľa nasledovného kľúča: KIB-KX-Y. KB označuje dokumentáciu v oblasti kybernetickej a informačnej bezpečnosti, KX znamená kategóriu minimálnych bezpečnostných opatrení I, II, III a Y znamená poradové číslo dokumentu. Pre lepšiu prehľadnosť je uvedený aj názov dokumentu a jeho aktuálna verzia (odkaz na zdroj je uvedený v prílohe č. 1 tohoto dokumentu).

Metodiky/vzory/šablóny sú rozdelené podľa kategórií nasledujúco:

1. Úvodné materiály pre všetky kategórie
  - a) KB-K1\_2\_3 Prvotná orientácia správcu ISVS,
  - b) KB-K1\_2\_3 Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník,
  - c) KB-K1\_2\_3 Legislatívne požiadavky pre všetky kategórie podľa vyhlášky 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
  - d) KB-K1\_2\_3 Výber dodávateľa služieb kybernetickej bezpečnosti Návod pre obce a mestá v piatich krokoch (vydané KCCKB),
  - e) KB-K1\_2\_3 Vzorová smernica o riadení dodávateľských vzťahov.
2. Metodiky pre minimálne bezpečnostné opatrenia kategórie I
  - a) KB-K1-1 Check list pre subjekty kategórie I podľa vyhlášky 179/2020,
  - b) KB-K1-2 Politika kybernetickej bezpečnosti a informačnej bezpečnosti,
  - c) KB-K1-3 Metodika pre spracovanie analýzy rizík pre minimálne bezpečnostné opatrenia kategórie I.,
  - d) KB-K1-4 Manuál bezpečnosti objektu,
  - e) KB-K1-5 Plán rozvoja bezpečnostného povedomia.
3. Metodiky pre minimálne bezpečnostné opatrenia kategórie II a III
  - a) KB-K2\_3-1 Povinnosti správcu ISVS v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní,
  - b) KB-K2\_3-2 Stratégia kybernetickej a informačnej bezpečnosti pre II. a III. kategóriu ISVS,
  - c) KB-K2\_3-3 Čo má obsahovať Politika kybernetickej a informačnej bezpečnosti pre II. a III. kategóriu ISVS a ako ju vypracovať,
  - d) KB-K2\_3-4 Špecifikácia obsahu špeciálnych bezpečnostných politík 2. úrovne,
  - e) KB-K2\_3-6 Plán Kontinuity činností BCP – Business Continuity Plan,
  - f) KB-K2\_3-7 Plán obnovy činností IS DRP – Disaster Recovery Plan,
  - g) KB-K2\_3-8 Pracovná náplň Manažéra kybernetickej a informačnej bezpečnosti,
  - h) KB-K2\_3-9 Bezpečnostný projekt (metodika spracovania bezpečnostného projektu).

#### 3.4.1.1 Popis zverejnených metodík a štandardov na webovom sídle MIRRI

## **1. Úvodné materiály pre všetky kategórie**

### **a) KB-K1\_2\_3 Prvotná orientácia správcu ISVS**

Tento dokument má poskytnúť prehľad o povinnostiach organizácie vyplývajúcich zo zákona o KB a prislúchajúcich vyhlášok. (Rozsah dokumentu 5 s.)

*Štruktúra dokumentu:*

1. Má naša organizácia zákonné povinnosti súvisiace s kybernetickou bezpečnosťou? – stručne popisuje dva zákony a k nim prislúchajúce vyhlášky;
2. Kategórie ITVS – stručne uvádza tri kategórie minimálnych bezpečnostných opatrení;
3. Ktorá kategória sme? – popisuje kritériá, na základe ktorých sa organizácia dokáže zaradiť do príslušnej kategórie I, II alebo III a tiež, ako má organizácia postupovať v prípade, že nespadá do žiadnej z uvedených kategórií;
4. Zákonné povinnosti podľa kategórií – odvoláva sa na Prílohu č. 2 k Vyhláške č. 179/2020 Z. z.;
5. Čo mám robiť ako prvé? – stručne odporúča, ktoré kroky je potrebné vykonať bez ohľadu na to, do ktorej kategórie organizácia spadá;
6. Aké zdroje potrebujeme? – stručne uvádza, že zdroje závisia od veľkosti organizácie a rozsahu jej činností;
7. Záver.

### **b) KB-K1\_2\_3 Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník**

Tento dokument má predstavovať úvod do informačnej a kybernetickej bezpečnosti pre laikov, ktorí sa zatiaľ s touto problematikou nestretli. Cieľom tohto textu je pomôcť čitateľovi zorientovať sa v problematike informačnej a kybernetickej bezpečnosti a vytvoriť si aspoň rámcovú predstavu o cieľoch a problémoch, ktoré táto disciplína rieši. (Rozsah dokumentu 30 s.)

V informačnej a kybernetickej bezpečnosti sa používa množstvo špecifických odborných termínov, ktoré sa často používajú bez predchádzajúceho vysvetlenia a ešte aj v rozličných významoch.

Na objasnenie najpodstatnejších pojmov sa v tomto dokumente nachádza aj Malý výkladový slovník termínov. Medzinárodná terminológia informačnej bezpečnosti je anglická, slovenská odborná verejnosť používa medzinárodnú terminológiu a len málo anglických termínov je adekvátne preložených do slovenčiny. Preto je tento slovník postavený ako výkladový a nie terminologický.

*Štruktúra dokumentu:*

Dokument je rozdelený na dve časti:

1. Úvod do kybernetickej a informačnej bezpečnosti – popisuje, čo je kybernetická bezpečnosť, kybernetické prostredie SR a základ terminológie;
2. Malý výkladový slovník termínov kybernetickej a informačnej bezpečnosti – obsahuje 290 termínov s výkladom abecedne zoradených.

**c) KB-K1\_2\_3 Legislatívne požiadavky pre všetky kategórie podľa vyhlášky č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy**

Tento dokument popisuje zákonné povinnosti organizácie podľa kategórií I, II a III a špecifický opis jednotlivých povinností. (Rozsah dokumentu 25 s.)

*Štruktúra dokumentu*

1. Zákonné povinnosti podľa kategórií;
2. Povinnosti I. kategórie;
3. Povinnosti II. Kategórie;
4. Povinnosti III. Kategórie.

**d) KB-K1\_2\_3 Výber dodávateľa služieb kybernetickej bezpečnosti: Návod pre obce a mestá v piatich krokoch (vydané KCCKB)**

Tento dokument poskytuje návod pre organizácie, ako pristupovať k výberu dodávateľa služieb kybernetickej bezpečnosti a ktoré aspekty je potrebné brať do úvahy a čoho by sa organizácie mali vyvarovať. (Rozsah dokumentu 4 s.)

*Štruktúra dokumentu*

1. Zodpovednosť štatutára;
2. Zmluva s dodávateľom služieb;
3. Typy služieb;
4. Prvý kontakt s potenciálnym dodávateľom;
5. Analýza rizík ako súčasť ponuky;
6. Technické znalosti dodávateľa;
7. Preukázateľná odbornosť tímu dodávateľa;
8. Prax v odbore;
9. Príloha č. 1 - Kvalifikačné požiadavky – uvádza minimálne požiadavky na úroveň vzdelania a prax profesionála, ktorý poskytuje služby manažéra kybernetickej bezpečnosti;
10. Príloha č. 2 - Zoznam odborných certifikátov – uvádza zoznam certifikátov, ktorými tím dodávateľa preukáže odbornú spôsobilosť

**e) KB-K1\_2\_3 Vzorová smernica o riadení dodávateľských vzťahov**

Cieľom vzorovej smernice je konsolidácia zmluvných vzťahov s tretími stranami v oblasti kybernetickej bezpečnosti v organizácii. Tento dokument reflektuje pravidlá a postupy v oblasti riadenia dodávateľských vzťahov v bežnej organizácii v kontexte bezpečnostných pravidiel, definovaných v platnej legislatíve v oblasti riadenia kybernetickej bezpečnosti. Vzorovú smernicu je potrebné upraviť na základe špecifických potrieb organizácie. (Rozsah dokumentu 5 s.)

*Štruktúra dokumentu*

1. Základné ustanovenie;
2. Riadenie dodávateľských vzťahov;
3. Zmluvy s tretími stranami;
4. Audit a kontrolné činnosti.

**2. Metodiky pre minimálne bezpečnostné opatrenia kategórie I**

**a) KB-K1-1 Check list pre subjekty kategórie I podľa vyhlášky č. 179/2020**

Tento dokument umožní organizácii zistiť základný stav bezpečnosti IT systémov. Pomocou checklistu je možné odhaliť nedostatky zabezpečenia IT systémov, na základe ktorých ich viete odstrániť. V prípade, že ste zaznamenali podozrivú aktivitu na Vašich zariadeniach alebo v informačnom systéme, obráťte sa na Vládnu jednotu CSIRT.

Pomocou checklistu bude organizácia schopná odhaliť nedostatky zabezpečenia IT systémov, na základe ktorých ich bude vedieť odstrániť. V prípade, že zaznamenala podozrivú aktivitu na jej zariadeniach alebo v informačnom systéme, je organizácii odporúčané, aby sa obrátila na Vládnu jednotu CSIRT. (Rozsah dokumentu 5 s.)

*Štruktúra dokumentu*

Dokument je koncipovaný do formy tabuľky a členený podľa oblastí:

1. Operačný systém;
2. Tvorba a uchovávanie hesiel;
3. Bezpečnosť dát;
4. Bezpečnosť aplikácií;
5. Bezpečnosť na internete;
6. Sieťová bezpečnosť.

Ku každej z oblastí sú priradené „odporúčania“ s checkboxom, či je odporúčanie splnené.

**b) KB-K1-2 Politika kybernetickej bezpečnosti a informačnej bezpečnosti**

Tento vzor politiky informačnej a kybernetickej bezpečnosti obsahuje minimálne bezpečnostné opatrenia pre Kategóriu I v zmysle ustanovenia § 3, ods. 2 Vyhlášky č. 179/2020 Z. z. Vzor je vypracovaný tak, že prostredníctvom Znak [●] v žltom poli alebo

text v žltom poli, si organizácia na toto miesto doplní relevantné údaje. (Rozsah dokumentu 10 s.)

#### *Štruktúra dokumentu*

1. Základné ustanovenia;
2. Organizácia kybernetickej bezpečnosti;
3. Riadenie rizík kybernetickej bezpečnosti;
4. Personálna bezpečnosť;
5. Riadenie prístupov;
6. Riadenie kybernetickej bezpečnosti vo vzťahoch s tretími stranami;
7. Bezpečnosť pri prevádzke informačných systémov a sietí;
8. Hodnotenie zraniteľností a bezpečnostné aktualizácie;
9. Ochrana proti škodlivému kódu;
10. Sieťová a komunikačná bezpečnosť;
11. Akvizícia, vývoj a údržba informačných technológií verejnej správy;
12. Zaznamenávanie udalostí a monitorovanie;
13. Fyzická bezpečnosť a bezpečnosť prostredia;
14. Riešenie kybernetických bezpečnostných incidentov;
15. Kryptografické opatrenia;
16. Audit a kontrolné činnosti.

#### **c) KB-K1-3 Metodika pre spracovanie analýzy rizík pre minimálne bezpečnostné opatrenia kategórie I.**

Táto metodika určená pre spracovanie analýzy rizík (formát .xlsx) je určená pre organizácie, implementujúce minimálne bezpečnostné opatrenia kategórie I. Pre spracovanie tejto analýzy rizík je aplikovaný prístup skúmania scenárov rizík kybernetickej bezpečnosti, a teda skúmania akéhokoľvek súhrnu udalostí, ktoré môžu nastať s určitou pravdepodobnosťou a spôsobiť negatívny dopad.

Ako úplne prvý krok pri skúmaní aktuálneho stavu kybernetickej a informačnej bezpečnosti odporúčame vykonať rámcové sebaposúdenie. Pre tento účel je vytvorený samostatný dokument vo formáte PDF s názvom "Check list pre subjekty kategórie I podľa vyhlášky 179/2020".

Táto metodika je pracovný nástroj, určený pre opis postupu spracovania analýzy rizík. Obsahuje postupy a definuje pravidlá pre jednotlivé kroky práce s týmto dokumentom.

Vzhľadom na minimálne bezpečnostné opatrenia kategórie I. a náročnosť predmetnej oblasti z pohľadu personálnych zdrojov pre subjekty / organizácie spadajúcej do kategórie I., je tento dokument spracovaný ako šablóna zahŕňajúca najvýznamnejšie scenáre rizík a opatrenia na ich zníženie. Zdrojmi pre tvorbu tohto dokumentu sú odborná verejnosť, akademický sektor i pracovníci Sekcie kybernetickej bezpečnosti MIRRI.

#### *Štruktúra dokumentu*

Celý dokument je zložený z nasledovných hárkov, pričom pri jeho vyplňaní je potrebné dodržať tu uvedený chronologický postup:

- a) Metodika – v tomto hárku je uvedená táto metodika ako návod na vyplnenie tohto dokumentu.
- b) Titulka – je to titulná strana celého dokumentu, kde organizácia uvedie svoje základné údaje, svoje očíslovanie dokumentu, ako aj osoby, ktoré sú v organizácii zodpovedné za bezpečnostnú dokumentáciu. Súčasťou tohto hárku je aj časť „Zmenový list“, v ktorej sa uvedú prípadné zmeny alebo revízie tohto dokumentu.
- c) Zoznam aktív – tu je uvedený predbežný zoznam kategórií aktív (teda toho, čo má pre organizáciu hodnotu) a predbežný zoznam konkrétnych aktív v organizácii. Tento zoznam je možné doplniť podľa potreby.

Organizácia tak získa zoznam aktív vo svojej organizácii a zoznam zodpovedných osôb.

#### **d) KB-K1-4 Manuál bezpečnosti objektu**

Tento vzor obsahuje minimálne bezpečnostné opatrenia pre Kategóriu I v zmysle ustanovenia § 3, ods. 2 Vyhlášky č. 179/2020 Z. z. Vzor je vypracovaný tak, že prostredníctvom Znak [●] v žltom poli alebo text v žltom poli, si organizácia na toto miesto doplní relevantné údaje. (Rozsah dokumentu 4 s.)

#### *Štruktúra dokumentu*

- 1. Účel dokumentu;
- 2. Rozsah platnosti;
- 3. Právomoci a zodpovednosť;
- 4. Fyzická bezpečnosť a bezpečnosť prostredia (zabezpečenie oblasti; bezpečnosť zariadení).

#### **e) KB-K1-5 Plán rozvoja bezpečnostného povedomia**

Tento vzor obsahuje minimálne bezpečnostné opatrenia pre Kategóriu I v zmysle ustanovenia § 3, ods. 2 Vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS. Vzor je vypracovaný tak, že prostredníctvom Znak [●] v žltom poli alebo text v žltom poli, si organizácia na toto miesto doplní relevantné údaje. (Rozsah dokumentu 4 s.)

#### *Štruktúra dokumentu*

- 1. Úvod;
- 2. Ciele bezpečnostného školenia;
- 3. Program a plán školení v rámci rozvoja bezpečnostného povedomia (tabuľka);



4. Hodnotenie účinnosti školení v rámci rozvoja bezpečnostného povedomia (tabuľka).

### **3. Metodiky pre minimálne bezpečnostné opatrenia kategórie II a III**

#### **a) KB-K2\_3-1 Povinnosti správcu ISVS v oblasti kybernetickej a informačnej bezpečnosti a postup pri ich napĺňaní**

Tento dokument vychádza z právnych predpisov, a to zákona o KB, vyhlášky č. 362/2018 Z. z., zákona o ITVS a príslušnej vyhlášky č. 179/2020 Z. z., ktoré vyžadujú od správcu ISVS II. a III. kategórie zaviesť v organizácii systém riadenia informačnej bezpečnosti. Cieľom tohto dokumentu je pomôcť vybudovať systém KIB tak, aby bol v súlade s uvedenou legislatívou 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. (Rozsah dokumentu 11 s.)

#### *Štruktúra dokumentu*

1. Povinnosti správcu ISVS – vymedzuje dva základné pojmy, a to „Správca“ a „Prevádzkovateľ“;
2. Základné kroky/opatrenia (podpora vedenia organizácie, vymenovanie manažéra KIB) - uvádza postupnosť krokov na zavedenie KIB podľa platnej legislatívy, význam podpory vedenia organizácie a vymenovanie manažéra KIB s uvedením prehľadu jeho zodpovedností a právomocí;
3. Nadefinovanie bezpečnostných cieľov – poskytuje prístup k správnej formulácii cieľov s vymenovaním možných všeobecných bezpečnostných cieľov organizácie;
4. Vytvorenie bezpečnostnej stratégie a celej koncepcie riadenia kybernetickej bezpečnosti – stručne uvádza význam stratégie KIB, poskytuje organizácii súbor otázok, na ktoré by mala vedieť zodpovedať pri stanovovaní bezpečnostných požiadaviek na činnosti, ktoré organizácia vykonáva;
5. Vytvorenie bezpečnostnej politiky – stručne popisuje, čo je bezpečnostná politika a ako sa ďalej rozpracúva;
6. Vytvorenie interných predpisov alebo smerníc – vymenúva oblasti/rozsah, pre ktoré sa vytvárajú interné predpisy alebo smernice;
7. Vybudovanie organizačného útvaru KIB – spresňuje bezpečnostné roly, systém zastupovania, komunikačnú maticu a vytvorenie bezpečnostného výboru organizácie;
8. Zahájenie riadenia rizík;
9. Implementovať bezpečnostné školenia;
10. Zahájiť implementáciu bezpečnostných opatrení.

V tomto dokumente sa nachádza odkaz (hypertextové prepojenie) na ďalší dokument „Checklist pre agendu IT a kybernetickú bezpečnosť“, avšak po kliknutí na tento odkaz sa zobrazí stránka – časť „Riadenie kvality (QA)“, na ktorej sa však uvedený dokument, v čase spracovania tejto analýzy, hneď nezobrazí. Až po podrobnejšom prehliadaní stránky a opätovnom „preklikávaní“ na stránke - časť „Riadenie kvality (QA)“ sa už predmetný „Checklist“ zobrazí. Len veľmi komplikovaným spôsobom sa organizácia dostane k tomuto



„Checklit-u“, ktorý by mohol byť pre organizácie využiteľný, najmä pri zaradení sa do príslušnej kategórie podľa ZoITVS a ZoKB a pri určení minimálnych bezpečnostných opatrení, ktoré by mala vo svojich podmienkach implementovať, resp. pri riešení projektov.

Koncepcia uvedeného materiálu spočíva vo vyselektovaní a predložení vybraných povinností a opatrení zo záväzných právnych noriem, ako aj odporúčaní, ktorých právny status je odporúčací pre povinnú osobu, ktorá sa zaoberá riadením projektov ISVS. Výber opatrení je zvolený tak, aby rámcovo pokrýval požiadavky na KIB budovaného ISVS z hľadiska požiadaviek na jeho koncept a architektúru riešenia. Je mimoriadne dôležité, aby sa už v počiatočných fázach projektu ITVS do projektu ITVS zaradila a priebežne vykonávala identifikácia, analýza a riadenie rizík KIB, nakoľko, okrem iného, má významný vplyv na architektúru technického riešenia ITVS. Táto aktivita je následne zdokumentovaná vo forme bezpečnostného projektu podľa vyhlášky č. 85/2020 Z. z.

„Checklist“ obsahuje výber záväzných opatrení zo ZoITVS, vyhlášky č. 179/2020 Z. z., ZoKB, vyhlášky č. 362/2018 Z. z., Nariadenia GDPR, zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a odporúčacích opatrení z Metodiky pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti Verzie dokumentu 2.1, uverejnenej na stránke Vládnej jednotky CSIRT z MIRRI.

„Checklist“ je spracovaný vo formáte .xlsx a obsahuje základné bezpečnostné zásady a opatrenia pre projektované ISVS pre daný projekt, v členení na dva hárk:

- prvý hárok (Checklist\_Poziadavky na IT BEZP):
  - o tabuľka je členená tak, aby organizácia bola schopná identifikovať kategóriu, do ktorej má byť zaradená, resp. projekt, ktorý rieši, a to podľa ZoITVS a ZoKB tak, aby v ďalšom kroku mohla identifikovať bezpečnostné opatrenia, ktorá má implementovať v danom projekte, podľa oblasti bezpečnosti, následne dokáže určiť formu výstupu (dokument, proces, aplikácia HW/SW), v ďalšom kroku organizácia pristúpi k overeniu (iniciačná fáza), v ktorej overí status zapracovania požiadavky (áno - zapracovaná/nie - nezapracovaná) a na konci overí (realizačná fáza) status overenia testom (áno - overené testom/nie - neoverené testom).
- druhý hárok (Vysvetlivky ku kategorizácii)
  - o obsahuje vysvetlivky ku kategorizácii ISVS.

Vlastníkom „Checklistu“ na portáli MIRRI sprístupnenom v uvedenej lokalite je CSIRT, pričom je v súvislosti s uvedenou QA lokalitou vzniká niekoľko nezrovnalostí:

- kontaktné osoby v dokumente nie sú aktualizované (sú uvedení neexistujúci zamestnanci),
- nedostatočné zladenie dokumentov, vzorov a šablón CSIRT a MIRRI (ORKIB),
- nie je zrejmé čo je povinné a čo je uvedené ako odporúčanie, prípadne vzor,
- obsah dokumentov na QA lokalite čiastočne nekorešponduje s tým, že majú byť využiteľné aj pre dodávateľa projektu,
- nie je zrejmé či a ktoré checklisty na QA lokalite sú určené pre prevádzkovateľa alebo dodávateľa projektu a za realizáciu/implementáciu ktorých častí checklistov je kto zodpovedný.

**b) KB-K2\_3-2 Stratégia kybernetickej a informačnej bezpečnosti pre II. a III. kategóriu ISVS**

Bezpečnostná stratégia kybernetickej bezpečnosti je súčasťou bezpečnostnej dokumentácie v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v kontexte požiadavky §2 ods. (1) písm. a) a zároveň Prílohy č. 1 k vyhláške č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Zároveň je spracovaná v kontexte požiadaviek medzinárodnej normy ISO/IEC 27001 a ISO/IEC 27002.

Daná bezpečnostná stratégia slúži ako metodika a návrh, ako môže organizácia pristupovať k jej spracovaniu. Všetky spomenuté príklady a opatrenia je potrebné upraviť a prispôbiť v kontexte pôsobenia konkrétnej organizácie. (Rozsah dokumentu 5 s.)

*Štruktúra dokumentu*

1. Určenie bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti;
2. Určenie spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov;
3. Určenie úlohy štatutárneho orgánu prevádzkovateľa základnej služby pri zabezpečovaní kybernetickej bezpečnosti a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti;
4. Určenie všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti;
5. Určenie základného rámca na riadenie aktív;
6. Určenie základného rámca riadenia rizík;
7. Určenie rozsahu a periodicity overovania stavu kybernetickej bezpečnosti prostredníctvom auditu kybernetickej bezpečnosti;
8. Postup a zodpovednosti pri revízii bezpečnostnej dokumentácie;
9. Harmonogram implementácie bezpečnostných opatrení.

**c) KB-K2\_3-3 Čo má obsahovať Politika kybernetickej a informačnej bezpečnosti pre II. a III. kategóriu ISVS a ako ju vypracovať**

Tento dokument je určený správcom ISVS II. a III. kategórie a má slúžiť ako návod na vypracovanie a následné rozpracovanie Bezpečnostnej politiky pre organizáciu správcu. Vychádza zo všeobecnejšej stratégie kybernetickej a informačnej bezpečnosti (KIB) organizácie, ktorá rámcovo definuje stav a ciele organizácie v KIB. Bezpečnostná politika rozpracováva Stratégiu do väčších podrobností: obsahuje deklaráciu vedenia organizácie o význame KIB pre organizáciu, hlavných cieľoch organizácie v KIB a záväzok vedenia presadzovať Politiku KIB a vytvárať pre jej implementáciu podmienky. Následne rozoberá jednotlivé oblasti KIB, identifikuje pre každú hlavné problémy, ktoré bude organizácia musieť riešiť. (Rozsah dokumentu 36 s.)

#### *Štruktúra dokumentu*

1. Úvod;
2. Politika kybernetickej a informačnej bezpečnosti;
3. Stratégia KIB a Politika KIB;
4. Špeciálne bezpečnostné politiky a iné dokumenty;
5. Čo ďalej?;
6. Referencie.

#### **d) KB-K2\_3-4 Špecifikácia obsahu špeciálnych bezpečnostných politík 2. úrovne**

V tomto dokumente, ktorý je určený manažérom KIB, je rozpracúva podrobnejšiu špecifikáciu 13 bezpečnostných politík (2.úrovne), ktoré bude organizácia potrebovať pre vytvorenie a využívanie systému riadenia informačnej (a kybernetickej) bezpečnosti. Oblasť, pre ktoré sú spracované špecifikácie bezpečnostných politík, vychádzajú z normy ISO/IEC 27002, ale ak sa ukáže potreba vypracovať ďalšie bezpečnostné politiky, alebo iné bezpečnostné dokumenty, je tento dokument možné doplniť. (Rozsah dokumentu 24 s.)

#### *Štruktúra dokumentu*

1. Manažérske zhrnutie;
2. Úvod;
3. Špeciálne bezpečnostné politiky 2. úrovne
  - Riadenie prístupu,
  - Klasifikácia informácie a narábanie s informáciou,
  - Fyzická bezpečnosť a bezpečnosť prostredia,
  - Bezpečnostné pravidlá pre koncového používateľa,
  - Zálohovanie,
  - Manažment bezpečnosti sietí,
  - Prenos informácie,
  - Ochrana pred škodlivým kódom,
  - Manažment technických zraniteľností,
  - Kryptografické opatrenia,
  - Ochrana súkromia a osobných údajov,
  - KIB vo vzťahoch s tretími stranami,
  - Zaznamenávanie udalostí a monitorovanie.

#### **e) KB-K2\_3-6 Plán Kontinuity činností BCP – Business Continuity Plan**

Cieľom metodiky je poskytnúť správcovi návod, ako postupovať pri tvorbe plánu kontinuity činností, popisuje možné scenáre v rámci plánu kontinuity činností s uvedením požadovanej štruktúry. V závere metodiky je uvedený návrh vzoru plánu kontinuity činností. (Rozsah dokumentu 9 s.)

**f) KB-K2\_3-7 Plán obnovy činností IS DRP – Disaster Recovery Plan**

Tento dokument popisuje význam plánu obnovy činností (DRP), aké kroky má organizácia vykonať, aby tento plán mohla zostaviť s uvedením príkladu jedného z opatrení ako výsledku analýzy rizík, na ktorých je postavený DRP. Ďalšia časť dokumentu metodicky popisuje štruktúru DRP, scenáre v rámci plánu kontinuity činností (BCP) a návrh vzoru plánu obnovy činností. (Rozsah dokumentu 7 s.)

**g) KB-K2\_3-8 Pracovná náplň Manažéra kybernetickej a informačnej bezpečnosti**

V dokumente je uvedené zaradenia podľa Katalógu pracovných činností, požadované vzdelanie, platová trieda a činnosti, ktoré zamestnanec zastávajúci túto pozíciu má vykonávať. (Rozsah dokumentu 1 s.)

**h) KB-K2\_3-9 Bezpečnostný projekt (metodika spracovania bezpečnostného projektu)**

Tento dokument je určený správcom IS, manažérom kybernetickej bezpečnosti a tým, ktorí budú zapojení do prípravy bezpečnostného projektu. Za udržiavanie a aktuálnosť tohto bezpečnostného projektu zodpovedá správca IS. (Rozsah dokumentu 23 s.)

*Štruktúra dokumentu*

- 1 Manažérske zhrnutie;
- 2 Ciele bezpečnostného projektu IS;
- 3 Štruktúra bezpečnostného projektu IS;
- 4 Správa rizík;
- 4.1 Prípravná fáza - stanovenie kontextu;
- 4.2 Ohodnotenie rizík;
- 4.2.1 Identifikácia aktív;
- 4.2.2 Identifikácia hrozieb;
- 4.2.3 Identifikácia zraniteľností;
- 4.2.4 Identifikácia existujúcich opatrení;
- 4.2.5 Identifikácia dopadov;
- 4.3 Analýza rizík;
- 4.4 Bezpečnostné opatrenia v súlade s platnou legislatívou;
- 5 Záver;
- 6 Prílohy;
- 6.1 Identifikácia aktív;
- 6.1.1 Identifikácia primárnych aktív;
- 6.1.2 Identifikácia podporných aktív;
- 6.2 Zoznam hrozieb;
- 6.3 Zoznam zraniteľností;
- 6.4 Bezpečnostné opatrenia definované Bundesamt für Sicherheit in der Informationstechnik (BSI);
- 6.5 Bezpečnostné opatrenia definované National Institute of Standards and Technology (NIST).

### 3.4.1.2 Čiastkový záver

Berúc do úvahy rozsah bezpečnostných opatrení pre ITVS, ktoré sú tvorené minimálnymi bezpečnostnými opatreniami troch úrovní podľa zaradenia do kategórie I, kategórie II alebo kategórie III a povinnosti ich implementácie v organizáciách verejnej správy je možné prijať záver, že vyššie uvedené a popísané súbory materiálov zverejnené na webovom sídle MIRRI metodicky nepokrývajú všetky oblasti bezpečnosti (príloha č. 1), ale iba sporadicky, aj to len pre niektoré oblasti a kategórie. Absentuje systematickosť a komplexnosť. V niektorých prípadoch je zverejnená len metodika, v niektorých prípadoch vzor smernice bez zdôvodnenia zvolenej formy zverejneného dokumentu.

Dalo by sa očakávať, že pri danom rozsahu vyplývajúceho z množstva oblastí v KIB budú súbory materiálov sprístupnené štruktúrovane, s príslušným komentárom (alebo uvedením do problematiky) tak, aby pomohli danému OVM čo najjednoduchším spôsobom dosiahnuť žiadaný súlad so zákonom o ITVS, resp. vyhláškou č. 179/2020 Z. z.

Čo sa týka funkčnosti zverejneného súboru dokumentácie ako celku, metodiky

- nie sú označované dátumom vydania/platnosti,
- nie sú jednoznačne označované ich verzie vydania alebo aktualizácie,
- nie je uvedený garant dokumentu alebo príslušný kontakt,
- nie je uvedený schvaľovateľ dokumentu,
- nie je jednoznačné priradenie názvu dokumentu ku konkrétnej oblasti bezpečnosti,
- majú rôznu štruktúru,
- v mnohých prípadoch nie je uvedený jednoznačný účel dokumentu,
- nie je uvedené ďalšie usmernenie, ako a akým spôsobom dokumenty efektívne uplatňovať v praxi,
- v mnohých prípadoch nie sú v dokumentoch uvedené aktuálne informácie či odkazy pričom tieto, ak sú uchopené nesprávne, neprispievajú ku zvýšeniu úrovne kybernetickej bezpečnosti, práve naopak; môže to mať za následok zvýšenie zraniteľnosti ISVS,
- v niektorých prípadoch nemajú aktívne odkazy (hypertextové prepojenia na iný súvisiaci dokument), na ktoré sa v textoch odkazujú, čo má za následok „nedostupnosť“ súvisiacich dokumentov alebo prepoja/odkážu na inú stránku, kde by mal byť súvisiaci dokument zverejnený a ten tam dostupný nie je; tieto nepresnosti pôsobia zmätočne a chaoticky a organizácia sa len ťažko dokáže v takejto situácii orientovať (konštatovanie platné v čase vypracúvania tejto analýzy).

Dala by sa očakávať, že bude:

- zavedená funkcionálna, ktorá bude záujemcov/organizácie/OVM upozorňovať na nové verzie dokumentov, iné aktualizácie alebo rozšírenia dokumentov o nové metodiky, vzory, smernice alebo šablóny; pritom povinnosť sprístupniť súbor

materiálov má MIRRI ako orgán vedenia uvedenú priamo v zákone o ITVS, resp. vyhláške č. 1479/2020 Z. z.;

- zriadený kontaktný bod (formulár, emailový kontakt, možnosť konzultácií – telefonicky alebo osobne) za účelom poskytnutia spätnej väzby a podpory pri zavádzaní a implementovaní bezpečnostných opatrení;
- poskytnutý návod alebo inštruktáž pre OVM ako s poskytnutými dokumentami pracovať efektívne a ako ich používať vo svojich podmienkach tak, aby bol súlad so zákonom o ITVS dosiahnutý;
- webové sídlo MIRRI v rámci časti „Kybernetická bezpečnosť“ štruktúrované tak, aby sa OVM vedeli jednoducho orientovať podľa kategórie I, II alebo III, do ktorej sú zaradené, s požadovaným rozsahom informácií a to tak aby bol splnený sledovaný cieľ, a to aplikovaním zákonom stanovených požiadaviek pre jednotlivé kategórie dosiahnuť zvýšenie odolnosti voči kybernetickým hrozbám.

Poskytnuté dokumenty a ich využiteľnosť v praxi zo strany OVM nebola overovaná v rámci „pilotného testovania“. Absentuje teda zo strany OVM spätná väzba o účinnosti a efektívnosti poskytnutých dokumentov. Nie je možné jednoznačne vyjadriť, ako tieto dokumenty dané OVM dokážu uchopiť, ako s nimi dokážu pracovať a ako realizujú implementáciu bezpečnostných opatrení.

Z uvedených dôvodov bude v rámci tejto analýzy vykonávaný vlastný prieskum, ktorého priebeh a výsledky budú súčasťou kapitoly 2.

Nakoľko skopírovaním, vyplnením a vytlačením uvedených vzorových dokumentov a ďalších podkladov sa reálna bezpečnosť organizácie nezvýši, je preto potrebné poskytnúť komplexné návody na ich efektívnu implementáciu a zavedenie do praxe. Takto zavedené procesy do praxe je potrebné ďalej optimalizovať, z čoho vzniká požiadavka na meranie účinnosti zavedených procesov, prostredníctvom nastavenia metrík a daných KPI.

*Pozn.:*

Cieľom analýzy zverejnených dokumentov nebolo ich podrobenie hĺbkovej analýze po obsahovej stránke, ale po koncepcnej stránke z pohľadu pokrytia jednotlivých oblastí bezpečnosti zverejnenými dokumentami na webovom sídle MIRRI.

### 3.4.2 Metodiky a štandardy vydané Národným bezpečnostným úradom

Na svojom webovom sídle NBÚ zverejňuje vzory, ktoré je možné vyplňať elektronicky. Pre oblasť kybernetickej bezpečnosti ide o nasledujúce vzory dokumentov:

- Základné služby
  - Oznámenie o prekročení identifikačných kritérií služby;
  - Príloha k oznámeniu o prekročení identifikačných kritérií;
  - Zmena oznámenia o prekročení identifikačných kritérií;



- Zmena prílohy k oznámeniu o prekročení identifikačných kritérií.
- Digitálne služby
  - Oznámenie o poskytovaní digitálnej služby;
  - Oznámenie o zástupcovi poskytovateľa digitálnej služby.
- Jednotky CSIRT
  - Žiadosť o posúdenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT;
  - Žiadosť o uznanie akreditácie jednotky CSIRT;
  - Hlásenie zmien ovplyvňujúcich riadne fungovanie akreditovanej jednotky CSIRT.

Na svojom webovom sídle tiež zverejňuje, okrem iných, aj nasledujúce informácie

- *Hlásenie kybernetických bezpečnostných incidentov* – popisuje povinnosti prevádzkovateľa základnej služby a Formulár na hlásenie kybernetických bezpečnostných incidentov;
- *Národná jednotka CSIRT* a jej úlohy;
- *Akreditácia jednotky CSIRT* – spresňuje podmienky akreditácie;
- *Bezpečnostné opatrenia* – popisuje základné informácie o bezpečnostných opatreniach a oblastiach, pre ktoré sa prijímajú;
- *Riadenie rizík* – popisuje kybernetické bezpečnostné riziká a ich riadenie, riziká pôsobiace na informačné aktíva, ďalej zraniteľnosť, hrozbu, incident, proces ošetrovania rizík
  - zverejnená metodika analýzy rizík;
- *Audit kybernetickej bezpečnosti* – popisuje význam auditu KB, účel, kým je vykonávaný
  - zverejnená metodika auditu kybernetickej bezpečnosti;
- *Krátky slovník hybridných hrozieb* – obsahuje približne 148 termínov s výkladom abecedne zoradených;
- *Samohodnotenie účinnosti prijatých bezpečnostných opatrení* v zmysle zákona o kybernetickej bezpečnosti - zjednodušený spôsob overenia miery implementácie požiadaviek zákona o kybernetickej bezpečnosti, ako mieru implementácie požiadaviek tohto zákona je možné overiť aj prostredníctvom tzv. samohodnotenia;
  - je zverejnený
    - formulár samohodnotenia,
    - návod na vyplnenie formuláru Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti,
    - samohodnotenie v zmysle zákona o kybernetickej bezpečnosti - Formulár pre dodatočné informačné systémy.

### 3.4.2.1 Popis zverejnených metodík a štandardov na webovom sídle Národného bezpečnostného úradu

#### a) metodika analýzy rizík

Tento dokument metodicky usmerňuje PZS pri výkone analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. (Rozsah 27 s.).

#### *Štruktúra dokumentu*

1. Úvod – popisuje význam riadenia rizika, význam metodiky a jej zásady, uvádza právny základ a normatívne odkazy;
2. Proces riadenia rizika – uvádza jednotlivé procesy riadenia rizika;
3. Metodika analýzy rizík – popisuje alternatívne prístupy k analýze rizika, metódy hodnotenia rizika;
4. Stanovenie kontextu rizika – popisuje činnosti za účelom stanovenie kontextu (identifikácia aktív a ich vlastníkov, identifikácia zraniteľností, identifikácia potenciálnych hrozieb, odhad dopadov, odhad pravdepodobností, identifikácia existujúcich opatrení);
5. Kvalitatívna analýza rizík – popisuje metodiku kvalitatívnej analýzy rizík;
6. Semikvantitatívna (zmiešaná) analýza rizík – popisuje metodiku semikvantitatívnej analýzy rizík
7. Ošetrovanie rizika – popisuje metódy ošetrovania rizika;
8. Akceptácia zvyškového rizika – popisuje, čo je zvyškové riziko, aké sú kritériá akceptácie rizika, jej proces;
9. Komunikácia rizika – popisuje význam komunikácie rizika, správu o riziku;
10. Prílohy – obsahuje vzor návrhu na akceptáciu rizika; vzor správy o riziku.

#### b) metodika auditu kybernetickej bezpečnosti

Tento dokument popisuje výkon auditu kybernetickej bezpečnosti v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

#### c) formulár samohodnotenia

Tento dokument obsahuje formulár určený na samohodnotenie účinnosti prijatých bezpečnostných opatrení, za PZS ho vyplňa manažér kybernetickej bezpečnosti. Na účely jeho správneho vyplnenia má manažér KB k dispozícii metodický návod.

### 3.4.2.2 Čiastkový záver

Úrad nemá taxatívne vymedzenú povinnosť pokryť metodikami všetky oblasti bezpečnosti. Podľa zákona o KB je uvedený ako orgán, ktorý vydáva metodiky a politiky správania sa v kybernetickom priestore, či na JISKB zverejňuje metodiky, usmernenia, štandardy, politiky



a oznamy. Použiteľnými metodikami na sledované účely je metodika analýzy rizík, metodika auditu kybernetickej bezpečnosti a elektronický formulár samohodnotenia.

Webové sídlo NBÚ metodicky pokrýva oblasti bezpečnosti taktiež čiastkovo. V sekcii JISKB je časť „Metodiky, usmernenia, štandardy, politiky, oznamy a formuláre“, aktívnou je však len zložka „formuláre“.

Prehľad o zverejnených metodikách pre jednotlivé oblasti bezpečnosti je uvedený v prílohe č. 1 tohto dokumentu.

Cieľom analýzy zverejnených dokumentov nebolo ich podrobenie hĺbkovej analýze po obsahovej stránke, ale po koncepcnej stránke z pohľadu pokrytia jednotlivých oblastí bezpečnosti zverejnenými dokumentami na webovom sídle NBÚ.

### 3.5 Vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike

CSIRT.SK (Computer Security Incident Response Team Slovakia) je vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike podľa zákona o KB zriadená ako organizačný útvar MIRRI SR. Zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci celej ITVS. Poskytuje aj služby preventívneho a vzdelávacieho charakteru.

K hlavným cieľom CSIRT.SK patrí:

- riešenie kybernetických bezpečnostných incidentov v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí ITVS, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a prípadne inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy),
- budovanie a rozširovanie povedomia verejnosti vo vybraných oblastiach informačnej, resp. kybernetickej bezpečnosti,
- kooperácia s partnerskými organizáciami a združeniami v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni.

Služby CSIRT.SK sú rozdelené na nasledujúce dve skupiny

- Reaktívne služby:
  - riešenie incidentov,
  - varovania a upozornenia,
  - detekcia incidentov,
  - analýza incidentov,
  - ohraničenie, vyhladenie incidentu a obnova,
  - poskytnutie pomoci pri riešení incidentu na mieste,
  - reakcia na incidenty,
  - podpora pri riešení incidentov,

- koordinácia činností pri reakcii na incidenty,
  - návrh opatrení na prevenciu ďalšieho pokračovania, šírenia a opakovania sa incidentov,
  - analýza škodlivého softvéru.
- Proaktívne služby:
- vzdelávanie a budovanie všeobecného povedomia v oblasti informačnej bezpečnosti,
  - odborné školenia a výcvik,
  - spolupráca s ostatnými jednotkami CSIRT,
  - monitorovanie a dokumentovanie incidentov,
  - pripojenie sa do jednotného systému kybernetickej bezpečnosti (JSKB),
  - prijímanie a zasielanie včasných varovaní o incidentoch cez (JSKB),
  - oznámenia o existujúcich zraniteľnostiach,
  - technologický dozor,
  - konfigurácia a údržba bezpečnostných nástrojov, aplikácií a infraštruktúry,
  - služby detekcie prienikov,
  - distribúcia informácií týkajúcich sa bezpečnosti,
  - monitorovanie stavu hrozieb v oblasti IKT,
  - vzdelávanie a budovanie bezpečnostného povedomia,
  - konzultačná činnosť v oblasti informačnej bezpečnosti,
  - audit informačnej bezpečnosti,
  - asistencia pri zakladaní nových jednotiek CSIRT.

Na svojom webovom sídle CSIRT.SK zverejňuje v sekcii

- **Dokumenty**
- Zvyšovanie povedomia ohľadom kybernetickej bezpečnosti
  - Naše publikácie
  - Mesačné prehľady kritických a závažných softvérových zraniteľností
  - Mesačné správy CSIRT.SK
- **Rady a návody**
- Návody a odporúčania – uvádza návody a odporúčania pre používanie, konfiguráciu a zabezpečenie zariadení IKT vrátane koncových staníc (desktopov, notebookov) a serverov.
  - Bezpečnosť IS organizácie – uvádza odporúčané postupy pre zníženie pravdepodobnosti výskytu alebo dopadov niektorých štandardných rizík na informačnú infraštruktúru.
  - Metodika zabezpečenia IKT - Informačné systémy a prostriedky používané v organizáciách musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu

infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované.

### 3.5.1 Popis zverejnených metodík a štandardov na webovom sídle jednotky CSIRT.SK

#### 1. Dokumenty

##### a) Zvyšovanie povedomia ohľadom kybernetickej bezpečnosti

Jednotka CSIRT.SK sa v rámci svojej činnosti venuje tiež zvyšovaniu povedomia ohľadom kybernetickej a informačnej bezpečnosti a zodpovedného správania sa na internete. Zamestnancom organizácií vo svojej konštituencii poskytuje tematické školenia. Na svojom webovom sídle má zverejnenú prezentáciu zo školenia „Informačná bezpečnosť“, určeného pre budovanie všeobecného prehľadu zamestnancov. Informácie z neho pomôžu účastníkom vyhnúť sa bežným rizikám, ktoré stretnú online v pracovnom aj osobnom živote.

##### b) Naše publikácie

V tejto časti sú zverejnené materiály publikované útvarom CSIRT.SK.

- **Metodiky pre minimálne bezpečnostné opatrenia kategórie I**  
Tento dokument umožní zistiť základný stav bezpečnosti IT systémov v organizácii. Pomocou checklistu bude schopná odhaliť nedostatky zabezpečenia IT systémov, na základe ktorých ich organizácia bude vedieť odstrániť.
- **Požiadavky na zabezpečenie infraštruktúry a riešenia implementovaného v rámci OPII**  
Metodika predstavuje návrh základných požiadaviek na systematické zabezpečenie informačnej bezpečnosti v organizácii.
- **Kontrolný zoznam pre bezpečnosť webových aplikácií**  
Kontrolný zoznam stručne sumarizuje najdôležitejšie bezpečnostné aspekty pri vývoji a prevádzke webových stránok a je možné ho využiť pri vykonávaní interného auditu bezpečnosti webových aplikácií a webových stránok.
- **Príručka pre hardening – Windows**  
Príručka sa zameriava na operačné systémy založené na Microsoft Windows NT jadre a popisuje ako hardenovať operačný systém Microsoft Windows 7.
- **Príručka pre hardening – Linux**
  - Staršia príručka sa zameriava na operačné systémy založené na Linuxovom jadre a popisuje ako hardenovať operačné systémy RHEL 5 a Debian.
  - Príručka zameraná na automatizovanú konfiguráciu systémov s OS Ubuntu Server, prípadne Debian.
- **Základná ochrana pred útokmi na web I**  
V staršej príručke sa popisujú tri základne druhy útokov na webové aplikácie a ochrana pred týmito útokmi.

- **Ochrana pred útokmi DDoS**  
V staršej príručke sa popisujú druhy DDoS útokov a prevencia pred útokmi.
- **Phishingové emaily: rozpoznanie a obrana**  
Príručka sa zameriava na odhaľovanie podvodných phishingových emailov na základe rozpoznanie ich znakov a na spôsoby, ako sa pred nimi chrániť. Obsahuje tiež analýzu hlavičky emailu.
- **Vedeli ste, že... – bezpečnostné odporúčania**  
Šestnásť zásad pre zvýšenie kybernetickej bezpečnosti pre používateľov aj administrátorov.
- **SÉRIA: Bezpečnosť linuxových systémov**  
Séria článkov o hardeningu Linuxu a konfigurácii linuxových serverov zameranej na bezpečnosť.

**c) Mesačné prehľady kritických a závažných softvérových zraniteľností**

Zverejňuje mesačný prehľad kritických a závažných softvérových zraniteľností.

**d) Mesačné správy CSIRT.SK**

Zverejňuje mesačnú správu CSIRT.SK a prehľad bezpečnostných udalostí vo svete a v SR.

**2. Rady a návody**

**a) Návody a odporúčania**

Tento dokument uvádza návody a odporúčania pre používanie, konfiguráciu a zabezpečenie zariadení IKT vrátane koncových staníc (desktopov, notebookov) a serverov. Ide o:

- Webové služby a e-mail
  - SPF, DKIM, DMARC: Odporúčané nasadenie overovacích a autorizačných systémov pre e-mailové servery (05-2021)
  - Šifrovanie e-mailov a súborov pomocou PGP (08-2019)
- Operačné systémy
  - Microsoft Windows Telemetria (01-2021)
- Bežné softvérové produkty
  - MS Office: Prečo používať formát Open XML (docx ..) namiesto binárneho (doc ..) (03-2021)
  - Odporúčané videokonferenčné riešenia (09-2020)
  - Zvyšovanie informačnej a kybernetickej bezpečnosti
  - Manažér hesiel KeePass (10-2018)
- Zvyšovanie bezpečnostného povedomia
  - Štandardy informačnej bezpečnosti
  - Kritické bezpečnostné opatrenia
  - Sociálne inžinierstvo

- Bezpečnosť organizácie
- Insider threat – Je vaša organizácia pripravená na hrozby z vnútra?
- Outsourcing informačných technológií a bezpečnosť
- Mobilné zariadenia
  - Bezpečnosť mobilných aplikácií

**b) Bezpečnosť IS organizácie**

Tento dokument uvádza odporúčané postupy pre zníženie pravdepodobnosti výskytu alebo dopadov niektorých štandardných rizík na informačnú infraštruktúru. Ide o popísanie:

1. Konfigurácia serverov;
2. Konfigurácia serverov;
3. Sieťová bezpečnosť;
4. Šifrovanie dát.

**c) Metodika zabezpečenia IKT**

Tento dokument sumarizuje minimálne opatrenia potrebné na zabezpečenie IS a infraštruktúry organizácie so zvýšenými požiadavkami na bezpečnosť tak, aby platili tieto princípy. Metodika je cielená pre využitie vo VS pre organizácie so zvýšenými požiadavkami na bezpečnosť, avšak v princípe je aplikovateľná pre akékoľvek veľké alebo stredne veľké počítačové siete, ktoré majú zvýšené požiadavky na bezpečnosť, ale potrebujú mať zabezpečenú KB na úrovni odolnosti voči štandardným cieľovým kybernetickým útokom. (Rozsah 62 s.)

*Štruktúra dokumentu*

Úvod

1. Organizačné opatrenia;
2. Technické opatrenia
  - a. Minimálne požiadavky na zabezpečenie implementovaného riešenia,
  - b. Minimálne požiadavky na zabezpečenie služieb dostupných z externých sietí – Webové aplikácie,
  - c. Minimálne požiadavky na zabezpečenie infraštruktúry,
  - d. Minimálne požiadavky na zabezpečenie externej infraštruktúry,
  - e. Minimálne požiadavky na zabezpečenie internej infraštruktúry,
  - f. Minimálne požiadavky na zabezpečenie pracovných staníc prístupujúcich k implementovanému riešeniu,
  - g. Administratívne opatrenia;
3. Príloha
  - a. Politika hesiel,
  - b. Zariadenia pre nasadenie a zabezpečenie webového servera.

### 3.5.2 Čiastkový záver

CSIRT.SK na svojom webovom sídle uverejňuje metodiky predovšetkým z pohľadu technického zabezpečenia systémov, technické zraniteľnosti a pod., pričom táto povinnosť komplexne pokryť metodikami všetky oblasti bezpečnosti nemá uvedené v legislatíve priamo. Preto je možné považovať túto činnosť za proaktívnu a nápomocnú pre dotknuté organizácie.

Medzi aktivity súvisiace so zvyšovaním bezpečnostného povedomia a aplikovaním bezpečnostných opatrení je možné zaradiť aj tzv. informačnú kampaň, ktorú CSIRT.SK taktiež zabezpečuje prostredníctvom emailových notifikácií na kontakt organizáciám s cieľom upozorniť OVM (emailom) na najväčšie aktuálne zraniteľnosti phishingové kampane, ransomvérové útoky a ďalšie aktivity záškodných skupín (APT) a pod.

Z pohľadu posúdenia využiteľnosti metodík pre účely tejto analýzy uvádzame aj pokrytie oblastí bezpečnosti dokumentami zverejnených na webovom sídle CSIRT.SK. Je možné konštatovať, že zverejnené dokumenty taktiež nepokrývajú komplexne všetky oblasti bezpečnosti definované legislatívnymi požiadavkami, nie je to však ani povinnosťou CSIRT.SK. Obsah metodiky zabezpečenia IKT je však nevyvážený a nevyrovnaný do tej miery, že obmedzuje jej praktické využitie. Niektoré oblasti KB sú spracované extrémne detailne, iné iba rámcovo resp. chýbajú úplne. Metodika navyše svojou štruktúrou a orientáciou nie je kompatibilná s legislatívnymi požiadavkami KB a zaužívanými postupmi z nich vyplývajúcimi. Ostatné metodiky taktiež nie sú súladné s metodikami popisovanými v časti 1.4.1. Z uvedeného dôvodu nie sú tieto metodiky súčasťou prílohy č. 1.

### 3.6 Agentúra Európskej únie pre kybernetickú bezpečnosť

ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) predstavuje hlavný riadiaci orgán pre zabezpečenie definovania minimálnych požiadaviek na kybernetickú odolnosť (požiadavky na implementovanie procesov v oblasti riadenia KB a implementovanie bezpečnostných opatrení na zaistenie tejto úrovne.

Definovanie a harmonizáciu týchto bezpečnostných požiadaviek aplikuje naprieč EÚ prostredníctvom smernice NIS (v príprave je smernica NIS 2). V Smernici NIS sú definované dva druhy hospodárskych subjektov, a to konkrétne prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb. Popri týchto subjektoch sú adresátmi právnych noriem obsiahnutých v Smernici NIS aj samotné členské štáty, ktoré musia plniť konkrétne povinnosti.

Portál ENISA (<https://www.enisa.europa.eu>) predstavuje rozcestník pre uvádzanie legislatívnych požiadaviek, taktiež však sprístupňuje rozsiahle množstvo metodických

dokumentov (primárne v anglickom jazyku), ktoré sú prehľadne usporiadané do skupín podľa preddefinovaných tém (topics) alebo tzv. značiek (tags).

Publikácie sú triedené aj kontextovo, a to *ENISA Reports, Corporate documents, Cyber security info notes, Opinion papers* a *ED's speeches*.

Portál sprístupňuje používateľovi aj sadu nástrojov (Tools), ako sú *napríklad CSIRT Maturity – Self-assessment tool, Cyber risk management for ports, National Cybersecurity Assessment Framework (NCAF) Tool, SecureSME*.

### 3.6.1 Čiastkový záver

ENISA predstavuje riadiacu organizáciu pre kybernetickú bezpečnosť v EÚ a je zodpovedná za vydávanie štandardov a legislatívnych požiadaviek vo forme smerníc EÚ. Aktuálnou smernicou je smernica NIS. ENISA svojou smernicou NIS určuje pravidlá KB pre úroveň EÚ. Členské štáty si ju adaptujú prostredníctvom svojich vlastných legislatívnych predpisov. V prostredí SR je NIS transformovaná do slovenskej legislatívy prostredníctvom zákona o KB a jej vykonávacích predpisov.

ENISA prostredníctvom svojho portálu sprístupňuje rozsiahle množstvo dokumentov a metodických materiálov pre oblasť kybernetickej bezpečnosti (Cyber security). Tieto sú pravidelne aktualizované a dopĺňané o nové alebo vysoko aktuálne témy ako je napríklad umelá inteligencia (AI) alebo Machine Learning (ML).

Aktuálnou témou a z pohľadu rizika sú aj početnosti, napríklad ransomvér útoky, kde ENISA spracovala metodický dokument vo forme PDF - *ENISA Threat Landscape for Ransomware attack*.

Usporiadanie metodických dokumentov na webovom sídle ENISA však nezodpovedá štruktúre požiadaviek, ktoré potrebujú riešiť OVM, v nadväznosti na požiadavky ZoITVS a ZoKB nie sú tam metodiky v slovenskom jazyku.

Metodiky sú v štruktúrach, ktoré môžu pomôcť len v riešení konkrétnych problémov v danej oblasti, napríklad uvedený ransomvér.

Nástroje (tools), ktoré sú k dispozícii, sú v anglickom jazyku, pomôžu taktiež pri riešení konkrétnej situácie alebo problému, prípadne pomôžu pri samohodnotení stavu kybernetickej bezpečnosti.

Pri komplexnom a efektívnom riešení požiadaviek uvedenej slovenskej legislatívy však nie sú využiteľné.



### 3.7 Komparácia legislatívnych požiadaviek s poskytnutými a zverejneným súborom materiálov

V nadväznosti na zákonom stanovené povinnosti uložené:

- orgánu vedenia MIRRI:
  - vydávať metodické usmernenia, usmerňovať a koordinovať orgány riadenia na účely jednotného spôsobu výkonu riadenia v správe informačných technológií verejnej správy a centrálneho riadenia informatizácie spoločnosti,
  - vydávať štandardy a výkladové stanoviská,
  - zverejňovať na ústrednom portáli rozhodnutia, iné dokumenty a informácie týkajúce sa informačných technológií verejnej správy a informatizácie verejnej správy,

čo je možné dosiahnuť poskytnutím súboru materiálov, ktorý obsahuje šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návody, školiace materiály a ukážky správcovi;

- NBÚ:
  - určovať štandardy, operačné postupy, vydávať metodiky a politiky správania sa v kybernetickom priestore,
  - zverejňovať metodiky, usmernenia, štandardy, politiky a oznamy vo verejnej časti JISKB;

a na čiastkové zistenia v rámci tejto analýzy je možné konštatovať, že je žiaduce zavedenie štandardov KIB pre oblasť sietí a ITVS štátnej a verejnej správy s cieľom efektívnejšieho zavádzania opatrení a krokov vedúcich k zvyšovaniu úrovne KB s cieľom štandardizácie riešení v oblasti KB a vytvorenie jednotného rámca pre oblasť implementácie bezpečnostných opatrení KIB, šablón bezpečnostnej dokumentácie s cieľom riadiť KIB na úrovni organizácií OVM a na centrálnej úrovni a zvyšovať úroveň KIB v podsektore VS. Zaistenie spoľahlivého a bezpečného fungovania ISVS je nevyhnutnou podmienkou zabezpečenia chodu jednotlivých organizácií ako aj celej spoločnosti z pohľadu fungovania verejného sektora. Prehľad zákonom stanovených požiadaviek ohľadom poskytnutých a dostupných metodík, usmernení či štandardov je uvedený v prílohe č. 1 tohto dokumentu. Stav pokrytia jednotlivých oblastí bezpečnosti poskytnutými dokumentami zverejnenými na webovom sídle MIRRI je uvedený v tabuľke č. 1.



Tabuľka č. 1 Stav pokrytia jednotlivých oblastí bezpečnosti

Vyhláška NBÚ č. 362/2018 Z. z.	Vyhláška ÚPVII č. 179/2020 Z. z.	stav
Organizácia kybernetickej bezpečnosti	A. Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	Pokrytá len čiastočne; ťažko prakticky vykonateľná; potreba spresňujúcej metodologickej podpory
Riadenie aktív, hrozieb a rizík	B. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	Je pokrytá len čiastočne; nie pre všetky kategórie; zverejnený dokument nie je postačujúci; absentuje metodická podpora pre riadenie aktív, hrozieb, rizík IB a KB (dostupná metodika analýzy rizík – NBÚ)
Personálna bezpečnosť	C. Personálna bezpečnosť	Nie je pokrytá
Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,	E. Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	Pokrytá len čiastočne; nie pre všetky kategórie; nedostatočne metodicky podporená
	J. Akvizícia, vývoj a údržba informačných technológií verejnej správy	Nie je pokrytá
Technické zraniteľnosti informačných systémov	G. Hodnotenie zraniteľností a bezpečnostné aktualizácie	Pokrytá len čiastočne, nie pre všetky kategórie; nedostatočne metodicky podporená
Riadenie bezpečnosti sietí a informačných systémov	I. Sieťová a komunikačná bezpečnosť	Nie je pokrytá
Riadenie prevádzky	F. Bezpečnosť pri prevádzke informačných systémov a sietí	Nie je pokrytá
	H. Ochrana proti škodlivému kódu	Nie je pokrytá
Riadenie prístupu	D. Riadenie prístupov	Nie je pokrytá
Kryptografické opatrenia	N. Kryptografické opatrenia	Nie je pokrytá
Riešenia kybernetických bezpečnostných incidentov	M. Riešenie kybernetických bezpečnostných incidentov	Nie je pokrytá
Monitorovanie, testovanie bezpečnosti a bezpečnostné audity	K. Zaznamenávanie udalostí a monitorovanie	Nie je pokrytá
	P. Audit a kontrolné činnosti	Nie je pokrytá (dostupná metodika auditu KB – NBÚ)
Fyzická bezpečnosť sietí a informačných systémov	L. Fyzická bezpečnosť a bezpečnosť prostredia	Pokrytá len čiastočne; nie pre všetky kategórie, nedostatočne metodicky podporená
Riadenia kontinuity procesov	O. Kontinuita prevádzky informačných technológií verejnej správy	Pokrytá len čiastočne, ťažko prakticky vykonateľné; nedostatočne metodicky podporená

Z vyššie uvedených čiastkových záverov a z uvedeného prehľadu (tabuľka č. 1, príloha č. 1) je možné prijať konštatovanie, že:

- je náročné zosúladiť plnenie požiadaviek oboch vyhlášok jedným súborom opatrení (rozdielne koncepčne uchopené riešenia v daných oblastiach KB),
- väčšina z oblastí bezpečnosti nie je vôbec pokrytá či už metodicky, vzorom dokumentu, šablónou alebo iným spôsobom a nevyhovuje ani z pohľadu požiadaviek na minimálne bezpečnostné opatrenia podľa stanovených kategórií,
- niektoré oblasti sú pokryté len čiastočne, tzn. že existuje metodika, vzor, smernica,
  - ale ani v jednom prípade nepokrývajú komplexne danú oblasť, resp. nie sú určené pre jednotlivé kategórie I, II, III;
  - tak ako sú koncipované, sú pre používateľov ťažko uchopiteľné, nakoľko neexistuje dostatočná metodická podpora, usmernenie alebo vysvetlenie o ich aplikovateľnosti.

V rámci tejto analýzy bolo taktiež zistené, že informácie nie sú aktualizované, resp. nie sú presné. Z toho vyplýva, že informácie, ktoré nie sú aktuálne, resp. priebežne aktualizované a ktoré sú nesúrodé a nesystematicky podané, bez dostatočne zrozumiteľných usmernení, môžu spôsobiť, že ich dané OVM uchopí koncepčne nesprávne alebo na základe zastaralých informácií nesprávne implementuje bezpečnostné opatrenia, čo v konečnom dôsledku môže mať zásadný vplyv na zníženie kybernetickej bezpečnosti OVM. Poskytnuté dokumenty by mali byť vypracované na kvalitatívne vyššej úrovni.

Nakoľko v prípade MIRRI ide o riadiaci orgán – orgán vedenia, ktorý má svojim dosahom vplyv na úroveň kybernetickej bezpečnosti VS ako celku, je žiaduce a zákonom jednoznačne stanovené, že dokumentácia, ktorú má poskytovať, má zodpovedať súčasným požiadavkám kladeným na riadenie kybernetickej bezpečnosti celého sektora, ktoré musí byť koncepčné a systematické v súlade s aktuálnymi bezpečnostnými štandardmi nadväzujúce na moderné trendy v oblasti kybernetickej bezpečnosti. Má reagovať na súčasné geopolitické hrozby a byť v súlade s bezpečnostnou stratégiou SR. Taktiež musí koncepčne nadväzovať na požiadavky na úrovni EÚ (ENISA).

## 4 Vlastný prieskum metodík a štandardov v oblasti kybernetickej bezpečnosti v prostredí verejnej správy

### 4.1 Realizácia vlastného prieskumu

Vlastný prieskum metodík a štandardov v oblasti kybernetickej bezpečnosti v prostredí verejnej správy sa realizoval vyplnením dotazníka, z ktorého údaje budú využité v rámci plnenia úloh vyplývajúcich z Plánu obnovy a odolnosti, reforma „Štandardizácia technických a procesných riešení kybernetickej bezpečnosti“. Cieľom reformy je priniesť subjektom verejnej správy štandardné riešenia v oblasti kybernetickej bezpečnosti ako je napríklad vytvorenie šablón dokumentov pre štruktúru bezpečnostnej dokumentácie, pomoc pri plnení požiadaviek (bezpečnostné opatrenia) legislatívy a zvýšiť tak bezpečnostnú úroveň orgánov verejnej moci (OVM) v oblasti kybernetickej a informačnej bezpečnosti.

Cieľom prieskumu bolo zistiť, aký je reálny stav implementácie požiadaviek zákona o KB a zákona o ITVS v podmienkach verejnej správy z pohľadu prijatej a schválenej bezpečnostnej dokumentácie v OVM a zistiť aký je stav využitia existujúcich metodických dokumentov v oblasti KB vo VS zverejnených MIRRI, NBÚ alebo Vládnou jednotkou CSIRT na svojich stránkach.

Pre účely prieskumu bol pracovnou skupinou expertov vypracovaný súbor otázok, ktoré boli vybrané, pripomienkované a schválené projektovou komisiou KPMG. V prostredí Sharepoint sa pripravil online dotazník, ktorý bol schválený zo strany MIRRI.

Dotazník má dva typy odpovedí na otázky, a to pevná časť (áno/nie; máme/nemáme; implementované/neimplementované a pod.) a variabilná možnosť odpovedí, kde môže respondent voľne odpovedať alebo hodnotiť úroveň na stupnici 0 až 10. Otázky v dotazníku sú hlavne zamerané na overenie, či boli využité existujúce metodiky MIRRI, NBÚ alebo CSIRT a či respondentom pomohli pri implementácii požiadaviek zákona o KB a zákona o ITVS, alebo či pomohli pri audite kybernetickej bezpečnosti a zároveň overil absolvovanie auditu kybernetickej bezpečnosti (AKB). Cieľom prieskumu bolo tiež urobiť koreláciu výsledkov vzhľadom na využité dostupné metodiky a dosiahnuté nezávislé hodnotenie AKB.

Vytvorený online dotazník v úvode (časť „A“) rieši všeobecné informácie, prostredníctvom ktorých sa identifikuje kategória OVM podľa §3 vyhlášky č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

V časti „B“ sa zisťuje ako respondent plní resp. neplní implementáciu zákonných požiadaviek ako je napríklad prijatie bezpečnostných opatrení podľa §20 zákona o KB, prijatie stratégie kybernetickej bezpečnosti, politiky informačnej a kybernetickej bezpečnosti. Cieľom tejto časti bolo zistiť, či majú OVM vypracovanú bezpečnostnú dokumentáciu, a či pri jej vytváraní využili externé spoločnosti alebo si dokumentáciu vytvorili svojpomocne, pričom sa riadili niektorou z metodík zverejnených na stránke MIRRI, NBÚ alebo CSIRT. Pri vyplnení časti „B“ respondent uvedie akým spôsobom im uvedené

metodiky (vzory dokumentov) pomohli (ak ich použili) pri spracúvaní bezpečnostnej dokumentácie alebo zlepšili súvisiace procesy.

Časť „B“ rieši aj absolvovanie auditu kybernetickej bezpečnosti certifikovaným audítorom, aká bola miera úspešnosti výsledku auditu v percentách, či má OVM vypracovaný Bezpečnostný projekt podľa požiadaviek zákona o ITVS, či má v rámci organizácie OVM menovaného zamestnanca zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, alebo má vytvorenú pozíciu manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii mimo organizačného útvaru zodpovedného za správu a prevádzku ITVS.

#### 4.2 Metodika zberu údajov formou online dotazníka

Dotazníky a prieskumy sú techniky, v ktorých sa predkladá zoznam uzavretých otázok na získanie presných údajov. Zvyčajne sa používajú v kvantitatívnom výskume, ale môžu sa zahrnúť aj otvorené otázky. Uzavreté otázky umožňujú získať percentuálny obraz pre jednotlivé oblasti prieskumu a umožňujú tak ich rýchlu analýzu. Je to agilná metóda, ktorá berie do úvahy, že nevyžaduje prítomnosť výskumného pracovníka.

Pre účely tohto prieskumu bol na zber údajov vytvorený online dotazník s preddefinovaným súborom uzavretých otázok.

Dotazník obsahuje:

- Časť A: Všeobecné informácie
- Časť B:
  - Implementácia zákonných požiadaviek,
  - Procesy,
  - Ktoré konkrétne usmernenia/metodiky/vzory smerníc použil respondent pri vypracúvaní bezpečnostnej dokumentácie?
- Súbor 38 otázok a jednu časť pre voľnú odpoveď (otázka č. 39).

Na základe pripravený podkladov bola projektovou komisiou KPMG vybraná vzorka 25 respondentov z rôznych kategórií, ktorej bol dotazník dňa 9.8.2022 zaslaný spolu so žiadosťou o vyplnenie.

Online dotazník používa pre analýzu súbor otázok, ktoré boli vopred prediskutované skupinou expertov, pričom zvyčajne sú tieto otázky tvorené dvoma časťami - pevnou, teda vopred danou, a variabilnou, podľa povahy skúmanej oblasti, kde môže respondent vyjadriť svoj pohľad na danú tematiku. Hodnotí sa podľa stupnice 0 až 10, pričom 10 je najvyššia hodnota, 0 - nepomohlo, proces je neimplementovaný, len základne nastavený, 10 - metodika/vzor pomohla vylepšiť proces tak, že je zavedený, zamestnanci sa ním riadia, výstupy procesu sú merané (prostredníctvom KPI) a po zhodnotení výsledkov meraní je proces optimalizovaný.

Kategórie respondentov boli zo sektorov:

- zdravotníctvo,
- verejná správa,
- samospráva,
- štátna správa,
- bankový sektor.

Respondenti pri prieskume neprichádzajú pri vyplňaní odpovedí do styku s výskumnými pracovníkmi, čím je zaručené, že nie sú ovplyvňovaní alebo navádzaní na odpovede. Výhodou prieskumu formou online dotazníka je menšia náročnosť na spotrebu zdrojov alebo času a jeho rýchle vyhodnotenie.

Postup odborného prieskumu formou online dotazníka bol rozdelený na niekoľkých etapách.

1. ETAPA - TVORBA PRACOVNEJ SKUPINY: úlohou pracovnej skupiny bolo zorganizovať postup expertného prieskumu.
2. ETAPA - VYBRATIE REFERENČNEJ VZORKY RESPONDENTOV: v súlade s časťou projektu - Analýza súčasného stavu metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy expertná skupina (výskumní pracovníci) vybrala pre tento účel vzorku respondentov z 5-tich rôznych sektorov, tak aby bola zabezpečená rôznorodosť.
3. ETAPA - FORMULÁCIA OTÁZOK: skupina expertov naformulovala znenie otázok, tak aby boli jasné a jednoznačne interpretované za predpokladu jednoznačných odpovedí. Následne projektová komisia otázky pripomienkovala a schválila.
4. ETAPA - ZASLANIE DOTAZNÍKA: predstavitelia MIRRI zaslali referenčnej vzorke respondentov sprievodný email spolu s odkazom na online dotazník so žiadosťou o zapojenie sa do prieskumu.
5. ETAPA - VYHODNOTENIE PRIESKUMU: odpovede z prieskumu sú po spracovaní prezentované v celkovom vyhodnotení formou kvantitatívnych výsledkov. Na základe týchto výsledkov sa vykonávajú závery prieskumu.

#### 4.3 Vyhodnotenie vlastného prieskumu

Prieskum metodík a štandardov v oblasti kybernetickej bezpečnosti v prostredí verejnej správy sa realizoval vyplnením dotazníka, ktorý predstaviteľ MIRRI zaslal 9.8.2022 zaslal 25-tim respondentom spolu so sprievodným emailom. Na dotazník reagovalo a odpovedalo 16 respondentov v časovom rozmedzí od 9.8.2022 do 31.8.2022. Musíme bohužiaľ konštatovať, že pre časovú tieseň v rámci tejto fázy projektu sa predstaviteľom MIRRI podarilo zabezpečiť veľmi malú vzorku respondentov pre účely tohto prieskumu, čo môže mať za následok skreslené výsledky.

Prieskum nebol robený na reprezentatívnej vzorke z pohľadu celkového počtu OVM. Aj napriek tejto situácii však prieskum môže dať základný obraz súčasného stavu používania metodík a štandardov v oblasti kybernetickej bezpečnosti v podmienkach verejnej správy.

Predstaviteľom MIRRI sa aj napriek malej vzorke respondentov podarilo pokryť päť rôznych kategórií OVM, čo má pozitívny prínos pre tento prieskum.

Výsledky prieskumu a odpovede respondentov boli spracované, kvantifikované a graficky vyhodnotené a sú súčasťou prílohy „Dotazník - OVM – Summary“, kde sú vyhodnotené jednotlivé oblasti.






### **Vyhodnotenie prieskumu metodík a štandardov v oblasti kybernetickej bezpečnosti v prostredí verejnej správy**

#### **ČASŤ A: všeobecné informácie ohľadom OVM**

V rámci prieskumu sa v kategórii I. identifikoval 1 respondent, v kategórii II. 2 respondenti, v kategórii III. 11 respondentov. Dvaja respondenti sa nevedeli identifikovať. Najviac respondentov z kategórie III. tvorili hlavne samosprávne kraje, ministerstvá alebo ostatné ústredné orgány verejnej správy a ostatné štátne orgány uvedené vo vyhláške č. 179/2020, § 3, ods. 4.

*Otázka č. 4 - počet a rozloženie respondentov v kategórii III.*

Kategória III.

	Obec, ktorá je aj krajským mest...	0
	Samosprávny kraj	2
	Ministerstvo a ostatný ústredný ...	5
	Ostatné štátne orgány uvedené ...	4
	Other	0



*Obrázok č. 1 Graf: Všeobecné informácie o OVM*

Z celkového množstva respondentov majú prijaté a dodržiavajú všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 ZoKB a sektorové bezpečnostné opatrenia iba 4 respondenti, ďalších 10 respondentov má bezpečnostné opatrenia v procese prípravy alebo schvaľovania.

**Otázka č. 5 – Prijatie a dodržiavanie bezpečnostných opatrení**

Má Vaša organizácia prijaté a dodržiava všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 ZoKB a sektorové bezpečnostné opatrenia, ak sú prijaté?



Obrázok č. 2 Graf: Prijatie a dodržiavanie bezpečnostných opatrení

Z uvedenej vzorky respondentov možno usúdiť, že veľká časť OVM nie je zatiaľ úplne pripravená a nedodržiava platnú legislatívu, avšak pozitívom je, že z tejto časti respondentov sa je značná časť vo fáze príprav alebo schvaľovania bezpečnostnej dokumentácie a procesov.

Z prieskumu podľa otázok č. 7 a č. 8 ďalej vyplýva, že organizácie, ktoré majú bezpečnostnú dokumentáciu v procese riešenia alebo ju už majú schválenú v prevažnej miere na použili na popis svojich základných procesov dokumenty typu „smernica“. Metodiky boli použité v menšej miere. Táto bezpečnostná dokumentácia je v prevažnej miere definovaná a čaká na schválenie (otázka č. 9). Pri náročnejších procesoch ako napr. kryptografické opatrenia, kontinuita prevádzky, riadenie súladu a pod., organizácie uvádzajú, že tieto procesy nemajú upravené, nastavené (otázka č. 8).

Tabuľka č. 2 Zhodnotenie formy použitej dokumentácie

Oblasť/Proces	Metodika	Smernica	Metodika aj Smernica	Proces nemáme upravený	iné
Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	0	9	4	2	1
Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	3	7	2	3	1
Personálna bezpečnosť	0	9	3	1	3
Riadenie prístupov	0	11	3	1	3
Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	1	6	2	6	1
Bezpečnosť pri prevádzke informačných systémov a sietí	1	9	3	1	2

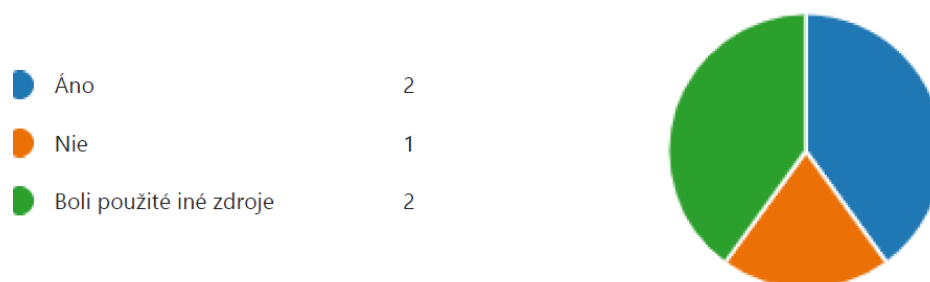


Hodnotenie zraniteľností a bezpečnostných aktualizácií	3	6	0	6	1
Ochrana proti škodlivému kódu	0	8	3	3	2
Sieťová a komunikačná bezpečnosť	0	8	3	4	1
Akvízia, vývoj a údržba informačných sietí a informačných systémov	1	4	3	7	1
Zaznamenávanie udalostí a monitorovanie	0	7	6	6	1
Fyzická bezpečnosť a bezpečnosť prostredia	0	11	2	1	1
Riešenie kybernetických bezpečnostných incidentov	0	7	4	3	2
Kryptografické opatrenia	0	5	3	7	1
Kontinuita prevádzky	1	4	1	9	1
Audit, riadenie súladu a kontrolných činností	2	4	2	6	2
Monitorovanie a vyhodnocovanie dodržiavania Politiky kybernetickej bezpečnosti a informačnej bezpečnosti	1	5	2	7	1

Z hľadiska tvorby bezpečnostnej dokumentácie podľa otázky č. 11 prevládala kombinácia vypracovania dokumentácie svojpomocne + dodávateľsky. V rámci prieskumu bolo formou otázky č. 12 skúmané, aké konkrétne metodiky MIRRI alebo NBÚ boli pri vypracúvaní bezpečnostnej dokumentácie OVM použité. Z celkového počtu respondentov iba menšia časť využila tieto metodiky, preto tu vzniká priestor na zlepšenie, lepšie informovanie a prezentovanie dostupných materiálov z MIRRI alebo NBÚ.

#### Otázka č. 5 – využitie metodík MIRRI alebo NBÚ

V prípade, že ste bezpečnostnú dokumentáciu vypracúvali svojpomocne, riadili ste sa niektorou z metodík zverejnených na stránke MIRRI alebo NBÚ?



Obrázok č. 3 Graf: Využitie metodík MIRRI alebo NBÚ

**ČASŤ B: konkrétne usmernenia/metodiky/vzory smerníc z MIRRI, ktoré použili respondenti pri vypracúvaní bezpečnostnej dokumentácie (otázky č. 14 až 49)**

Tabuľka č. 3 Stav využitia zverejnených dokumentov pri vypracúvaní bezpečnostnej dokumentácie (ot. 14 – 49)

č.	Otázka	ÁNO (počet resp.)	NIE (počet resp.)
14	Prvotná orientácia správcu ISVS	5	11
16	Úvod do KIB_slovník	7	9
18	Legislatívne požiadavky podľa vyhlášky č. 179/2020 Z. z.	8	8
20	Výber dodávateľa služieb kybernetickej bezpečnosti	7	9
22	Vzorová smernica o riadení dodávateľských vzťahov	5	11
24	Checklist	5	11
26	Bezpečnostná politika	6	10
28	Analýza rizík	5	11
30	Manuál bezpečnosti objektu	3	13
32	Plán rozvoja bezpečnostného povedomia	5	11
34	Povinnosti správcu ISVS	7	9
36	Stratégia KIB	2	14
38	Politika KIB	6	10
40	Špeciálne politiky KIB	4	12
42	Business Continuity Plan	4	12
44	Disaster Recovery Plan	3	13
46	Pracovná náplň MKIB	3	13
48	Bezpečnostný projekt ISVS	6	10
<b>Priemer</b>		<b>5</b>	<b>11</b>
<b>Percentuálne vyjadrenie</b>		<b>31,25%</b>	<b>68,75%</b>

Na základe týchto výsledkov môžeme konštatovať, že metodiky MIRRI pri vypracúvaní bezpečnostnej dokumentácie využilo cca 31% respondentov, čo tvorí zhruba jednu tretinu z celkového množstva oslovených OVM.

**ČASŤ B: konkrétne usmernenia/metodiky/vzory smerníc z NBÚ, ktoré použili respondenti pri vypracúvaní bezpečnostnej dokumentácie (otázky č. 50 až 60)**

Tabuľka č. 4 Stav využitia zverejnených dokumentov pri vypracúvaní bezpečnostnej dokumentácie (ot. 50 - 60)

č.	Otázka	ÁNO (počet resp.)	NIE (počet resp.)
50	Jednotný informačný systém kybernetickej bezpečnosti	6	10
52	Hlásenie kybernetických bezpečnostných incidentov	10	6
54	Bezpečnostné opatrenia	8	8
55	Samohodnotenie účinnosti prijatých bezpečnostných opatrení v zmysle ZoKB	0	8
57	Metodika analýzy rizík	1	7
<b>Priemer</b>		<b>5</b>	<b>7,8</b>
<b>Percentuálne vyjadrenie</b>		<b>31,25%</b>	<b>48,75%</b>




Na základe týchto výsledkov môžeme konštatovať, že metodiky NBÚ pri vypracúvaní bezpečnostnej dokumentácie využilo cca 31% respondentov, čo tvorí zhruba tiež jednu tretinu z celkového množstva oslovených OVM. Zhruba 20% respondentov sa v tejto časti nevyjadřilo.

### ČASŤ B: Implementácia zákonných požiadaviek (otázky č. 61 až 68)

V tejto časti prieskumu bolo účelom zistiť stav plnenia ďalším legislatívnych povinností OVM. Oslovené organizácie majú prevažne vypracovanú bezpečnostnú dokumentáciu. Podľa predchádzajúcich otázok, je možné konštatovať, že dokumentácie je v prevažnej miere v stave „spracováva sa, čaká na schválenie alebo je schválená štatutárom“.

#### Otázka č. 61 – stav vypracovania bezpečnostnej dokumentácie

Má Vaša organizácia vypracovanú bezpečnostnú dokumentáciu v súlade s požiadavkami § 2 Obsah a štruktúra bezpečnostnej dokumentácie (vyhláška č. 362/2018 Z. z.)?

	Áno	5
	Nie	3
	Čiastočne spĺňa	8





Obrázok č. 4 Graf: Stav vypracovania bezpečnostnej dokumentácie

Ďalším cieľom prieskumu bolo na tejto vzorke respondentov zistiť aj stav absolvovania auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z..

#### Otázka č. 62 – miera úspešnosti auditu KB

V prípade, že Vaša organizácia absolvovala audit kybernetickej bezpečnosti, aká bola miera úspešnosti výsledku auditu v percentách?

	Naša organizácia neabsolvovala ...	2
	Other	14



Obrázok č. 5 Graf: Miera úspešnosti auditu

Tabuľka č. 5 Percentuálne vyjadrenie úspešnosti auditu KB

ID	Respondent	Percentuálna úspešnosť auditu KB
5	Kategória I.	Menej ako 10%
6	Kategória III.	nemáme vyhodnotenie v percentách
7	Neidentifikoval som sa	52%
8	Kategória III.	65%
9	Kategória III.	47%
10	Kategória III.	Naša organizácia neabsolvovala audit kybernetickej bezpečnosti
11	Kategória III.	priemerne po jednotlivých oblastiach niekde okolo 25%
12	Kategória III.	Naša organizácia neabsolvovala audit kybernetickej bezpečnosti
13	Kategória III.	39%
14	Kategória III.	44,5%
15	Kategória III.	3,55%
16	Neidentifikoval som sa	60%
17	Kategória III.	55%
18	Kategória III.	50%
19	Kategória II.	70%
20	Kategória II.	70%

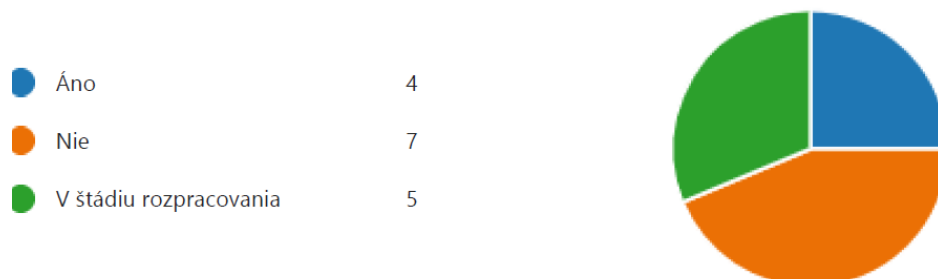
- úspešnosť auditu KB 100% – žiadny z respondentov
- úspešnosť auditu KB 30 až 50% – 4 respondenti z celkového počtu
- úspešnosť auditu KB viac ako 50% – 6 respondentov z celkového počtu
- úspešnosť auditu KB viac ako 70% (vrátane) – 2 respondenti z celkového počtu

Z uvedeného možno konštatovať, že pripravenosť OVM z referenčnej vzorky voči požiadavkám legislatívy je nízka. Organizácie majú ešte veľký priestor na zlepšovanie svojich procesov pri implementácii bezpečnostných opatrení. Túto skutočnosť potvrdzuje aj ďalšia otázka č. 63, kde až 9 respondentov z celkového počtu uvádza, že nemá vedomosť o potrebe zaviesť ďalšie procesy (navyše) okrem základných, vyžadovaných legislatívou (ktoré sú uvedené v otázke č.7). Iba štyria respondenti uvažujú o potrebe zvýšiť úroveň svojej bezpečnosti nad hranicu požadovanú zákonom a to napr. rozšírením procesov v oblasti kontinuity prevádzky, navýšením počtu zamestnancov zaoberajúcich sa kybernetickou bezpečnosťou, nastavením krízového manažmentu.

Súčasťou bezpečnostnej dokumentácie je aj bezpečnostný projekt podľa ZoITVS

*Otázka č. 65 – stav spravovania bezpečnostného projektu.*

Má Vaša organizácia vypracovaný Bezpečnostný projekt/Bezpečnostné projekty IS podľa ZolTVS?



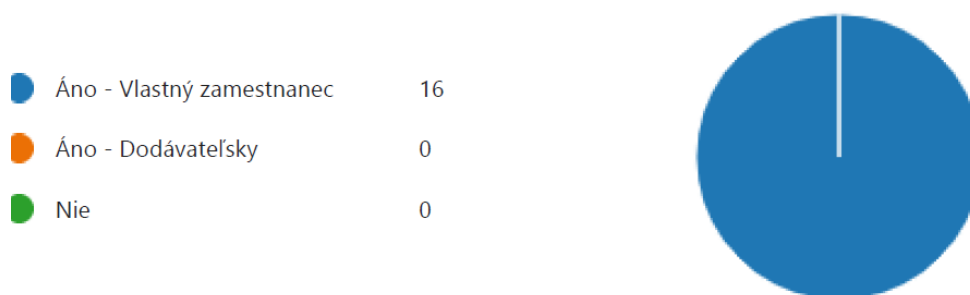
*Obrázok č. 6 Graf: Stav vypracovania bezpečnostného projektu*

Bezpečnostný projekt má vypracovaný iba 25% respondentov, ďalších 31% má túto dokumentáciu v stave rozpracovania. Z celkového počtu Organizácií, ktoré uvideli, že majú bezpečnostný projekt vypracovaný alebo v stave rozpracovania, sa metodikou MIRRI zverejnenou na webovom sídle riadila iba jedna organizácia (otázka č. 66).

Podľa prieskumu majú všetky oslovené organizácie pre účely koordinácie kybernetickej a informačnej bezpečnosti určeného samostatného zamestnanca.

*Otázka č. 67 – koordinácia činností KB a IB*

Má Vaša organizácia zamestnanca zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti?






*Obrázok č. 7 Graf: Koordinácia činností KIB*

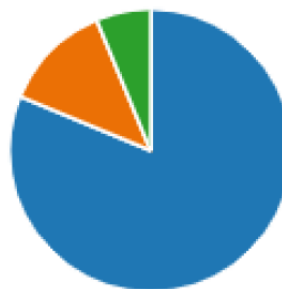
Súčasťou prieskumu bolo aj overenie skutočnosti, či má organizácia vytvorenú pozíciu manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu **mimo organizačného** útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy, tak ako si to vyžaduje legislatíva. Prevažná väčšina respondentov pre účel splnenia tejto legislatívnej povinnosti, vyčlenila samostatného, vlastného zamestnanca

spadajúceho pod štatutára, ktorý je priamo zodpovedný za riadenie kybernetickej a informačnej bezpečnosti (Otázka č. 68).

*Otázka č. 68 – vytvorenie samostatnej pozície MKB priamo pod štatutárom*

Má Vaša organizácia vytvorenú pozíciu manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu mimo organizačného útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy?

	Áno - Vlastný zamestnanec	13
	Áno - Dodávateľsky	2
	Nie	1



*Obrázok č. 8 Graf: Vytvorenie samostatnej pozície pod štatutárom*

## 5 Záver

Na základe posúdenia súčasného stavu metodík a štandardov a záverov vlastného prieskumu je možné konštatovať, že vznikla akútna potreba aktualizácie existujúcej dostupnej vzorovej dokumentácie, s cieľom vytvoriť komplexný systém obsahujúci jednotný súbor dokumentov a vzorových šablón vhodných pre efektívny návrh, implementáciu a optimalizáciu procesov riadenia KB účinnú implementáciu bezpečnostných opatrení v oblasti kybernetickej a informačnej bezpečnosti v zmysle požiadaviek platnej legislatívy SR a EÚ.

Poskytované metodiky, vzory, šablóny a ďalšia dokumentácia sprístupnená na portáloch verejnej správy, najmä na webovom sídle MIRRI, nereflektujú v požadovanej miere na legislatívne požiadavky a štandardy pre oblasť KIB. Po obsahovej stránke a po stránke pokrytia legislatívnych požiadaviek nespĺňajú ani základné požiadavky na metodickú podporu pre aplikovanie a implementáciu bezpečnostných opatrení, ani pre zavedenie a nastavenie procesov riadenia KIB. Uvedená dokumentácia je nekonzistentná, s rozdielnou štruktúrou a nie je možné jednoznačne definovať oblasť bezpečnosti, na ktorú sa má aplikovať.

Táto nejednoznačnosť v jej použiteľnosti a to, ktorá oblasť bezpečnosti uplatnením tej - ktorej metodiky či vzoru bude vyriešená, je spôsobená aj tým, že v niektorých prípadoch je poskytnutá len metodika, v niektorých prípadoch len vzor smernice bez ďalšieho usmernenia jej aplikácie jednak v procese tvorby interného riadiaceho aktu v danom OVM a jednak v procese zavádzania bezpečnostných opatrení. Tak, ako je poskytnutá dokumentácia koncipovaná, nezaručí, že OVM budú podľa nej schopné vytvoriť si vlastnú bezpečnostnú dokumentáciu, nastaviť procesy a zaviesť bezpečnostné opatrenia do praxe.

Povaha poskytnutej dokumentácie môže navodiť dojem, že bola vypracovaná v časovej tiesni s cieľom aspoň čiastočne pokryť požiadavky legislatívy.

Absentuje aj akékoľvek usmernenie ako implementované procesy ďalej optimalizovať a zlepšovať prostredníctvom jasne stanovených metrík na meranie účinnosti zavedených procesov a opatrení.

Poskytnutá dokumentácia nie je dostatočne komunikovaná a prezentovaná daným zástupcom OVM a ich zamestnancom na pozíciách bezpečnostných špecialistov tak, aby ju dokázali efektívne uchopiť a v danom rozsahu zaviesť. Absentuje ďalšia metodická podpora vo forme možných konzultácií vrátane definovania kontaktných osôb kompetentných a schopných poskytnúť podporu pri riešení problémov súvisiacich s implementáciou v danej oblasti.

Od poskytovanej metodickej pomoci na úrovni ministerstva sa očakáva, že podpora bude poskytnutá komplexne vo forme jednotného metodického rámca, ktorý nebude obsahovať iba metodiky, vzorové šablóny a dokumenty, ale zároveň poskytne štruktúrované inštrukcie,



ktoré sú jasne a jednoznačne definované reflektujúce na kategóriu, do ktorej OVM spadá podľa ZoITVS.

Na základe výstupov dotazníkového prieskumu názorov OVM vyplýva, že sprístupnené metodiky a vzorové dokumenty neboli pre aplikovanie požiadaviek súčasnej legislatívy v oblasti KIB postačujúce, vo väčšine prípadov neboli využité, alebo využité čiastočne a respondenti uviedli, že si OVM dokumentáciu a procesy tvorili zväčša svojpomocne alebo dodávateľsky.

Pre jednoduchú a efektívnu navigáciu v súboroch dokumentov je preto nevyhnutné vytvoriť štruktúrovaný komplexný systém, prostredníctvom ktorého bude možné zaradiť jednotlivé OVM do určených kategórií a navigovať zodpovedné osoby zastupujúce dané OVM (najvhodnejšie podľa rolí, bezpečnostní špecialisti), ktoré „balíčky“ (moduly) opatrení, vzorovej dokumentácie a odporúčaní sa ich týkajú a ako ich majú implementovať a naďalej udržiavať (a optimalizovať). V podkapitole 3.2 sú uvedené návrhy a odporúčania na zlepšenie súčasného stavu poskytnutia pomoci OVM zo strany orgánu vedenia (MIRRI), pre ktoré je povinnosťou vydávať metodické usmernenia, usmerňovať a koordinovať orgány riadenia na účely jednotného spôsobu výkonu riadenia v správe informačných technológií verejnej správy a centrálneho riadenia informatizácie spoločnosti, vydávať štandardy a výkladové stanoviská, zverejňovať na ústrednom portáli rozhodnutia, iné dokumenty a informácie týkajúce sa informačných technológií verejnej správy a informatizácie verejnej správy.

Dokument „Právna analýza súčasného stavu právnej úpravy kybernetickej bezpečnosti v slovenskej republike“ (JUDr. Jozef Andraško, PhD., JUDr. Matúš Mesarčík, PhD., LL.M), ktorého cieľom je zmapovať legislatívu kybernetickej bezpečnosti v SR a navrhnuť čiastkové či koncepcné riešenia popisuje analýzu súčasného stavu z legislatívneho pohľadu. Dokument sa venuje identifikovaným problémovým oblastiam, a taktiež navrhuje riešenia legislatívnych úprav vo forme troch alternatív.

Legislatívne úpravy budú na základe zistení z uvedenej analýzy zrejme vyžadovať buď konsolidáciu rozdielnych legislatívnych požiadaviek (ZoITVS vs. ZoKB) do jedného zákona, alebo harmonizáciu existujúcich zákonov a súvisiacich vyhlášok.

Z pohľadu tejto analýzy, teda roviny praktickej implementácie sprístupnených metodík a existujúcich zdrojov a na základe záverov z preskúmania ich súčasného využívania, spomenuté vyhlášky navrhujú rozdielny prístup ku kategorizácii IS a sietí (ZoKB vo Vyhláške č. 362/2018) a rozdeleniu organizácií do kategórií definovaných „napevno“ (ZoITVS vo Vyhláške č. 179/2020, Kategória I. Až III.) Bezpečnostné opatrenia sa potom aplikujú podľa identifikovaných kategórií v definovaných rozsahoch.

Tento rozdielny prístup je značne mätúci a implementáciu komplikuje, aj keď sa v niektorých prípadoch budú požiadavky čiastočne zhodovať, iba sú formulované iným spôsobom. Za zváženie možno stojí aj hybridný model, teda prístup, kde sa definujú kritériá podľa dopadových a ďalších kritérií, a v niektorých prípadoch je možné použiť napevno nastavené kategórie OVM, prípadne s ďalším ošetrovaním výnimiek.

Na niektorý z týchto modelov bude potom potrebné nastaviť aj navrhovanú schému – súbor metodických dokumentov a vzorov tak aby dané kategórie sprehľadnili rozdelenie požiadaviek na aplikovanie procesov riadenia KIB a súvisiacich bezpečnostných opatrení. Výsledkom by mal byť model, ktorý prácu s aplikovaním bezpečnostných požiadaviek (na technickej, technologickej, ale aj procesnej úrovni) a tiež nastavovaním procesov riadenia KIB zjednodušuje prevádzkovateľom a správcom (OVM) na maximálnu možnú mieru, pričom priebežne reflektuje na zmeny v požiadavkách legislatívy SR a EÚ a tiež aplikuje súčasné požiadavky na zachovania princípu minimálnych nákladov, komplexne previazaných riešení, ktoré synergicky budú tvoriť dostatočnú podporu tak aby bola dosiahnutá požadovaná miera kybernetickej odolnosti OVM ako celku.

### 5.1 Návrhy a odporúčania

- Aktualizovať existujúcu dokumentáciu a vzorové šablóny a vytvoriť jednotný súbor dokumentov a vzorových šablón pre efektívnu a čo najjednoduchšiu implementáciu procesov riadenia KIB a opatrení kybernetickej a informačnej bezpečnosti v zmysle požiadaviek platnej legislatívy ako aj vytvorenie metodických materiálov pre zavádzanie a aplikáciu pravidiel kybernetickej bezpečnosti; pri aktualizácii dokumentácie reflektovať na aktuálne trendy a vývoj legislatívy v oblasti KIB, a to nielen na národnej úrovni a na úrovni EÚ (napr. aktuálne pripravovaná smernica NIS2), ale aj celosvetovej úrovni, napr. zmeny v normách radu ISO 27000 a NIST.
- Vytvoriť prehľadný, koncepčne ucelený súbor metodík vo forme jednotného metodického rámca pre jednotlivé kategórie OVM tak, aby spĺňal požiadavky súčasnej legislatívy SR a EÚ, nadväzoval na aktuálne technologické štandardy a umožnil používateľovi jednoducho a efektívne implementovať dané bezpečnostné opatrenia a vytvoriť, implementovať a optimalizovať procesy riadenia KIB.
- Jednotný metodický rámec, by mal zahŕňať nielen súbor metodík, vzorových šablón a dokumentov, ale poskytovať štruktúrované inštrukcie, jasne a jednoznačne definované reflektujúce na kategóriu, do ktorej OVM spadá podľa ZoITVS.
- Jednotný metodický rámec by mal predstavovať komplexný systém vo forme webového sídla (portálu), ktorý OVM prevedie celým procesom implementácie legislatívnu stanovených požiadaviek na zavedenie procesov riadenia KIB a bezpečnostných opatrení. Súčasťou funkcionality portálu by malo byť napríklad usmernenie pre zaradenie OVM do príslušnej kategórie, samohodnotenie úrovne súčasného stavu implementovaných bezpečnostných opatrení, meranie výkonnosti zavedených procesov a bezpečnostných opatrení v praxi, ďalej by mal obsahovať moduly pre jednotlivé oblasti KIB vrátane modulu pre vzdelávanie zamestnancov VS, ako podpora procesu zvyšovania bezpečnostného povedomia.
- Definovať technické a procesné nástroje a postupy na splnenie bezpečnostného minima spĺňajúce súčasné technologické požiadavky pre oblasť KIB.
- Navrhnuť postupy pre penetračné testovanie v prostredí verejnej správy, vrátane metodiky výkonu penetračných testov, reflektujúcej jednotlivé stanovené kategórie

OVM, definovanie požiadaviek na výstupy penetračných testov v súlade s aktuálnymi medzinárodnými štandardmi.

- Vypracovať súbor etických štandardov pre sektor VS.
- Zabezpečiť pravidelnú aktualizáciu sprístupnenej dokumentácie, a to voči existujúcej legislatíve SR, taktiež voči legislatívnym požiadavkám a nariadeniam zo strany EÚ ako aj aktualizáciu zoznamov a databáz (napr. databázy hrozieb a zraniteľností) a technologických štandardov (napr. aktualizácia definícií kryptografických požiadaviek s ohľadom na existujúce kryptografické štandardy). Aktualizácia by mala reflektovať aj na zmeny v štruktúrach OVM a v prípade, že je to nevyhnutné, aktualizovať aj samotnú kategorizáciu OVM.
- Zabezpečiť dostatočne efektívnu, včasnú a transparentnú informačnú kampaň na podporu využívania vypracovaných riešení (vrátane zaškoľovacích/školiacich kurzov na používanie uvedených metodík a vzorov).
- Zaviesť systém kontinuálneho zvyšovania bezpečnostného povedomia, ktorý bude podporovaný aj v jednotnom metodickom rámci prostredníctvom príslušných metodických usmernení a pokynov vrátane metrík na meranie a optimalizáciu výkonnosti procesov vzdelávania.
- Zaviesť systém vzdelávania bezpečnostných špecialistov podľa jednotlivých pozícií a rolí stanovených legislatívou.
- Vzhľadom na vzájomnú nekompatibilitu súčasných legislatívnych rámcov v oblasti KIB a štandardov (ZoKB vs. ZoITVS vs. napr. rodina noriem ISO 27000) odporučiť (vyvolať diskusiu so zainteresovanými stranami kompetentnými na zmenu legislatívy) ich harmonizáciu aj v súvislosti s pripravovanou smernicou NIS2, ktorej implementácia do podmienok SR bude nevyhnutná a prípadne ďalšími štandardami (ISO 27001 a 27002 taktiež prechádzajú významnými zmenami).

## Zoznam použitých zdrojov

- [1] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- [2] Vyhláška Úradu podpredsedu vlády SR pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- [3] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- [4] 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
- [5] [www.mirri.gov.sk](http://www.mirri.gov.sk)
- [6] [www.nbu.gov.sk](http://www.nbu.gov.sk)
- [7] <https://gdpr.eu/>
- [8] <https://www.enisa.europa.eu/about-enisa/regulatory-framework>
- [9] Právna analýza súčasného stavu právnej úpravy kybernetickej bezpečnosti v slovenskej republike (Andraško, Mesarčík, 2022)
- [10] [www.enisa.europa.eu](http://www.enisa.europa.eu)