ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

Zápisnica z XI. zasadnutia Rady vlády SR
pre digitalizáciu verejnej správy a jednotného digitálneho trhu (ďalej len „Rada vlády“)

Číslo: 4412/2019/oSAEG-3

Dátum: 1. júl 2019, 9.00 hod
Miesto konania: Úrad vlády SR, Bratislava, zasadačka č. 103
Prítomní:

	rezort	menovaní	prítomní
predseda Rady vlády	Úrad podpredsedu vlády SR pre investície a informatizáciu (ÚPVII)	Richard Raši	Richard Raši
podpredseda	Ministerstvo vnútra SR	Rudolf Urbanovič	Pavol Maliarik v z.
podpredseda	ITAS	Emil Fitoš	Emil Fitoš
stály člen	Ministerstvo financií SR	Radko Kuruc	Erik Minarovič v z.
stály člen	Ministerstvo školstva, vedy, výskumu a športu SR	Peter Krajňák	Branislav Baláž v z.
stály člen	Ministerstvo zdravotníctva SR	Stanislav Špánik	Michal Kondáš v z.
stály člen	Ministerstvo hospodárstva SR	Rastislav Chovanec	Miriam Letašiová v z.
stály člen	Ministerstvo práce, sociálnych vecí a rodiny SR	Ivan Švejna	ospravedlnený
stály člen	Ministerstvo dopravy a výstavby SR	Ladislava Cengelová	Ladislava Cengelová
stály člen	ÚPVII	Jaroslav Kmeť	Jaroslav Kmeť
stály člen	Úrad vlády SR	Matúš Šutaj Eštok	Matúš Šutaj Eštok
stály člen	NASES	Peter Ďurica	ospravedlnený
stály člen	NBÚ	Roman Konečný	Rastislav Janota v z.
stály člen	ZMOS	Milan Muška	Adrián Belánik v z.
stály člen	Združenie samosprávnych krajov SK8	Ján Marušinec	neospravedlnený
stály člen	Slovenská informatická spoločnosť	Milan Ftáčnik	Milan Ftáčnik
stály člen	Partnerstvá pre prosperitu	Milan Ištván	Štefan Červenka v z.
stály člen	ITAS	Marián Marek	Marián Marek
stály člen	Slovensko.Digital	Ľubomír Illek	Ľubomír Illek
nestály člen	Ministerstvo spravodlivosti SR	Edita Pfundtner	Attila Bencze v z.
nestály člen	Ministerstvo kultúry SR	Konrád Rigó	ospravedlnený
nestály člen	Ministerstvo zahraničných vecí a európskych záležitostí SR	František Ružička	ospravedlnený
nestály člen	Úrad na ochranu osobných údajov	Vladimír Šafárik	Vladimír Šafárik
tajomníčka	ÚPVII	Edita Antoniaková	Edita Antoniaková
prizvaný	Ministerstvo hospodárstva SR		Peter Szakács
prizvaný	ÚV SR		Miriama Letovanec

prizvaný	ÚV SR		Michal Jerga
prizvaný	ÚPVII		Radoslav Repa
prizvaný	ÚPVII		Tomáš Jucha
prizvaný	ÚPVII		Valentína Michálková
prizvaný	ÚPVII		Ervín Šimko
prizvaný	ÚPVII		Vladimír Sedláček
prizvaný	ÚPVII		Martin Bezek
prizvaný	ÚPVII		A. H. Suchánková

Program zasadnutia:

Návrh programu XI. zasadnutia bol spolu s materiálmi zaslaný členom Rady vlády 21.6.2019.

Predseda Rady vlády dal priestor na doplnenie alebo zmenu programu rokovania. P. Illek navrhol doplniť do bodu rôzne diskusiu k návrhu zákona o identifikátore fyzickej osoby. P. Kmeť požiadal o zaradenie súhrnnej implementačnej správy za rok 2018 na začiatok rokovania, vzhľadom na neodkladné povinnosti.

Program XI. zasadnutia Rady vlády jednomyseľne schválili všetci členovia nasledovne:

1. Otvorenie
2. Súhrnná implementačná správa za rok 2018 - na diskusiu, predkladá ÚPVII a Úrad vlády SR
3. Návrh dokumentu "Akčný plán digitálnej transformácie Slovenska na roky 2019 - 2022" - na pripomienky, predkladá ÚPVII
4. Návrh dokumentu "Strategická priorita Informačná a kybernetická bezpečnosť" - na schválenie, predkladá ÚPPVII
5. Návrh na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh - na pripomienky, predkladá ÚPVII
6. Návrh dodatku č. 1 k Rokovaciemu poriadku Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh - na schválenie, predkladá ÚPVII
7. Príprava implementácie nariadenia EP a Rady č. 2018/1724 o zriadení jednotnej digitálnej brány v podmienkach SR - na informáciu, predkladá ÚPVII
8. Rôzne – diskusia k návrhu zákona o identifikátore fyzickej osoby
9. Záver

K bodu 1:

Podpredseda vlády SR pre investície a informatizáciu a predseda Rady vlády p. Richard Raši privítal zúčastnených na XI. zasadnutí. Poďakoval prítomným za účasť a poprosil zúčastnených, aby rokovali odborne, vecne a stručne.

Predseda Rady vlády na úvod konštatoval, že Rada vlády je uznášaniaschopná. Z 23 členov Rady vlády bolo 19 prítomných, z toho 17 stáli a 2 nestáli členovia.

K bodu 2:

Predseda Rady vlády uviedol bod 2. Súhrnnú implementačnú správu za rok 2018“. Materiál bol vypracovaný Úradom vlády SR a schválený uznesením vlády SR č. 188 dňa 17.4.2019 ako príloha k Programu stability SR. Predseda Rady vlády odovzdal slovo riaditeľke Implementačnej jednotky p. Letovanec, ktorá uviedla materiál. Následne predseda Rady vlády otvoril diskusiu.

P. Letovanec predstavila Implementačnú jednotku. Implementačná jednotka vznikla na Ministerstve financií ako druhý pilier Útvaru hodnoty za peniaze, od 1.8. 2018 je na Úrade vlády SR. Úlohou Implementačnej jednotky je dozerať, monitorovať plnenie implementácií a opatrení, ktoré sú definované v revízii výdavkov pre informatizáciu SR v uznesení 461/2016 - v októbri 2016 ako súčasť návrhu rozpočtu 2017 – 2019.

Je to dokument uzatvorený, nemenný, ktorý odzrkadľuje plnenie revízie výdavkov pre informatizáciu. V rámci tohto dokumentu implementačná jednotka hodnotí každé jedno z 32. opatrení, ktoré boli identifikované v roku 2017 a časť z nich je už splnená. Niektoré opatrenia sú ešte stále v procese, alebo v progrese. V súčasnosti je to 21 opatrení a v podstate ukladá Úradu podpredsedu vlády SR pre investície a informatizáciu ešte dodatočné úlohy. Hlavné odporúčanie Implementačnej jednotky je to, aby sa podarilo štrukturálne zlepšenie a aby sa úsporné a rozpočtové opatrenia intenzívnejšie plnili.

Dokument mapuje zmeny od 1.1. 2018 do 31.12. 2018. V súčasnosti Implementačná jednotka začína pracovať na update tohto dokumentu. Priebežná Implementačná správa 2019, ktorá bude mapovať prvých 6 mesiacov, bude súčasťou prílohy zákona o štátnom rozpočte na roky 2020 – 2022.

Implementačná jednotka v dokumente za rok 2018 tiež prehodnotila opatrenia revízie výdavkov na informatizáciu z dôvodu, že bolo prijatých ešte množstvo ďalších strategických dokumentov. Tím zložený z ÚHP, ÚPVII a Implementačnej jednotky pracuje na úprave týchto opatrení.

Predseda Rady vlády poďakoval za správu a otvoril diskusiu.

P. Illek upozornil, že v implementačnej správe je zo strany ÚPVII veľa nesplnených úloh a malý dosiahnutý progres. P. Ftáčnik by očakával, aby bolo uvedené, kto je zodpovedný za neplnenie.

P. Sedláček vysvetlil, že sekcia ITVS plní úlohy, pričom niektoré úlohy s termínom priebežne nemôžu byť označené ako splnené, keďže sme v polovici. V súčasnosti pracujeme spolu s ÚHP a Implementačnou jednotkou na prioritizácii úloh z implementačného plánu. Pripravujeme prehodnotenie úloh a ich rozbitie na menšie časti.

P. Ftáčnik žiadal, aby nové pohľady a návrhy, úpravy boli predložené na posúdenie Rade vlády. P. Kmeť reagoval, že návrh môžeme dať na informáciu, keďže nositeľom témy je ÚHP. P. Letovanec doplnila, že správa bude v prílohe k zákonu o štátnom rozpočte, a predloženie na diskusiu v Rade vlády pravdepodobne ÚHP povolí na diskusiu. Ďalej doplnila, že úlohy nebudú zrušené, ale prehodnotené, skôr rozbité na viacero úloh. Rozpracovaný je analytický materiál z pohľadu hodnoty za peniaze, ktorý bude k dispozícii na konci roka 2019. Implementačné správy budú ešte dve.

P. Illek konštatoval, že každoročne sa predkladá na rokovanie vlády informácia o plnení NKIVS, podľa jeho názoru z implementačnej správy vidieť lepšie, čo sa splnilo a čo nie, preto navrhol, aby informácia o plnení NKIVS obsahovala plnenie opatrení sledovaných v Implementačnej správe. Predseda Rady vlády vyjadril s tým súhlas.

Predseda Rady vlády poďakoval za pripomienky a diskusiu a uzavrel diskusiu.

K bodu 3:

Predseda Rady vlády uviedol bod 3 „Akčný plán digitálnej transformácie Slovenska na roky 2019 – 2022“, ktorý vypracovala Sekcia digitálnej agendy ÚPVII. Materiál prešiel medzirezortným pripomienkovým konaním a 24.6.2019 bol predmetom rokovania Hospodárskej a sociálnej Rady SR. Materiál bude predložený na rokovanie vlády SR na začiatku júla 2019.

Predseda Rady vlády odovzdal slovo generálnemu riaditeľovi Sekcie digitálnej agendy p. Repovi, ktorý oboznámil prítomných s detailmi a obsahom akčného plánu. Následne predseda Rady vlády otvoril diskusiu k bodu 3.

P. Ftáčnik konštatoval, že nebola predložená doložka finančných vplyvov. Ďalej poznamenal, že sú spomenuté nepodstatné veci, napr. že študenti majú v osnovách IT a nie je spomenutá kvalita slovenských IT firiem, ktoré predávajú služby do zahraničia. Materiál by mal obsiahnuť celé hospodárstvo, širší priemysel. Materiál je dobrým východiskom a očakáva prerokúvanie odpočtov na rokovaní Rady vlády.

P. Repa doplnil, že ide o živý materiál, ktorý sa bude dopĺňať a spresňovať, pričom bolo dôležité, aby východiskový materiál bol schválený.

P. Fitoš podotkol, že mnohé opatrenia, napr. vzdelávanie a digitálny inovačný hub, je potrebné naštartovať už v roku 2019 a položil otázku, či sú zabezpečené finančné prostriedky na rok 2019.

P. Repa poďakoval za podnetné pripomienky, ktoré budú zapracované. Schválením materiálu sa pridáme k inovatívnym štátom, pričom sa SR môže zapojiť do projektov a získať aj netradičné zdroje. Napr. EK bude podporovať centrá malých inovácií, startup-y. Indexom DESI hodnotí EK širší index priemyslu, tu ide o priemysel ako taký, ktorý musí prejsť digitalizáciou. ÚPVII vytvorí zásobník nových projektov, ktoré prerokuje v pracovnej skupine a v Rade vlády.

P. Letašiová konštatovala, že ide o prierezový materiál, pričom vyzdvihla dobrú spoluprácu s ÚPVII, pri kreovaní materiálu. Rovnako v nadväznosti na akčný plán inteligentného priemyslu, CDI a smart cities sa teší na spoluprácu a úspešnú implementáciu.

P. Illek sa vyjadril, že dokument je postavený príliš analyticky a v teoretickej rovine a považoval by za viac ako vhodné, aby boli ciele stanovené konkrétne. Je navrhnutých veľa úloh pre verejnú správu. Taktiež sa vyjadril, že mnohé z uvedených úloh sú veľmi ťažko dosiahnuteľné, až nesplniteľné. Dve úlohy týkajúcich sa blockchain nepovažuje za potrebné pre verejnú správu.

P. Repa nadviazal, že oblasť blockchain podporuje Európska komisia, SR sa zúčastňuje na projekte EK, a rovnako táto oblasť je hodnotená v rámci EÚ. Preto boli navrhnuté úlohy, kde nám novátori urobia analýzy a poradia v tejto novej oblasti. K financovaniu doplnil, že k finančným vplyvom k materiálu sa uskutočnili rokovania s MF SR, za podpory vedenia úradu. Celý rozpočet na akčný plán sa odhaduje na 10 mil. EUR, na rok 2019 je to 300 tis EUR.

Predseda Rady vlády dodal, že finančné prostriedky na úlohy akčného plánu sú zabezpečené, čo nebývalo pravidlom. K oblasti blockchain požiadal o otvorenosť k novým témam.

Predseda Rady vlády poďakoval za pripomienky a diskusiu a dal hlasovať o návrhu uznesenia k predmetnému materiálu. Konštatoval, že uznesenie č. 6/2019 Rada vlády schválila.

K bodu 4:

Predseda Rady vlády uviedol bod 4 návrh materiálu „Strategická priorita Informačná a kybernetická bezpečnosť“. Materiál bol odsúhlasený v pracovnej skupine k strategickým prioritám informatizácie: Kybernetická bezpečnosť. Prekladateľom materiálu je sekcia kybernetickej bezpečnosti ÚPVII. Materiál bol vypracovaný v zmysle úlohy B.5. uznesenia vlády SR č. 437/2016 k Národnej koncepcii informatizácie verejnej správy. Slovo odovzdal riaditeľovi odboru kybernetickej a informačnej bezpečnosti p. Šimkovi, aby predstavil materiál. Následne po predstavení dokumentu predseda Rady vlády otvoril diskusiu k bodu 4.

Ako prvý reagoval p. Illek, ktorý poznamenal, že do kapitoly 4 materiálu je potrebné doplniť informácie o termínoch a finančnom zaťažení a jasnejšie určiť cieľ úlohy.

Niektoré termíny sú nereálne. Napríklad 1 rok na personálne zabezpečenie na OVM. Z pohľadu financií sa peniaze rozdelili na 3 alebo 4 centrálne projekty na kybernetickú bezpečnosť a množstvo menších orgánov verejnej správy nedostalo žiadne prostriedky.

P. Šimko reagoval, že termíny ustanovuje zákon o kybernetickej bezpečnosti, ako aj zákon o ITVS. Čo sa týka financií, vývoj je veľmi dynamický a nevieme určiť spoľahlivo dopady. Na to nadviazal p. Janota, ktorý dodal, že pokiaľ sa nevyčísli hodnota, financovanie sa neuskutoční.

P. Šimko ďalej dodal, že je mnoho národných projektov a projektov kybernetickej bezpečnosti, od budovania spôsobilosti a vzdelávania pracovníkov na všetkých úrovniach, kde sú finančné dopady vyčíslené. Samotná pracovná skupina sa vyjadrila, že nie je možné vyčísliť reálny odhad. Konkrétny odhad bude možné stanoviť po verejnom obstarávaní.

P. Illek pokračoval pripomienkou týkajúcou sa klasifikácie informácie systémov, ktoré pre bezpečnosť neznamená prínos, skôr si myslí, že by pomohlo zjednotiť doterajšie opatrenia.

P. Šimko reagoval, že klasifikácia nebude odlišná od tých, ktoré už existujú, a budeme vychádzať z pripravovanej vyhlášky. Predseda Rady vlády doplnil, že pri vytváraní klasifikácie informácií je potrebné urobiť prierez všetkých legislatívnych opatrení a legislatívy, ktorá už bola prijatá.

P. Janota z NBÚ doplnil, že k téme klasifikácie je platná vyhláška, ktorá však nevzťahuje na ISVS. Ideálny stav v oblasti klasifikácie by bolo zjednotenie. Klasifikácia vznikala dosť dlho a bol to kompromis medzi precíznosťou a schopnosťou realizovať klasifikáciu.

P. Šimko dodal, že nebudú sa vytvárať žiadne nové klasifikácie, ktoré by boli rozporuplné. Cieľom je zjednotiť to, aby kybernetická bezpečnosť bola v jednotná.

P. Baláž mal otázku ohľadom základného cieľa uvedeného dokumentu. P. Šimko odpovedal, že strategická priorita pri budovaní kybernetickej bezpečnosti obsahuje súčasný stav a cieľ, kam sa chceme v budúcnosti dostať.

P. Baláž dodal, že cieľový stav je podľa jeho názoru dosť nekonkrétny. Ďalšou pripomienkou je vzdelávanie v KIB, ktoré s MŠVVŠ SR nikto nekonzultoval. P. Šimko odpovedal, že ide o riešenie z národných projektov.

Predseda Rady vlády doplnil, že aj napriek veľkej dynamiky z hľadiska nákladovosti, je potrebné uviesť sumy, ktoré nebudeme musieť revidovať. Otázne je, či to vieme urobiť a či takýto dokument v budúcom období nevyvolá otázky, že odhadované finančné prostriedky budú o pár rokov odlišné.

P. Baláž doplnil, že ak chceme vzdelávať, mali by sme vedieť povedať koľko ľudí chceme preškoliť a koľko to bude približne stáť. V rámci požiadaviek si myslí, že vieme financie vyčísliť. Ak pôjde o financovanie z rozpočtu, konkrétne čísla netreba uvádzať, ale v prípade požiadaviek nad rámec ŠR je to potrebné.

P. Illek dodal, že pripomienku mienil pozitívne, nejde o kritiku, financie sú potrebné a postupom času sa môžu spresňovať.

P. Ftáčnik vyjadril, že úlohy uvedené v dokumente sú väčšinou organizačné, s výnimkou vzdelávania a vzdelanie je opreté o eurofondové projekty, ktoré sú už schválené. V tejto chvíli nevidí potrebu navyšovania rozpočtu. Z dokumentu nevyplývajú požiadavky na ďalšie financie, tento dokument sa dá zrealizovať z tých prostriedkov, ktoré sú už na ceste.

Predseda Rady vlády dodal, že je potrebné, aby to v dokumente bolo uvedené, pretože ak sú národné projekty MŠVVŠ SR schválené a v realizácii, majú vypracovaný aj rozpočet. Vyjadril požiadavku na p. Šimka, aby z dokumentu bolo jasné, že projekty MŠVVŠ SR sú finančne zabezpečené z EŠIF ako národné projekty. Zvyšok bude financovaný v rámci existujúcich rozpočtov a tým pádom je otázka ohľadom financovania jasná.

Predseda Rady vlády dal hlasovať o dokumente s pripomienkami MŠVVŠ SR, NBÚ, p. Ftáčnika a p. Illeka v tých častiach, ktoré vieme zvládnuť. Rada vlády schválila dokument Strategická priorita informačná a kybernetická bezpečnosť s pripomienkami. Konštatoval, že uznesenie č. 7 Rada vlády schválila s pripomienkami.

K bodu 5 a 6:

Ďalšími bodmi v programe bol návrh na zmenu a doplnenie Štatútu Rady vlády a návrh dodatku č. 1 k Rokovaciemu poriadku Rady vlády. Materiály predstavila p. Antoniaková, tajomníčka Rady vlády. Cieľom návrhov je zjednotiť postavenie stálych a nestálych členov Rady vlády pri účasti na zasadnutiach a reflektuje na organizačnú zmenu na ÚPVII, ktorou došlo k zániku pôvodnej sekcie riadenia informatizácie a vzniku štyroch samostatných sekcií.

Návrh na zmenu Štatútu Rady bude predložený na MPK, následne na rokovanie a schválenie vláde SR. Schválenie Rokovacieho poriadku je v kompetencii Rady vlády. Účinnosť obidvoch dokumentov bude rovnaká.

Po predstavení materiálov predseda Rady vlády otvoril diskusiu k bodom 5 a 6. Členovia Rady vlády neuplatnili žiadne pripomienky.

Predseda Rady vlády uzatvoril diskusiu a následne dal hlasovať o návrhu uznesenia č. 8 k návrhu na zmenu a doplnenie Štatútu Rady vlády a uznesenia č. 9 k dodatku č. 1 k Rokovaciemu poriadku Rady vlády. Obe uznesenia Rada vlády schválila.

K bodu 7:

Predseda Rady vlády uviedol ďalší materiál a to Informáciu o príprave implementácie nariadenia EP a Rady č. 2018/1724 o zriadení jednotnej digitálnej brány v podmienkach SR. Predložený materiál bol vypracovaný na základe Nariadenia EÚ 2018/1724 o zriadení Jednotnej digitálnej brány na poskytovanie prístupu k informáciám, postupom a asistenčným službám a službám riešenia problémov. Tento materiál pripravila Sekcia digitálnej agendy na rokovanie vlády SR. Predseda Rady vlády odovzdal slovo generálnemu riaditeľovi Sekcie digitálnej agendy p. Repovi, aby predstavil materiál.

Predseda Rady vlády poďakoval za informáciu a otvoril diskusiu.

P. Belánik požadoval do dokumentu doplniť samosprávu v súlade so závermi rokovania na ÚPVII, kde bolo dohodnuté, že do oblasti patrí aj samospráva. Napríklad poplatok za rozvoj obce, miestne dane a poplatky, v ktorých by mal byť cezhraničný prvok obsiahnutý.

P. Michálková doplnila, že na stretnutí sa dohodli na presnom znení a to, že členmi pracovnej skupiny budú zástupcovia samospráv. Uvedená informácia bude doplnená do vlastného materiálu.

P. Illek dodal, že materiál vníma veľmi pozitívne a zároveň podotkol, že navrhuje veľké množstvo úloh. K informačným službám konštatoval, že obsah služieb na www.slovensko.sk je používateľsky veľmi neprívetivý, preto je potrebné zamyslieť sa nad informačným obsahom, nie len preložiť terajší portál do anglického jazyka. Ďalšiu poznámku mal k online službám. eIDAS sme formálne splnili, dá sa prihlásiť zahraničnými identifikačnými dokladmi, ale žiadna služba sa nedá vykonať. Nové online služby nesmú skončiť len formálne splnené.

P. Repa doplnil, že úradníci komisie dohliadajú na včasné plnenie, ak členský štát meška so zavádzaním, komisia začne konanie proti porušeniu, čomu sa chceme vyhnúť.

Predseda Rady vlády poďakoval za pripomienky a diskusiu, uzatvoril rozpravu a uviedol, že materiál Rada vlády berie na vedomie.

K bodu 8:

V rámci bodu rôzne predseda Rady vlády otvoril diskusiu k návrhu zákona o bezvýznamových identifikátoroch. P. Illek sa zaujímal o stanovisko UPVII a Úradu pre ochranu osobných údajov. Ďalej uviedol, že zavedenie ID vníma ako nákladnú vec.

P. Maliarik reagoval, zhrnul fakty. Dnes o 13.00 sa koná rozporové konanie, kto má kompetenciu, zúčastní sa konania. Dodal, že po technickej stránke bol projekt zrealizovaný a otestovaný, overený za súčinnosti Sociálnej poisťovne a neočakáva žiadne závratné náklady, ktoré boli uvedené v masmédiách.

P. Illek konštatoval, že hľadisko potreby bezvýznamového identifikátora a potreby sektorových identifikátorov, neboli uvedené v dokumentoch v MPK.

P. Maliarik odpovedal, že potreba je z dôvodu zvýšenia kybernetickej bezpečnosti a ochrany dát. MV SR ako garant bezpečnosti SR je zodpovedné a bojuje proti zneužívaniu osobných údajov, t.j. aby nebolo možné získať údaje s tzv. synergickým efektom, kde postačuje jeden identifikátor na získanie informácií rôzneho druhu. Bezpečnosť je zásadným dôvodom, prečo bol tento projekt pripravený. Takéto riešenia majú obdobu aj v iných štátoch EÚ.

P. Illek pripomenul, že v časti sektorové identifikátory nepochopil, že ako to prispeje k zvýšeniu bezpečnosti. Pokiaľ ide o vyčíslenie nákladov, mal otázku či bude pripravovaná analýza vyčíslenia nákladov. Podľa názoru p. Illeka by bolo opodstatnené riešenie časti bezvýznamového ID a neriešiť sektorový ID.

P. Maliarik k otázke financovania uviedol, že finančné náklady nie sú obrovské, technické riešenie bude implementované ako modul existujúceho informačného systému. Ani pre ÚPVS to nebudú gigantické dopady. V zákone bude prechodné obdobie na realizáciu.

K bodu 9:

Tajomníčka Rady vlády poďakovala prítomným za účasť. Poznamenala, že zo zasadnutia bude vyhotovená zápisnica, ktorá bude zaslaná na pripomienky. Po zapracovaní pripomienok bude zápisnica zverejnená na stránke ÚPVII. Zároveň popriala pekný zvyšok dňa a XI. zasadnutie uzavrela.

Prílohy k zápisnici:

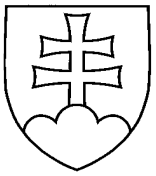
1) Uznesenia Rady vlády SR pre digitalizáciu verejnej správy a jednotný digitálny trh č. 6 až 10 / 2019 zo dňa 16. mája 2019
2) Akčný plán digitálnej transformácie Slovenska na roky 2019 – 2022 – upravené znenie
3) Strategická priorita Informačná a kybernetická bezpečnosť – upravené znenie
4) Návrh na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh
5) Dodatok č. 1 k Rokovaciemu poriadku Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

Richard Raši, v. r.
predseda Rady vlády SR
pre digitalizáciu verejnej správy a jednotný
digitálny trh

Príloha č. 1

Uznesenia Rady vlády SR pre digitalizáciu verejnej správy a jednotný digitálny trh č. 6 až 10 / 2019 zo dňa 16. mája 2019

RADA VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH



UZNESENIE RADY VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

č. 6/2019

z 1. júla 2019

k Akčnému plánu digitálnej transformácie Slovenska na roky 2019 -2022

Číslo materiálu:	004080/2019/oINT-1
Predkladateľ:	podpredseda vlády SR pre investície a informatizáciu

Rada vlády

A. berie na vedomie

A.1. Akčný plán digitálnej transformácie Slovenska na roky 2019 - 2022

B. súhlasí

B.1. s predložením Akčného plánu digitálnej transformácie Slovenska na roky 2019 – 2022 na rokovanie vlády SR

RADA VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

UZNESENIE RADY VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

č. 7/2019

z 1. júla 2019

k dokumentu Strategická priorita Informačná a kybernetická bezpečnosť

Číslo materiálu:	004423/2019/ORKIB-3
Predkladateľ:	podpredseda vlády SR pre investície a informatizáciu

Rada vlády

A. schvaľuje

A.1. dokument Strategická priorita Informačná a kybernetická bezpečnosť s pripomienkami

RADA VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

UZNESENIE RADY VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

č. 8/2019

z 1. júla 2019

k návrhu na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

Číslo materiálu:	4518/2019/oSAEG-1
Predkladateľ:	podpredseda vlády SR pre investície a informatizáciu

Rada vlády

A. berie na vedomie

A.1. návrh na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

B. súhlasí

B.1. s predložením materiálu na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh na rokovanie vlády SR

RADA VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

UZNESENIE RADY VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

č. 9/2019

z 1. júla 2019

k dodatku č. 1 k Rokovaciemu poriadku Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

Číslo materiálu:	4519/2019/oSAEG-1
Predkladateľ:	podpredseda vlády SR pre investície a informatizáciu

Rada vlády

B. schvaľuje

A.1. dodatok č. 1 k Rokovaciemu poriadku Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

RADA VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU
VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

UZNESENIE RADY VLÁDY SLOVENSKEJ REPUBLIKY PRE DIGITALIZÁCIU VEREJNEJ SPRÁVY A JEDNOTNÝ DIGITÁLNY TRH

č. 10/2019

z 1. júla 2019

k informáciám predloženým na zasadnutí

Predkladateľ: podpredseda vlády pre investície a informatizáciu

---

Rada vlády

A. berie na vedomie

A.1. informáciu o príprave implementácie nariadenia EP a Rady č. 2018/1724 o zriadení jednotnej digitálnej brány v podmienkach SR
č. LP/2019/407

A.2. informáciu k súhrnnej implementačnej správe za rok 2018, časť Informatizácia
č. UV-11086/2019

Príloha č. 2

Akčný plán digitálnej transformácie Slovenska na roky 2019 – 2022 – upravené znenie

sa nachádza na https://rokovania.gov.sk/RVL/Material/24027/1

Príloha č. 3

Strategická priorita Informačná a kybernetická bezpečnosť – upravené znenie

ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

Strategická priorita Informačná a kybernetická bezpečnosť

Bratislava, 25. júl 2019

Informácia o dokumente

Názov:	Strategická priorita: Informačná a kybernetická bezpečnosť
Pripravil:	Pracovná skupina Kybernetická bezpečnosť
Verzia:	1.0
Dátum poslednej revízie:	16. 7. 2019

Členovia pracovnej skupiny k strategickým prioritám informatizácie 9.7 Kybernetická bezpečnosť

Meno	Organizácia
Ervín Šimko	ÚPVII
Lukáš Hlavička	ÚPVII
Jan Majtan	ÚPVII
Richard Kiškovač	ÚPVII
Peter Fischer	CSIRT
Henrich Slezák	CSIRT
Richard Pospiš	MV SR
Jaroslav Málik	PZ SR
Juraj Rehák, Martina Jančíková	NASES
Rozalia Harhovská, Pavel Jurečka	MDV SR
Stanislava Schubert	MF SR
Dušan Lukáč	MS SR
Tibor Szabó	MH SR
Rastislav Machel	MK SR
Miroslav Ódor, Danilák	MZ SR
Michal Kozák	ÚGKK SR
Peter Miazdra	DEUS
Miroslav Fíger	GP SR
Viliam Špeťko	MŽP SR
Pavol Frič	Ditec
Peter Weber, Julia Steinerová	ITAS
Daniel Chromek	Eset
Ľubor Illek	Slovensko Digital
Rado Matajs	Sociálna poisťovňa
Rastislav Janota	NBÚ
Peter Pazdera	Občianske združenie IT service management

História verzií

Verzia	Dátum verzie	Pripravil/ Zmenil	Pripomienkoval	Kľúčové zmeny
0.1-0.16	20.10.2017	Peter Poliak	Členovia PS	Príprava dokumentu
0.17	17.10.2018	Ervín Šimko		Prepracovanie dokumentu
0.30	15.4.2019	Členovia PS	Diskusia k dokumentu v PS	Doplnenie textu
0.31	23.5.2019	Členovia PS	Diskusia k dokumentu v PS	Doplnenie textu
0.32	11.6.2019	ÚPVII	IPK	Zapracovanie pripomienok
0.33	18.6.2019	Členovia PS	Diskusia k dokumentu v PS	Schválenie
0.34	28.6.2019	Ervín Šimko	Porada vedenia úradu	Schválenie
0.35	1.7.2019	Ervín Šimko	Rada vlády SR	Schválenie s pripomienkami
0.36	16.7.2019	Ervín Šimko	Zapracovanie pripomienok Rady vlády SR	Doplnenie financovania a termínov do kapitoly 3 a 4 – upravené znenie
1.0	25.7.2019			Schválenie PVII

Obsah

Zoznam skratiek

BSI	nemecký Spolkový úrad pre informačnú bezpečnosť, Bundesamt für Sicherheit in der Informationstechnik
CCD CoE	(NATO) Cooperative Cyber Defence Centre of Excellence
CERT®	Computer emergency response team
CECSP	Central European Cyber Security Platform
CIAA	confidentiality, integrity, availability, authenticity
CIRT	Computer incident response team
CSIRT	Computer security incident response team
DC	Datacentrum
ENISA	European Network and Information Security Agency
EÚ	Európska únia
eIDAS	The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market
FIPS	(us) Federal information processing standard
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
Govnet	vládna dátová sieť orgánov verejnej správy
GSI	Global Security Index
IKT	informačné a komunikačné technológie
IP	Internet protocol
ISACA	medzinárodná, nezisková nezávislá asociácia špecialistov na informačnú a kybernetickú bezpečnosť, pôvodne **Information Systems Audit and Control Association**
ISVS	informačné systémy verejnej správy
ITU	International Telecommunication Union
ITVS	informačné technológie verejnej správy
OP EVS	Operačný program Efektívna verejná správa
OPII	Operačný program Integrovaná infraštruktúra
OP VaI	Operačný program Výskum a Inovácie
OP ĽZ	Operačný program Ľudské zdroje
KIB	kybernetická a informačná bezpečnosť
MISP	Malware Information Sharing Platform (projekt NATO)
MV SR	Ministerstvo vnútra Slovenskej republiky
MS SR	Ministerstvo spravodlivosti Slovenskej republiky
MŠVVŠ SR	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky
NASES	Národná agentúra pre sieťové a elektronické služby
NBÚ SR	Národný bezpečnostný úrad Slovenskej republiky
NIS	Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
NKIVS	Národná koncepcia informatizácie verejnej správy
R&D	Research and development
Red Teaming	cvičenie je simuláciou útoku na organizáciu ako celok, procesy a bezpečnostné opatrenia organizácie s cieľom zlepšiť pripravenosť organizácie, zlepšiť tréning pre zamestnancov.
SANET	Slovenská akademická sieť
SASIB	Slovenská asociácia pre informačnú bezpečnosť
SR	Slovenská republika
TLD	***top level domain***
ÚPVII	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
ÚPVS	Ústredný portál verejnej správy

1 Manažerské zhrnutie

Národná koncepcia informatizácie verejnej správy (ďalej len „NKIVS“) ustanovuje 10 strategických priorít informatizácie verejnej správy:

1 Multikanálový prístup,

2 Interakcia s verejnou správou, životné situácie a výber služby navigáciou,

3 Integrácia a orchestrácia,

4 Rozvoj agendových informačných systémov,

5 Využívanie centrálnych spoločných blokov,

6 Riadenie údajov a Big data (Manažment údajov),

7 Otvorené údaje,

8 Vládny cloud,

9 Komunikačná infraštruktúra,

10 **Informačná a kybernetická bezpečnosť**.

NKIVS ku každej strategickej priorite informatizácie verejnej správy vysvetľuje jej cieľ, prístup k riešeniu a tiež rámcový architektonický model. Účelom tohto dokumentu je, v zmysle úlohy B.5. uznesenia vlády SR č. 437/2016, podrobne rozpracovať jednotlivé výstupy definované v NKIVS uvedené v kapitole 9 Súvisiace dokumenty. V tomto prípade ide o dokument: Strategická priorita: Informačná a kybernetická bezpečnosť.

V dokumente sme rozpracovali v zmysle potrieb NKIVS postupy systematického zvyšovania kybernetickej bezpečnosti vo verejnej správe v nasledovných oblastiach:

- zjednotenie formálnych požiadaviek na riešenie jednotlivých oblastí kybernetickej bezpečnosti,
- riadenie rizík pre ISVS,
- inteligentné systémy a technické riešenia - založené na centrálne spravovanej metodike / šablóne pre kvalitatívnu analýzu rizík a katalógu hrozieb,
- centralizované riadenie kontinuity činností, vrátane realizácie vyhodnotenia dopadov pre jednotlivé komponenty, ako aj plánovanie náhradného výkonu (napríklad nedostupnosť platformy dátovej integrácie), koordinácia havarijného plánovania a pod.,
- navrhnú sa programy zvyšovania bezpečnostného povedomia používateľov (interných aj externých),
- centrálne riadenie požiadaviek na bezpečnosť u dodávateľov IT riešení pre verejnú správu,
- zavedie sa režim nepretržitého výkonu auditu bezpečnosti prevádzkovaných riešení,
- podporí sa inovácia štandardov a riešení v oblasti identifikácie, autentifikácie, autorizácie a vytvárania záznamov,
- navrhnú sa špecifické systematické riešenia ochrany údajov pri realizácii princípu "jedenkrát a dosť", najmä v oblasti ochrany osobných údajov a riadenia prístupu k údajom, ktorý bude štandardne založený na princípe „laissez-faire“ (pozri tiež Základné pojmy).

1.1 Účel dokumentu

Tento dokument je výstupom pracovnej skupiny Kybernetická bezpečnosť, ktorá sa zaoberá informačnou a kybernetickou bezpečnosťou.

Dokument v zmysle NKIVS obsahuje definíciu problematiky, ciele v danej oblasti, návrh organizačného zabezpečenia, výber strategického prístupu a použitých alternatív, návrh riešenia, posúdenie problémov a rizík, vyhodnotenie legislatívnych požiadaviek a plánovanie realizácie v podobe konkrétnych pracovných balíčkov. Zodpovednosť za detailné riešenie navrhovaných pracovných balíčkov, t.j. vypracovanie reformného zámeru, štúdie realizovateľnosti a následnú realizáciu formou zabezpečenia implementácie príslušného projektu, resp. projektov, má gestor podľa nemu prislúchajúcej kompetencie alebo objektívne určený gestor.

Dnešná spoločnosť v podstatnej miere závisí od spoľahlivého fungovania IKT, ktoré sa používajú na spracovanie informácií vo všetkých oblastiach života spoločnosti; od úplnosti, pravdivosti, aktuálnosti a dostupnosti informácií, ktoré sa pomocou IKT spracovávajú a dostupnosti a dôveryhodnosti služieb, ktoré sa prostredníctvom nich poskytujú. Zaistenie dostatočnej úrovne kybernetickej (infraštruktúra) a informačnej bezpečnosti (obsah) je nevyhnutnou podmienkou informatizácie verejnej správy; t. j. aj nevyhnutnou podmienkou na dosiahnutie cieľov, ktoré si kladie NKIVS. Vzhľadom na charakter IKT (rozšírenosť a vzájomná prepojenosť) si zaistenie KIB vyžaduje spoluprácu všetkých zainteresovaných subjektov; štátnych inštitúcií, súkromných organizácií, občanov a keďže slovenský virtuálny priestor je súčasťou globálneho virtuálneho priestoru, aj efektívnu spoluprácu na medzinárodnej úrovni.

1.2 Ciele dokumentu

Tento dokument sa sústreďuje na KIB v zmysle nižšie uvedených definícií v rozsahu podľa NKIVS. Jeho základným cieľom je identifikovať/stanoviť úlohy a kroky,

- ktoré štát potrebuje vyriešiť na to, aby zaistil primeranú úroveň bezpečnosti ISVS a ich bezpečnostného okolia;
- ktoré majú jednotlivé kategórie zainteresovaných pri zaisťovaní primeranej úrovne ochrany ISVS.

Dokument menovite

- vymedzil rozsah problémov KIB, ktoré bude potrebné riešiť na úrovni verejnej správy;
- špecifikoval, čo je potrebné zaistiť v záujme zabezpečenia ISVS a úloh vyplývajúcich z NKIVS; t. j. stanovil ciele v oblasti KIB pre verejnú správu;
- opísal aktuálny stav KIB v ISVS a navrhne postupnosť krokov potrebných na naplnenie stanovených cieľov
- stručne rozobral existujúcu relevantnú legislatívu vyplývajúcu z postavenia SR v EÚ, vrátane aktuálnych materiálov, o ktoré by sa bolo možné oprieť,
- stručne popísal existujúce kompetencie,
- navrhol konkrétné úlohy a ďalšie kroky.

1.3 Adresáti dokumentu

Dokument je určený šiestim kategóriám ľudí, ktorí používajú, prevádzkujú, zabezpečujú IKT, resp. ovplyvňujú prostredie, v ktorom IKT pôsobia; jeho spoločným cieľom pre každú kategóriu užívateľov je vysvetliť podstatu a úlohu KIB; pre jednotlivé kategórie potom špeciálne

- vedúcim pracovníkom inštitúcií verejnej správy zabezpečujúcich, alebo sa podieľajúcich na zabezpečení ochrany slovenského virtuálneho priestoru prehľad úloh, ktoré v súvislosti so zabezpečením slovenského virtuálneho priestoru vo všeobecnosti a ISVS zvlášť je potrebné riešiť;
- vedúcim pracovníkom inštitúcií verejnej správy, ktoré prevádzkujú ISVS má dokument vysvetliť význam zabezpečenia KIB a systémov v pôsobnosti organizácie, ktorú riadia, povinnosti ktoré im vyplývajú z legislatívy a rámcovo čo pre to musia robiť;
- pracovníkom inštitúcií verejnej správy, ktorí sú zodpovední za zaistenie ochrany ISVS: ako rozpracovať všeobecné úlohy vyplývajúce zo zákonov do systematického riešenia KIB; kde nájsť na to potrebné podrobnejšie informácie a na ktoré štátne inštitúcie sa obrátiť v prípade problémov;
- dodávateľom IKT, služieb pre štátne inštitúcie: požiadavky na ochranu ISVS a podmienky, ktoré musia dodávané IKT a služby spĺňať;
- prevádzkovateľom systémov komunikujúcich s ISVS – podmienky, ktoré musia ich systémy spĺňať, aby ich bolo možné pripojiť k ISVS bez rizika kompromitácie ISVS;
- používateľom ISVS a občanom pristupujúcim k ISVS základné zásady, ktoré musia dodržiavať pri využívaní elektronických služieb verejnej správy.

1.4 Základné pojmy

Terminológia KIB sa ešte len vyvíja a neexistujú všeobecne akceptované definície ani mnohých základných pojmov (kybernetický priestor, kybernetická bezpečnosť). V tejto časti vysvetlíme základné pojmy nevyhnutné pre čítanie ďalšieho textu.

Kybernetický priestor tvoria technické systémy spracovávajúce informáciu (univerzálne aj špecializované počítače, mobilné telefóny,...), siete, ktoré tieto technické systémy prepájajú a informácie, ktoré sa pomocou systémov a sietí spracovávajú. Technické systémy, siete a informácie, ktoré sa v nich spracovávajú, tvoria *prvky kybernetického priestoru*.

Podpriestorom kybernetického priestoru sú systémy a siete vyznačujúce sa vlastnosťou, ktorá vymedzuje podpriestor. Tie prvky kybernetického priestoru, ktoré danú vlastnosť nemajú, nepatria do podpriestoru. Všetko, čo nepatrí do systému, ale čo má vplyv na činnosť systému (miestnosť, v ktorej je umiestnený, napájanie, obslužný personál, používatelia, prevádzkové pravidlá, zákony a pod.) tvorí *okolie systému*.

Bezpečnostným okolím systému sú tie prvky jeho okolia, ktoré majú vplyv na bezpečnosť systému.

Okolím podpriestoru kybernetického priestoru je všetko, čo nepatrí do podpriestoru, ale má vplyv na prvky podpriestoru, *bezpečnostným okolím podpriestoru* sú tie prvky jeho okolia, ktoré majú vplyv na bezpečnosť podpriestoru[1]. Čokoľvek, čo má pre organizáciu cenu (a vyžaduje si ochranu) predstavuje *aktívum organizácie*.

Aktívami organizácie sú napr. technické zariadenia, budovy, informácie, ľudia, dobré meno organizácie a pod.

Objektívne existujúca možnosť narušenia štandardného chodu systému (organizácie, podpriestoru) sa nazýva *hrozba*. (Hrozbou je napríklad technická porucha, blesk, požiar, ľudská chyba, omyl, škodlivý kód, útok hackera a i.) Hrozba môže zasiahnuť jedno alebo viacero aktív systému alebo organizácie.

[1] V ďalšom budeme kvôli zrozumiteľnosti hovoriť o bezpečnosti systému a organizácie; uvedené pojmy sa však primerane vzťahujú aj na siete, podpriestory kybernetického priestoru a ich okolia.

Negatívny dôsledok naplnenia hrozby voči aktívu/organizácii sa nazýva *dopad*. Na to, aby došlo k naplneniu hrozby voči aktívu, aktívum musí mať vlastnosť alebo sa používať spôsobom, ktoré naplnenie hrozby umožňuje (ponechanie notebooku na sedadle auta). Takáto vlastnosť alebo okolnosť sa nazýva *zraniteľnosťou* aktíva. Hrozby s katastrofickým dopadom na organizáciu (napr. pád lietadla na budovu) sa nemusia vyskytovať často.

Riziko vyjadruje dopad hrozby a pravdepodobnosť jej naplnenia voči aktívu (systému, organizácii); *hodnota rizika* je stredná hodnota dopadu hrozby.

Činiteľ, ktorý je schopný hrozbu realizovať, sa nazýva *nositeľ hrozby* (krádež – zlodej).

Cieľavedomý pokus o naplnenie hrozby sa nazýva *útok* a pôvodca útoku – *útočník.*

Akákoľvek udalosť, ktorá spôsobí/môže mať negatívny dopad na bezpečnosť systému alebo organizácie, sa nazýva *bezpečnostný incident*. Bezpečnostné incidenty môžu mať rozličné dôsledky, ale tie sa spravidla dajú vyjadriť prostredníctvom straty/narušenia dôvernosti, integrity, dostupnosti informácií, resp. služieb, ktoré na ich základe organizácia alebo systém poskytuje.

Zaistenie *dôvernosti* (confidentiality) informácie znamená zamedzenie prístupu nepovolaných osôb k informáciám, ktoré údaje obsahujú.

Zaistenie *integrity* (integrity) informácie znamená vylúčenie možnosti nepozorovanej modifikácie údajov; požiadavka na *autentickosť* (authenticity) údajov je naplnená, ak je zaručená pôvodnosť údajov, t.j. integrita a autorstvo.

Napokon *dostupnosť* (availability) informácií (služieb) znamená zaistenie prístupu k údajom a možnosti využívania služieb vždy, keď to oprávnená osoba vyžaduje.

Tieto štyri požiadavky[2] na bezpečnosť informácií sú základom pre zaistenie potrebnej ochrany systémov. Organizácia analyzuje hrozby voči aktívam organizácie, odhaduje riziká, ktoré z hrozieb voči aktívam vyplývajú a prijíma opatrenia (technické organizačné, personálne a iné riešenia), ktorých cieľom je eliminovať riziká alebo aspoň znížiť hodnotu rizík na akceptovateľnú úroveň.

Informačná bezpečnosť je

- ideálny stav systému, organizácie, keď IKT fungujú bez narušenia a je zaručená dôvernosť, integrita, autentickosť a dostupnosť údajov, resp. služieb
- činnosť zameraná na dosiahnutie a udržanie požadovaného stavu IKT
- multidisciplinárny odbor zaoberajúci sa skúmaním hrozieb voči údajom a systémom a hľadaním opatrení na elimináciu rizík, ktoré z nich vyplývajú.

Kybernetická bezpečnosť nie je definovaná jednoznačne, chápe sa *v úzkom zmysle* ako zaistenie odolnosti systémov voči kybernetickým útokom (t.j. útokom na IKT, resp. útokom vedeným na IKT), *v širokom zmysle* ako informačná bezpečnosť kybernetického priestoru. Úzke chápanie je zjavne nedostatočné, lebo ponecháva bokom bezpečnostné incidenty, ktoré neboli spôsobené úmyselne, ochranu okolí IKT systémov, informácií, ktoré nie sú v elektronickej podobe. Široké chápanie kybernetickej bezpečnosti je konzistentnejšie, ale na zaistenie bezpečnosti systému/organizácie je potrebné chrániť aj netechnické a nemateriálne aktíva organizácie.

Princíp „laissez-faire“ je metódou optimistického riadenia prístupu, ktorej cieľom je v komplexných systémoch minimalizovať prekážky kladené koncovému používateľovi údajov v plnení jeho potrieb na

[2] Niekedy sa uvádzajú len tri - confidentiality, integrity, availability, tzv. CIA, pričom integrita zahŕňa aj autentickosť.

prístup k údajom, pri zachovaní požadovaného stupňa bezpečnosti na systémovej aj individuálnej úrovni.

Ide o protiklad najmä voči v súčasnosti používaným centrálne preemptívne riadeným politikám riadenia prístupu, v ktorých sa pri raste zložitosti systému (z hľadiska množstva riadených používateľov a údajov) obzvlášť znižuje jeho flexibilita a tým aj rýchlosť vybavenia nových požiadaviek na prístup.

2 Súčasný stav v KIB

KIB je spoločenským problémom aj v globálnom meradle. Okrem objektívnych problémov spôsobených charakterom digitálnych IKT a spôsobom ich používania[3], dramaticky stúpa rozsah a závažnosť cielených útokov na IKT a údaje, ktoré sa v nich spracovávajú. Podľa najnovšej Správy EÚ[4] sa za necelých päť rokov (2013-2017) zvýšil ekonomický dopad kybernetickej kriminality päťnásobne a do roku 2019 sa odhaduje štvornásobný nárast oproti súčasnosti. Nejedná sa už len o ekonomicky motivovanú kriminalitu, závažné kybernetické útoky vedú často štáty, organizácie, teroristické skupiny, niekedy aj jednotlivci na kritickú infraštruktúru štátu a usilujú sa dokonca aj o narušenie základných demokratických procesov nevyhnutných pre fungovanie štátu. Využívanie prínosov informačnej spoločnosti bude možné len vtedy, ak sa na potrebnej úrovni podarí komplexne zaistiť KIB; t.j. vypracovať, prijať a implementovať komplexnú stratégiu KIB, vytvoriť potrebné kapacity na jej presadzovanie, zaistiť potrebný počet kvalifikovaných odborníkov a udržiavať potrebnú úroveň bezpečnostného povedomia širokej verejnosti.

2.1 Koncepcia a legislatíva EÚ v KIB

EÚ sa dlhodobo zaoberá KIB. V tomto dokumente sa nebudeme podrobnejšie venovať aktivitám EÚ,, preto uvádzame len najdôležitejšie legislatívne a koncepčné dokumenty EÚ týkajúce sa KIB[5], z ktorých pre SR vyplývajú, resp. v budúcnosti vyplynú nejaké povinnosti

1) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017
2) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 477 final
3) Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
4) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

[3] Internet Security Threat Report 2017, https://www.symantec.com/security-center/threat-report.

[4] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017.

[5] Podrobnejší zoznam na http://cordis.europa.eu/search/result_en?q=cybersecurity obsahuje 165 položiek.

5) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).
6) Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.
7) Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016
8) The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014.
9) Regulation (EU) 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
10) Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.
11) Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013).
12) COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
13) Regulation (EC) n° 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1.
14) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Kľúčovým odborným (zatiaľ poradným a metodickým) orgánom Európskej komisie je Agentúra ENISA. V súčasnosti sa pripravuje nariadenie na posilnenie jej postavenia (viď bod 2 vyššie).

Tieto (a ďalšie súvisiace) dokumenty sa premietli do slovenskej legislatívy, resp. budú do nej zapracované v najbližšom čase.

2.2 KIB SR a ISVS

Slovenský kybernetický/virtuálny priestor je podpriestor globálneho kybernetického priestoru, na ktorý sa vzťahuje slovenská legislatíva. Vlastníkmi prvkov slovenského kybernetického priestoru sú štátne inštitúcie, súkromné spoločnosti a jednotlivci.

Podstatnú časť systémov vo vlastníctve štátu predstavujú ISVS. Infraštruktúra, na ktorú sú ISVS pripojené a iné systémy, s ktorými ISVS komunikujú, právne prostredie, technologická infraštruktúra a obsluhujúci personál zabezpečujúci chod ISVS, ako aj všetko to, čo nie je ISVS, ale ovplyvňuje bezpečnosť ISVS, predstavuje bezpečnostné okolie ISVS.

S výnimkou malého počtu izolovaných systémov sú takmer všetky ISVS v pôsobnosti ústredných orgánov štátnej správy (ďalej len „ÚOŠS“) a organizácií so zvýšenými požiadavkami na bezpečnosť pripojené na Govnet a teda pripojené na Internet buď prostredníctvom Govnet, alebo priamo.

2.2.1 Legislatívny rámec KIB v SR

Ochrana systémov, sietí a informácií je predmetom úpravy viacerých zákonov, jednotiaci *lex generalis* pre oblasť KIB v slovenskej legislatíve je **Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“). Ďalšími osobitnými predpismi, ktoré upravujú pôsobnosť vo vzťahu ku KIB** sú:

Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov upravuje podmienky, postup a rozsah slobodného prístupu k informáciám.

Bezpečnostné požiadavky na systémy a informácie sú obsiahnuté aj v ďalších zákonoch, napr.

Zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov .

Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov (MV SR), ktorý okrem iného upravuje elektronický záznam (informácií).

Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení neskorších predpisov.

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ktorý upravuje podmienky na ochranu utajovaných skutočností, práva a povinnosti právnických osôb a fyzických osôb pri tejto ochrane, pôsobnosť Národného bezpečnostného úradu a pôsobnosť ďalších štátnych orgánov vo vzťahu k utajovaným skutočnostiam a zodpovednosť za porušenie povinností ustanovených týmto zákonom.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov okrem iného upravuje trestné činy z oblasti počítačovej kriminality.

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov (Ministerstvo vnútra SR) upravuje organizáciu a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry, postup pri určovaní prvku kritickej infraštruktúry, povinnosti prevádzkovateľa pri ochrane prvku kritickej infraštruktúry a zodpovednosť za porušenie týchto povinností.

Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov okrem iného upravuje práva a povinnosti podnikov a užívateľov elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu elektronických komunikačných sietí a elektronických komunikačných služieb, ochranu súkromia a ochranu spracúvania osobných údajov v oblasti elektronických komunikácií a pôsobnosť orgánov štátnej správy v oblasti elektronických komunikácií.

Výnos Ministerstvo vnútra Slovenskej republiky č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry.

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov, ktorý upravuje okrem iného identifikáciu osôb a autentifikáciu osôb vo virtuálnom priestore.

Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (Národný bezpečnostný úrad) upravuje podmienky poskytovania dôveryhodných služieb, povinnosti poskytovateľov dôveryhodných služieb, pôsobnosť Národného bezpečnostného úradu v oblasti dôveryhodných služieb a sankcie za porušenie povinností podľa osobitného predpisu a tohto zákona.

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Úrad na ochranu osobných údajov SR), ktorý upravuje ochranu práv fyzických osôb pred neoprávneným

zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov, práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb, postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky. Týmto zákonom bol zrušený pôvodný zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov s účinnosťou od 25.05.2018.

Podrobnosti o ochrane údajov a systémov sú rozvedené v početných vykonávacích predpisoch (Príloha).

Pre ISVS je najdôležitejší

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktorý okrem iného upravuje práva a povinnosti orgánu vedenia a orgánov riadenia v oblasti vytvárania, prevádzkovania, využívania a rozvoja informačných technológií verejnej správy, základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných technológií verejnej správy.

Podrobné bezpečnostné požiadavky na ISVS ustanovuje

Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.

2.2.2 Kompetencie

KIB je nutným prepokladom fungovania akýchkoľvek systémov postavených na digitálnych IKT a ochrana takýchto systémov vychádza z rovnakých základných princípov. Kompetencie v KIB v SR (pozri časť Legislatívny rámec) sú stanovené buď po vecných oblastiach (utajované skutočnosti, elektronický podpis, osobné údaje, počítačová kriminalita) alebo po type systémov (ISVS, kritická infraštruktúra, telekomunikačné siete).

V roku 2018 bol prijatý zákon, ktorý niektoré povinnosti zainteresovaných subjektov v oblasti kybernetickej oblasti explicitne špecifikoval. V súčasnosti NBÚ SR vykonáva činnosti potrebné na zabezpečenie slovenského kybernetického priestoru.

V rámci zabezpečenia KIB ÚPVII v súlade so zákonom o kybernetickej bezpečnosti delimitoval vládnu jednotku CSIRT.sk a ďalej vyvíja aktivity na systematické zabezpečenie organizácií verejnej správy z pohľadu KIB.

2.2.3 Koncepcie KIB a ich realizácia

V minulosti boli pokusy koncepčne riešiť Informačnú/kybernetickú bezpečnosť na celoštátnej úrovni (celého virtuálneho priestoru SR). K najvýznamnejším patria dve vládou schválené koncepcie Národná stratégia pre informačnú bezpečnosť v Slovenskej republike na roky 2008-2013 schválená uznesením vlády Slovenskej republiky č. 570/2008 a Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schválená uznesením vlády Slovenskej republiky č. 328/2015 . Obe koncepcie sa zhodli na rovnakých najdôležitejších prioritách.

MF SR, ktoré do roku 2015 riadilo a koordinovalo bezpečnosť ISVS podľa v tom čase platného znenia zákona č . 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vypracovalo systém vzdelávania v informačnej bezpečnosti a realizovalo rozsiahly dvojročný projekt vzdelávania pracovníkov verejnej správy, vytvorilo CSIRT.SK,

harmonizovalo bezpečnostné štandardy ISVS s medzinárodnými, uskutočnilo dva prieskumy stavu informačnej bezpečnosti v SR (2011 a 2013).

Po roku 2014, s výnimkou činnosti CSIRT.SK, MF SR ďalšie aktivity v informačnej bezpečnosti nevyvíjalo. V roku 2015 získal kompetencie v oblasti kybernetickej bezpečnosti NBÚ SR. Vláda schválila Koncepciu kybernetickej bezpečnosti v roku 2015 a v roku 2016 Akčný plán realizácie Koncepcie, ktorý definoval 37 konkrétnych termínovaných úloh. Pri Bezpečnostnej rade SR bol zriadený Výbor pre kybernetickú bezpečnosť[6], NBÚ v roku 2016 zriadil Komisiu pre kybernetickú bezpečnosť.

Mnohé z uvedených úloh sú kľúčovým predpokladom pre systematické riešenie KIB vo verejnej správe. Niektoré z úloh bolo náročné implementovať v praxi z administratívnych dôvodov napriek vysokej pridanej hodnote realizácie navrhovaných riešení.

Zaistenie dostatočnej úrovne KIB štátu si vyžaduje riešenie úloh na celoštátnej aj lokálnej úrovni a tomu prislúchajúcu organizačnú štruktúru a zdroje. Centrálne potreby štátu nezávisia od jeho veľkosti a dajú sa orientačne odhadnúť na základe porovnania s podobnými organizáciami v zahraničí, napr. nemeckým Spolkovým úradom pre informačnú bezpečnosť, ktorý v roku 1992 začínal s 200 zamestnacami a momentálne ich má vyše 600. Počet odborníkov na centrálnej úrovni závisí od toho, aké úlohy sa budú na centrálnej úrovni riešiť a na tom, ktoré riešenia sa budú preberať (a nebudú vyvíjať vlastné). Druhú skupinu odborníkov tvoria tí, ktoré pôsobia "v teréne" a ich počet závisí napr. aj od počtu systémov, o ktoré sa majú starať. EÚ odhaduje, že v roku 2020 bude potrebovať 350.000 špecialistov na KIB, t.j. na Slovensku by sme ich potrebovali cca 3.500.

Podľa kvalifikovaného odhadu založeného na poznatkoch expertov z organizácií ISACA a ohlasoch na projekt vzdelávania v informačnej bezpečnosti MF SR a činnosti CSIRT.SK, v SR je nedostatok kvalifikovaných špecialistov na KIB dokonca aj v súkromnom sektore. V štátnych inštitúciách je situácia skomplikovaná obmedzeniami na výšku platu odborníka a možnosťami súkromných firiem, ktoré majú záujem o kvalifikovaných pracovníkov a sú schopné ich finančne lepšie ohodnotiť. Výsledkom je stav, keď štátne inštitúcie nemajú kvalifikovaných odborníkov a bezpečnosť svojich systémov riešia nedostatočne vlastnými silami, alebo využívajú outsourcing.

2.2.4 Hodnotenie stavu KIB SR podľa GSI

Vyššie uvedené skutočnosti sa zohľadňujú aj v medzinárodných hodnoteniach stavu KIB v SR.

Global Security Index (GSI) je agregovaný ukazovateľ spracovaný organizáciou ITU (International Telecommunication Union) v rokoch 2014 a 2017. Index z roku 2017 bol vyhodnotený ako dotazník, ktorý bol spracovaný na základe online prieskumu od januára do septembra 2016 pozostával z údajov 193 členských krajín ITU.

Zloženie indexu je postavené na piatich základných pilieroch:

1. **Právny:** meria sa na základe existencie právnych rámcov a zodpovednosti inštitúcií zaoberajúcimi sa kybernetickou bezpečnosťou a zločinom.

2. **Technický:** meria sa na základe existencie technických rámcov a zodpovednosti inštitúcií zaoberajúcimi sa kybernetickou bezpečnosťou.

[6] § 10b zákona č. 110/2004 Z. z. fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru.

3. **Organizačný:** meria sa na základe existencie politiky koordinácie inštitúcií a stratégií pre kybernetickú bezpečnosť s ohľadom na rozvoj na národnej úrovni.

4. **Budovania kapacít:** meria sa na základe existencie výskumu a vývoja, vzdelávania a školiacich programov, certifikácie profesionálov a existencie agentúr verejného sektora podporujúcich budovanie kapacít v oblasti kybernetickej bezpečnosti.

5**. Kooperácie:** meria sa na základe existencie partnerstiev a rámcov spolupráce a výmeny informácií v oblasti kybernetickej bezpečnosti.

Postavenie SR

Rok	Skóre	Globálne poradie	Poradie v Európe
2014	0,618	8	5
2017	0,362	82	34 (8. od konca)

Aj keď metódy zberu informácií nie sú pre roku 2014 a 2017 úplne totožné[7], prínosom údajov vychádzajúcich z GSI je jeho celosvetový záber, snaha o objektivizáciu porovnania a celkový trend vývoja v relatívnom porovnaní medzi krajinami, kde je zrejmé relatívne zaostávanie SR v poslednom období.

Výsledky vybraných krajín v roku 2017

V rámci regiónu zostáva za SR v rebríčku GSI 2017 už len 8 krajín, medzi ktorými sa nachádzajú krajiny ako Albánsko, Srbsko, Lichtenštajnsko, Andorra, Vatikán, Bosna Hercegovina.

GSI vybraných krajín 2017

Krajina	Skóre	Globálne poradie	Poradie v Európe
Estónsko	0,846	5	1
Nórsko	0,786	11	3
UK	0,783	12	4
Izrael	0,691	20	10
Nemecko	0,679	24	12

[7] GSI 2017, International Telecommunication Union (ITU) 2017, s.20 Methodology.

Dánsko	0,617	34	18
Česká republika	0,609	35	19
Slovensko	0,362	82	34 (8. od konca)

Iné V4 pre ilustráciu			
Krajina	**Skóre**	**Globálne poradie**	**Poradie v Európe**
Poľsko	0,622	33	17
Maďarsko	0,534	51	25

Metodika výpočtu a podrobnosti o hodnotení ITU sú uvedené v prílohe 8.3.

Z hľadiska obsahového zameranie existujú aj ďalšie indexy popisujúce stav krajiny z pohľadu rôznych aspektov kybernetickej bezpečnosti.

Ani v rámci indexu GSI nedochádza ku komplexnému auditu stavu kybernetickej bezpečnosti v krajinách, v súčasnosti však z hľadiska komplexnosti a hĺbky.

2.2.5 Stav bezpečnosti ISVS podľa zistení CSIRT.SK

Nedostatky popísané v predchádzajúcich častiach sa prejavujú aj v prístupe k ochrane ISVS a celkovej úrovni zabezpečenia ISVS. Posledný prieskum stavu informačnej bezpečnosti robilo MF SR v roku 2013[8], súborné informácie o stave zabezpečenia ISVS chýbajú. Istý obraz o stave bezpečnosti ISVS dávajú výsledky CSIRT.SK[9].

Špecializovaný útvar CSIRT.SK ÚPVII je jednotka pre riešenie informačno-bezpečnostných incidentov, ktorá v súčasnosti vykonáva činnosti vladnej jednotky CSIRT pre podsektor Informačné systémy verejnej správy. CSIRT.SK rieši informačno-bezpečnostné incidenty vo svojom sektore a vykonáva aj penetračné testovanie (hľadanie zraniteľností, ktoré umožňujú útočníkovi preniknúť do systému). Poznatky, ktoré získala pri svojej činnosti dopĺňajú obraz o stave informačnej bezpečnosti vo verejnej správe.

Zistenia CSIRT.SK sú postavené na riešení bezpečnostných incidentov vo verejnej správe a IP adresnom priestore SR[10], informácií získaných z threat intelligence platformy implementovanej CSIRT.SK[11], vykonaných bezpečnostných auditoch organizácií vo verejnej správe a vykonaných penetračných testov (príp. iných aktivít, v rámci rôznych kontrol).

CSIRT.SK identifikoval v roku 2016 10731 incidentov a upozornil na ne dotknuté organizácie verejnej správy. 93.8% bezpečnostných odhalených incidentov tvorili zraniteľnosti, robotické siete a škodlivý kód. CSIRT.SK riešil závažné bezpečnostné incidenty, ktoré nahlásili samotné organizácie verejnej správy. V roku 2016 10% zo závažných bezpečnostných incidentov tvorili pokusy o prienik do ISVS.

[8] Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike, MF SR, 2013.

[9] https://www.csirt.gov.sk.

[10] IP adresy pridelené subjektom v Slovenskej republike, webové portály a služby v rámci TLD domény .sk.

[11] Systém založený na systéme Malicious Domain Manager, ktorý zbiera a vyhodnocuje informácie z verejných zdrojov threat intelligence a informácie získané od zahraničných partnerov týkajúce sa detegovaných bezpečnostných incidentov najčastejšie na základe SinkHole serverov pre škodlivý kód.

Správne bezpečnostné povedomie zamestnancov, ktorí majú prístup k ISVS je pre zaistenie jeho bezpečnosti základnou podmienkou. V roku 2013 CSIRT.SK počas národného cvičenia na ochranu kritickej infraštruktúry SISE 2013 simuloval phishingový útok prostredníctvom emailu adresovaného jednotlivým rezortom, 31,32% adresátov navštívilo podvodnú stránku a 10,04% útočníkovi poskytlo svoje prihlasovacie údaje do ISVS organizácie (!). Od 2013 nebolo uvedené meranie opakované.

CSIRT.SK vykonal počas svojej existencie viac ako 150 interných a externých penetračných testov a retestov (v roku 2016 bolo vykonaných celkovo 55 penetračných testov z toho 33 testov a 22 retestov), počas ktorých simuloval správanie sa útočníkov a ich útok na konkrétne časti infraštruktúry a vybrané služby poskytované organizáciami verejnej správy.

Podrobný popis zistení CSIRT.SK je uvedený v prílohe 8.4.

2.2.6 Problémové oblasti z pohľadu bezpečnosti ISVS

Kľúčovým problémom KIB je nedostatok kvalifikovaných odborníkov :

1) informatik (bezpečnostní správcovia systémov a sietí, vývojári bezpečnostných riešení, operátori bezpečnostných systémov, analytici, členovia CSIRT-ov,...)
2) manažér (bezpečnostní manažéri rôznych úrovní)
3) audítor (audítor bezpečnosti informačných systémov)
4) informaticky vzdelaný právnik (európska a slovenská legislatíva, vnútorná legislatíva organizácií, ochrana osobných údajov, autorké práva, počítačová kriminalita, vyšetrovatelia, prokurátori, advokáti a sudcovia a i.)
5) učiteľ/lektor KIB pre žiakov, študentov stredných a vysokých škôl a dospelých,
6) výskumník pracujúci v informačnej a kybernetickej bezpečnosti (kryptológia, informačné systémy, vzdelávanie detí a dospelých, siete, právne vedy, psychológia, sociológia, a i.)
7) edukovaný novinár a iný zástupca médií.
8) Špecialista riadenia rizík
9) Bezpečnostný architekt
10) Špecialista ochrany osobných údajov
11) Špecialista objektovej ochrany

Dôležité je aj rozmiestnenie a využitie odborníkov: štát na zaistenie bezpečnosti svojho virtuálneho priestoru potrebuje odborníkov

1) na centrálnej úrovni (koncepčná činnosť, legislatíva, expertná činnosť pre štátne orgány, medzinárodná spolupráca, terminológia, štandardy, metodiky, monitorovanie stavu KIB, koordinácia riešenia bezpečnostných incidentov, koordinácia spolupráce medzi rezortami, so súkromným a akademickým sektorom, vzdelávanie, osveta, špeciálny výskum a i.)
2) na úrovni rezortov (všeobecné: riadenie aktivít na zaistenie bezpečnosti rezorných systémov, sietí a informácií, vzdelávanie, kontrola bezpečnosti organizácií v rezorte, riešenie bezpečnostných incidenov, zabezpečenie informačných systémov, budovanie bezpečnostného povedomia, špeciálne: podľa zamerania rezortu napr. MV SR – počítačová kriminalita, identifikácia a autentifikácia ľudí, kritická infraštruktúra, e-Government (archívy, registratúry)
3) na úrovni organizácií (riadenie KIB, ochrana vlastných systémov, vnútorná legislatíva, školenia pracovníkov, budovanie bezpečnostného povedomia a špeciálne úlohy závisiace od poslania organizácie).

U vyššie uvedených špecialistov na KIB je možné špecifikovať, aké znalosti a schopnosti by mali mať a v prípade potreby ich vyškoliť, alebo nechať vyškoliť. Okrem nich sú však potrební experti na koncepčnú činnosť a riadiaci pracovníci rozličnej úrovne znalí odbornej problematiky a schopní zadávať úlohy a posudzovať ich riešenie (vrátane analýz a koncepcií). Tieto dve kategórie sú pre zaistenie KIB štátu mimoriadne dôležité, ale takýchto ľudí nie je možné pripravovať štandardným spôsobom.

Ucelený prehľad o potrebách, súčasnom počte a rozmiestnení odborníkov na KIB nie je k dispozícii.

Druhým, rovnako kľúčovým nedostatkom je chýbajúci komplexný prístup k riadeniu a implememtácií informačnej bezpečnosti v organizáciách verejnej správy, kompetenčné spory medzi zainteresovanými inštitúciami a formalistický prístup k požiadavkam legislatívy z pohĺadu zabezpečenia informačnej bezpečnosti v organizácií.

2.3 Zhrnutie stavu KIB v SR

Dlhodobá stratégia a jej realizácia. Aktuálnu štátnu stratégiu predstavuje Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020, rozpracovaná v Akčnom pláne realizácie Koncepcie. Štátnym orgánom zodpovedným za kybernetickú bezpečnosť je NBÚ SR. Oficiálna správa o plnení úloh Akčného plánu zatiaľ nebola zverejnená.

Nedostatočné odborné kapacity. Štát nemá dostatočné odborné kapacity na riešenie potrebných úloh na centrálnej a rezortnej úrovni, ale ani výkonných pracovníkov na zabezpečenie ochrany vlastných systémov. Potrebných odborníkov (počtom a zameraním) nemá ani súkromná sféra, ani akademický sektor. Bezpečnosť štátu nemožno postaviť na externých spolupracovníkoch.

3 Navrhované riešenia

Stav KIB v SR je neuspokojivý a za takýchto podmienok (odborné kapacity, zdroje, úroveň bezpečnostného povedomia) štát nedokaže zabezpečiť adekvatnu ochranu v oblasti ISVS. Takýto stav je vzhľadom na možné dôsledky vyradenia kritických IKT a/alebo systémov v masovom rozsahu neprijateľný. Ak bude štát chcieť zaistiť dostatočnú ochranu (a fungovanie) svojich ISVS, bude potrebovať súčasne riešiť identifikované problémy KIB virtuálneho priestoru, ako aj ISVS. Vychádzajúc z poznania stavu, kritických problémov a disponibilných zdrojov a zohľadňujúc problémy s realizáciou predchádzajúcich koncepcií, navrhujeme na riešenie globálneho stavu KIB v SR a zvlášť bezpečnosti ISVS nasledujúci postup:

- rýchle riešenie kritických problémov KIB v štáte a v ISVS (v rámci platnej legislatívy, prostredníctvom vzdelávania, štandardizácie, koordinácie činnosti, medzinárodnej spolupráce, podporou existujúcich pracovísk)
- priebežne upresňovanie údajov o stave KIB a bezpečnosti ISVS v SR (monitorovanie a vyhodnocovanie bezpečnostných incidentov, inventarizácia odborných kapacít, možných zdrojov, analytická činnosť, cielený vedecký výskum)
- stanovenie priorít pre systematické riešenie KIB ISVS (závisí od zdrojov a malo by sa prehodnocovať raz ročne na úrovni vlády SR
- vybudovanie kompetenčného centra KIB vo verejnej správe, ktoré by na centrálnej úrovni zabezpečovalo riadenie KIB vo verejnej správe, technickú podporu pre špecializované činnosti v oblasti informačnej bezpečnosti a kontrolné mechanizmy na zabezpečovanie adekvátnej úrovne bezpečnosti IS VS.

V nasledujúcich častiach stručne rozoberieme uplatňovanie vyššie navrhovaného postupu.

3.1 Priority a princípy riešenia

Kybernetická bezpečnosť je jednou z priorít NKIVS, pričom dokument OPII obsahuje špecifický cieľ 7.9 Zvýšenie kybernetickej bezpečnosti v spoločnosti. Tento dokument sa odvoláva na európsku legislatívu, konkrétne na Stratégiu kybernetickej bezpečnosti EÚ a Smernicu Európskeho parlamentu

a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Riešenia bezpečnosti ISVS by podľa NKIVS mali byť postavené na nasledovných princípoch:

- silná štandardizácia riešení, najmä v zmysle určených bezpečnostných opatrení pre typizované situácie,
- stanovia sa minimálne nevyhnutné požiadavky na bezpečnosť, tak z dôvodu efektívnosti investícií, ako aj pre minimalizáciu obmedzení vyplývajúcich z nasadených bezpečnostných opatrení,
- dôsledné sa odmieta princíp „security by obscurity“, utajené a neprístupné budú iba nevyhnutné skutočnosti,
- realizuje sa systematická podpora používateľov pri bezpečnom používaní elektronických služieb,
- dôsledne pristúpime k riešeniu rizík prameniacich zo zdieľanej zodpovednosti za prevádzku integrovaného informačného systému verejnej správy.

V ďalšom postupe systematického zvyšovania kybernetickej bezpečnosti vo verejnej správe budú rozpracované riešenia najmä v nasledovných oblastiach:

- zjednotenie formálnych požiadaviek na riešenie jednotlivých oblastí kybernetickej bezpečnosti,
- riadenie rizík pre ISVS, inteligentné systémy a technické riešenia - založené na centrálne spravovanej metodike / šablóne pre kvalitatívnu analýzu rizík a katalógu hrozieb,
- centralizované riadenie kontinuity činností, vrátane realizácie vyhodnotenia dopadov pre jednotlivé komponenty, ako aj plánovanie náhradného výkonu (napríklad nedostupnosť platformy dátovej integrácie), koordinácia havarijného plánovania a pod.,
- navrhnú sa programy zvyšovania bezpečnostného povedomia používateľov (interných aj externých),
- centrálne riadenie požiadaviek na bezpečnosť u dodávateľov IT riešení pre verejnú správu,
- zavedie sa režim nepretržitého výkonu auditu bezpečnosti prevádzkovaných riešení, - podporí sa inovácia štandardov a riešení v oblasti identifikácie, autentifikácie, autorizácie a vytvárania záznamov,
- navrhnú sa špecifické systematické riešenia ochrany údajov pri realizácii princípu "jedenkrát a dosť", najmä v oblasti ochrany osobných údajov a riadenia prístupu k údajom, ktorý bude štandardne založený na princípe „laissez-faire“ (pozri tiež slovník pojmov).

NKIVS taktiež predpokladá „zavedenie centrálnej a jednotnej správy kybernetickej bezpečnosti a zavedenia výkonu kybernetickej bezpečnosti na všetkých úrovniach a v rámci všetkých organizácií verejnej správy.“

3.2 Koncepcia, legislatíva, kompetencie

V súčasnosti je legislatívou *lex generalis* pre oblasť KIB v slovenskej legislatíve **zákon o kybernetickej bezpečnosti**. a **zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, ktorý** je zameraný len na IKT v pôsobnosti orgánov verejnej správy a jeho cieľom je definovať kompetencie ohľadne vedenia a riadenia bezpečnosti ISVS.

Jedným z hlavných dôvodov nedostatočnej úrovne KIB ISVS je nedostatočné technické, personálne a finančné zdroje na zabezpečenie úloh súvisiacimi s kybernetickou bezpečnosťou.

Súčasne s realizáciou všeobecného zámeru informatizácie, ktorým je postupná centralizácia informačných systémov verejnej správy a ich prevádzka v cloudovom prostredí, je potrebné adekvátne tomu vytvoriť aj proces pre postupné centralizovanie riadenia KIB.

Pre efektívny proces koordinácie KIB bude musieť byť vytvorený aj efektívny spôsob presadzovania bezpečnostných opatrení vo verejnej správe. Považujeme za dôležité zaviesť do praxe metódy účinne brániace prevádzkovaniu kriticky dôležitých ISVS v nedostatočne zabezpečenom prostredí, napr. podmieniť možnosť nasadíť nový IS do prevádzky až po úspešnom overení bezpečnosti jeho prevádzkového prostredia.

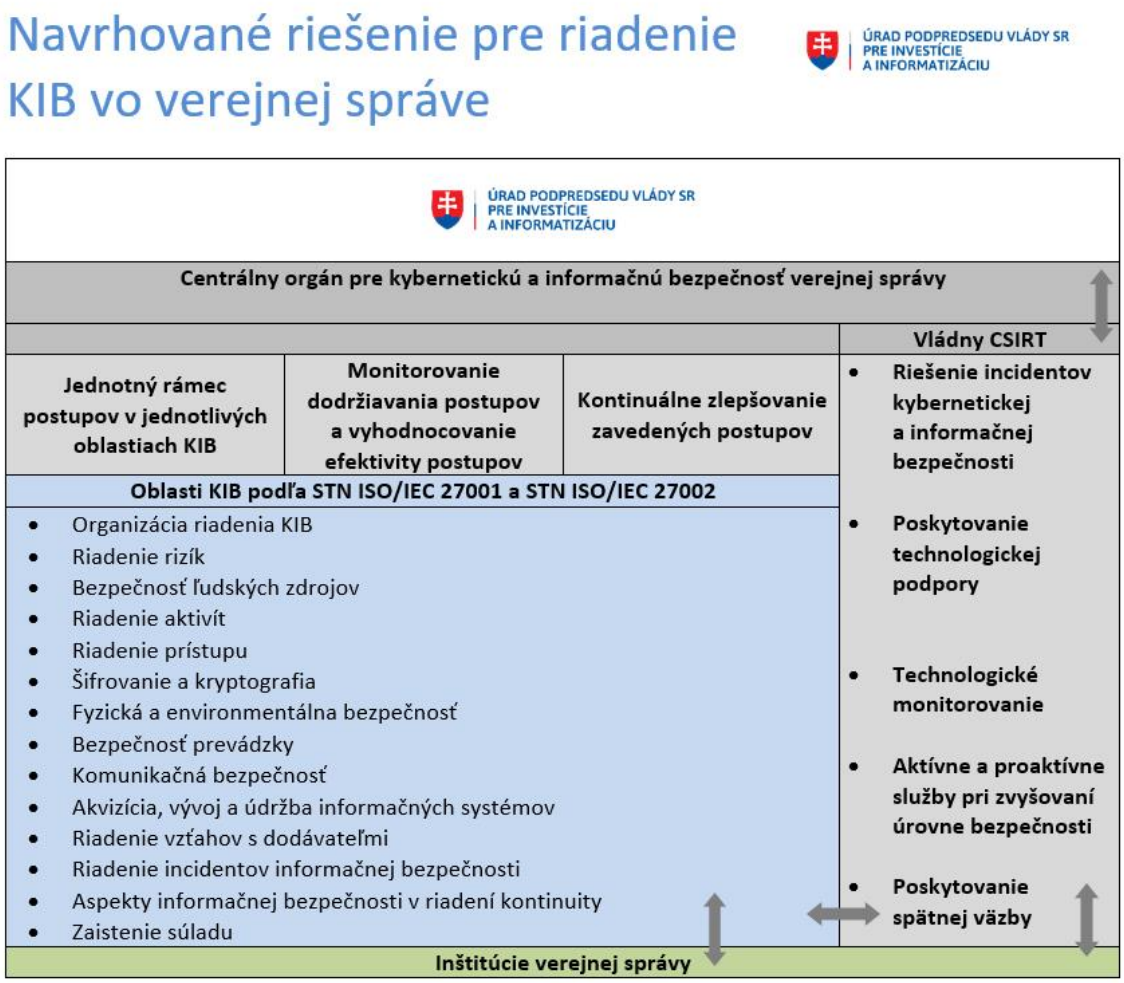


Figure 1 Schéma navrhovaného riešenia pre riadenie KIB vo verejnej správe

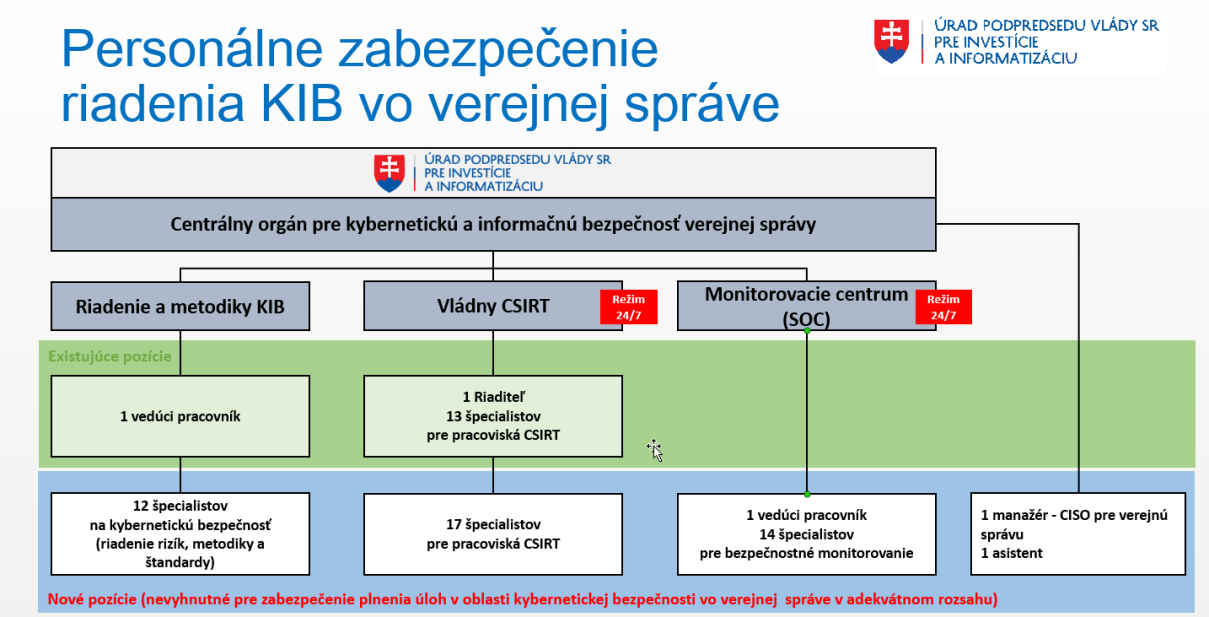


Figure 2 Personálne zabezpečenie riadenia KIB vo verejnej správe

3.3 Zabezpečenie základnej úrovne ochrany kybernetického priestoru VS

Z centrálnej úrovne (ÚPVII) riadenia ISVS je na zabezpečenie aspoň základnej úrovne ochrany vo všeobecnosti a zvlášť pre bezpečnosť ISVS možné v krátkom čase zabezpečiť nasledujúce kroky:

- dohodnúť pokrytie čo najväčšieho počtu ISVS Vládnym CSIRT-om podľa zákona o ITVS
- definovať minimálne požiadavky na systémy a siete (v podobe štandardov ISVS) a súbor opatrení (baseline), ktorého implementácia stačí na splnenie minimálnych požiadaviek,
- kontrolovať dodržiavanie minimálnych požiadaviek (audit),
- sledovať nové hrozby a zraniteľnosti a aktualizovať minimálne požiadavky a súbor základných opatrení (baseline),
- pravidelne vyhodnocovať stav kybernetickej bezpečnosti prostredníctvom vykonávania kontrol dodržiavania štandardov ISVS a bezpečnostných auditov,

- pripraviť a udržiavať vzorové/šablónové riešenia pre všetky požadované opatrenia kde je tento prístup možný – napr. analýza rizík, katalóg hrozieb,
- riadiť rozdelenie zodpovednosti za bezpečnosť a plynulú prevádzku vzájomne prepojených a závislých IS.

Úlohy sú jednorazové, ale na vypracovanie Štandardov ISVS bude potrebné nadviazať metodickou a kontrolnou činnosťou. Rovnako riešenie informačno-bezpečnostných incidentov a sledovanie hrozieb a zraniteľností sú dlhodobé úlohy, ktoré by mohli riešiť CSIRT-y, ale na aktualizáciu záväzných štandardov pre ISVS je potrebná opora v zákone, podporné mechanizmy a tiež dostatočná odborná a personálna kapacita na ústrednom orgáne, ako aj v rámci jednotlivých ÚOŠS.[12] Odporúčame použiť COBIT na mapovanie pre všetky procesy povinnej osoby, ale hlavne premostenie na argumentáciu v GAP analýze, čo chýba v štandardoch ISVS, kde:

[12] Katalóg hrozieb, zraniteľností a opatrení Spolkového úradu pre informačnú bezpečnosť má niekoľko tisíc strán.

- štandardy ISVS pre pokrytie úplne chýbajú alebo
- ich je potrebné doplniť tak, aby to zlepšilo jednoznačnosť textu, ako aj praktickú implementáciu špecificky pre kybernetickú bezpečnosť,
- je potrebné existujúce štandardy podporiť z pohľadu efektívnej aplikácie, t. j. štandardy sú jednoznačné, avšak často sa v praxi nedodržiavajú.

3.4 Systematické zabezpečenie informačnej bezpečnosti vo verejnej správe

Pre systematické zabezpečenie ochrany organizácií verejnej správy musí byť táto ochrana založená na štyroch pilieroch :

- Prevencia - definícia bezpečnostných štandardov, definícia procesov a ich implementácia
- Reakcia – riešenie bezpečnostných incidentov, proaktívne a reaktívne služby riešenia bezpečnostných incidentov
- Podpora - zabezpečenie dostatočných materiálnych, finančných, personánych a technických zdrojov pre inštitúcie verejnej správy na vykonávanie požadovaných úloh v rámci kybernetickej bezpečnosti.[13]
- Kontrola – kontrolná činnosť dodržiavania bezpečnostných štandardov, vykonávanie bezpečnostných auditov, ohodnotení zraniteľností a penetračných testov,

doplnená a zastrešená systematickým riadením KIB vo verejnej správe na na nadrezortnej úrovni.

3.4.1 Prevencia a riadenie KIB

Pre štandardizáciu postupov v oblasti riadenia[14] bezpečnosti v ISVS by bol veľmi nápomocný holistický procesný model, ktorý by bol nastavený ako referenčný model pre riadenie IT v štátnej správe. Rozumným základom sa javí COBIT, ktorý je používaný aj v mnohých veľkých korporáciách.

Procesný model COBITu a framework sú popísané v prílohe 9.9. Tabuľka mapovanie funkcií CSF na procesy COBITu pre ďalšie rozpracovanie v komplexnom procesnom modeli[15] je uvedená ako príloha 9.10 v samostatnom súbore frameworkCSF_MappingCOBIT_StandardyISVS.xlsx.

Na úrovni riadenia informačnej bezpečnosti vo verejnej správe je potrebné definovať a implementovať procesy riadenia informačnej bezpečnosti vo verejnej správe. Vhodným riešením sa javí pre tento účel vybudovať centrálny riadiaci a koordinačný orgán na ÚOŠS zodpovednom za ISVS. Toto riešenie je potom rozpracované v ďalších kapitolách tohto dokumentu.

V rámci riadenia KIB je potrebné na úrovni organizácií podporených centrálnym orgánom zabezpečiť:

- organizačne, materiálne a personálne zabezpečiť riešenie informačnej bezpečnosti v organizácií vrátane zabezpečenia spôsobilostí riešenia bezpečnostných incidentov v rámci organizácie,
- implementovať štruktúry riadenia informačnej bezpečnosti na rezortnej,
- implementovať systém riadenia informačnej bezpečnosti v organizácií (vrátane analýzy bezpečnostných rizík) a implementáciu bezpečnostných opatrení za účelom vytvorenia bezpečnostného baseline v organizácií,

[13] Bude samostatne rozpracovaný ako dokument UPVII.

[14] Rozpracované v kapitole 6.8.

[15] Úloha spracovať v samostatnom projekte komplexný procesný model pre všetky aktivity informačnej bezpečnosti na úrovni governance, manažment či už v organizácii povinnej osoby alebo e-Govermente štátu/rezortu.

- pravidelné vykonávať kontrolné činnosti (audity bezpečnosti vrátane penetračných testov).

Vzhľadom na štruktúru Internetu, typy a rozsahy hrozieb a potrebné odborné spôsobilosti na ich zvládanie je potom na vládnej úrovni ďalej potrebné:

- vytvoriť/dobudovať spôsobilostí poslednej inštancie na vládnej úrovni,
- vytvoriť/dobudovať spôsobilostí na analytické a proaktívne činnosti,
- vydávať štandardy v oblasti informačnej bezpečnosti pre organizácie verejnej správy a pravidelne ich aktualizovať,
- vydávať postupy na bezpečnú konfiguráciu jednotlivých technológií (tzv. hardening guidov),
- školiť zamestnancov – špecialistov v oblasti informačnej bezpečnosti,
- zvyšovať povedomie všetkých zamestnancov organizácií.

Na definíciu samotných bezpečnostných štandardov, ako aj systému riadenia informačnej bezpečnosti v organizáciách resp. na národnej úrovni vo verejnej správe je vhodné použiť skupinu štandardov ISO 27000, špeciálne štandardy ISO 27001 a ISO 27005. Tieto štandardy je potrebné doplniť o technické štandardy konfigurácie jednotlivých technológií. Pre verejnú správu bola v roku 2017 vypracovana špecializovaným útvarom CSIRT.SK v spolupráci s Úradom podpredsedu vlády SR pre investície a informatizáciu.[16] metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti. Táto metodika obsahuje požiadavky na organizáciu rozdelenú do oblastí:

- administratívna a organizačná bezpečnosť,
- vývoj a nasadenie informačného systému,
- zabezpečenie externe dostupných služieb,
- zabezpečenie externe dostupných služieb – webové služby,
- zabezpečenie internej infraštruktúry,
- zabezpečenie pracovných staníc.

Motiváciou pre vznik tohto dokumentu bola snaha vytvoriť ucelený podklad pre organizácie verejnej správy na systematické zabezpečenie informačnej bezpečnosti v organizácii, ktorý by odzrkadľoval aktuálne využívané technológie s dôrazom na nasadzovanie projektov implementovaných v rámci Operačného programu integrovaná infraštruktúra. Hoci bola metodika pôvodne navrhnutá pre zabezpečenie informačnej bezpečnosti infraštruktúry a riešenia implementovaného v rámci projektov Operačného programu integrovaná infraštruktúra je aplikovateľná aj pre ďalšie typy informačných systémov, webových aplikácií i koncových staníc organizácií verejnej správy.

Požiadavky uvedené v dokumente boli vybrané tak, aby po ich splnení organizácia mala zabezpečenú základnú úroveň bezpečnosti (baseline), ktorá pokrýva štandardné bezpečnostné hrozby pre organizáciu.

3.4.2 Reakcia na bezpečnostné incidenty a narušenia základných atribútov informačnej bezpečnosti

V rámci riešenia incidentov a narušenia základných atribútov informačnej bezpečnosti na národnej úrovni vo verejnej správe je potrebné rozdeliť riešenie incidentov na tieto časti:

- príprava na riešenie bezpečnostných incidentov
- riešenie bezpečnostných incidentov v rámci organizácie
- koordinácia riešenia bezpečnostných incidentov na úrovni rezortu

[16] https://www.csirt.gov.sk/aktualne-7d7.html?id=120.

- koordinácie riešenia bezpečnostných incidentov na národnej úrovni vo verejnej správe.
- koordinácia riešenia bezpečnostných incidentov na medzinárodnej úrovni a na na národnej úrovni s centrálnym orgánom pre kybernetickú bezpečnosť

Príprava na riešenie bezpečnostných incidentov a narušenia základných atribútov informačnej bezpečnosti z hľadiska organizácie obsahuje minimálne nasledujúce kroky[17]:

- zber údajov o infraštruktúre
- príprava technických spôsobilostí a komunikačných kanálov
- implementácia detekčných mechanizmov v rámci organizácie
- návrh a implementácia procesu riešenia bezpečnostných incidentov

Okrem uvedených mechanizmov je potrebné dostatočne zabezpečiť efektívnu spoluprácu medzi jednotlivými zložkami pri riešení bezpečnostných incidentov.

Pre jednotlive zložky a organizačné útvary je potrebné vypracovať komplexné komunikačné a koordinačné schémy, implementovať zodpovedajúce procesy a pravidelne ich testovať.

3.4.3 Podpora realizácie úloh

Za bezpečnosť svojich ISVS zodpovedá ich správca, ktorý v spolupráci s prevádzkovateľom zaisťuje nasadenie a prevádzku stanovených bezpečnostných opatrení a realizáciu ďalších úloh v oblasti KIB. Už v súčasnosti je množstvo úloh, ktoré správca musí za týmto účelom zabezpečiť enormné. Na základe doterajších skúseností môžeme konštatovať, že jedným z hlavných dôvodov nedostatočného plnenia úloh v oblasti KIB zo strany orgánov verejnej moci (ďalej len „OVM“) je nedostatok potrebných zdrojov.

Do budúcnosti je možné predpokladať ďalšie zvýšenie počtu týchto úloh a aj tlaku na ich realizáciu, ktoré vyplýva najmä z nárastu hrozieb v oblasti KIB a prechod na centrálne riadenie v tejto oblasti.

Preto je nevyhnutné všetkým OVM zaistiť dostatočnú podporu pre realizáciu jednotlivých úloh, najmä pomocou uplatnenia nasledovných prístupov:

- v gescii ÚPVII vytvorenie a udržiavanie centrálneho prehľadu úloh a opatrení v oblasti KIB, ktoré sú jednotlivé typy OVM povinné realizovať, bez ohľadu na zdroj povinnosti,
- systematické centrálne zaisťovanie podpory pre OVM, najmä vyčlenením dostatočných finančných prostriedkov na realizáciu úloh v oblasti KIB,
- stav plnenia najdôležitejších úloh v oblasti KIB, stav kapacít OVM v tejto oblasti a plán ďalšieho postupu má byť deklarovaný v Koncepcii rozvoja ISVS jednotlivých OVM,
- pri plánovaní nových úloh v oblasti KIB, napr. pri zmenách legislatívy, prijímaní štandardov atď. je potrebné vždy vyhodnotiť dopady na OVM ktoré ich majú vykonávať a zaistiť pre nich dodatočné zdroje potrebné na realizáciu nových úloh.

Ako jeden z prvých krokov v tejto oblasti by jednotlivé OVM mali vykonať rozdielovú analýzu súčasného stavu plnenia požiadaviek a úloh v oblasti KIB voči všetkým povinnostiam v tejto oblasti. Na základe takto deklarovaného stavu ÚPVII zaistí pre OVM zdroje potrebné na dosiahnutie uspokojivého stavu v oblasti KIB, odporúčame formou centrálne financovaných dopytových výziev.

[17] Jednotlivé kroky sú podrobne rozpísané v Metodike pre spoločné postupy a podporu.

3.4.4 Kontrolné mechanizmy a mechanizmy posúdenia bezpečnosti

Nevyhnutným predpokladom vytvorenia a udržania požadovanej úrovne informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom sú kontrolné mechanizmy resp. mechanizmy na posúdenie bezpečnosti[18] .

Niektoré mechanizmy posúdenia bezpečnosti sú špecifikované v tabuľke č. 1. Pre každý mechanizmus sú uvedené:

- názov mechanizmu posúdenia informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom,
- popis mechanizmu posúdenia informačnej bezpečnosti z hľadiska odolnosti voči kybernetickým útokom,
- cieľ mechanizmu (dôvod vykonávania),
- frekvencia opakovania : potrebná periodicita vykonania posúdenia informačnej bezpečnosti,
- predpoklady vykonania daného posúdenia informačnej bezpečnosti,
- súvisiace aktivity.

Názov	Popis	Cieľ	Frekvencia opakovania	Predpoklady	Súvisiaca aktivita
Analýza rizík	Identifikácia a posúdenie rizík informačnej bezpečnosti na základe identifikácie a ohodnotenia aktív, bezpečnostných zraniteľností a bezpečnostných hrozieb a ohodnotenie pravdepodobnosti a možných dopadov zneužitia zraniteľnosti aktíva hrozbou.	Získanie prehľadu o rizikách informačnej bezpečnosti, prioritizácia ich zmierňovania, identifikácia opatrení na ich zmiernenie, určenie miery akceptovateľného rizika.	Vždy pred nasadením IS do produkčného prostredia. Aspoň raz ročne aktualizácia a prehodnotenie zvyškových rizík.	Stredná úroveň vyspelosti bezpečnostných opatrení.	Audit informačnej bezpečnosti
Audit informač-nej bezpečnosti	Technické, procesné alebo dokumentačné posúdenie informačnej bezpečnosti	Posúdenie zhody informačnej bezpečnosti so štandardom alebo súlad s legislatívnymi, normatívnymi, regulačnými alebo zmluvnými požiadavkami.	Podľa zákona č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov	Stredná úroveň vyspelosti bezpečnostných opatrení, nezávislosť audítora na predmete auditu.	Analýza rizík, Posúdenie zraniteľností

[18] Uvedené mechanizmy je možné nahradiť ekvivalentnými mechanizmami v prípade, že ich súčasťou budú výstupy špecifikované nižšie.

Posúdenie zraniteľ-ností	Identifikácia a technické posúdenie bezpečnostných zraniteľností	Identifikácia čo možno najväčšieho množstva zraniteľností a ich závažnosti a prioritizácia ich odstraňovania.	Vždy pred nasadením IS do produkčného prostredia. Aspoň raz ročne.	Nízka alebo stredná úroveň vyspelosti bezpečnostných opatrení, počiatočné fázy implementácie bezpečnostného programu.	Penetračné testovanie
Penetrač-né testovanie	Technické posúdenie informačnej bezpečnosti za použitia techník a nástrojov útočníkov, ide napr. o prienik do IS a následnú exfiltráciu údajov, získanie doménového administrátora alebo modifikáciu informácií.	Overenie úrovne zabezpečenia informačných systémov pred počítačovými útokmi, identifikovanie zraniteľností a navrhnutie bezpečnostných opatrení	Po implementácii všetkých opatrení vyplývajúcich z posúdenia zraniteľností. Aspoň raz za tri roky.	Vysoká úroveň vyspelosti bezpečnostných opatrení, predchádzajúce vykonanie viacerých posúdení zraniteľností a implementácia všetkých opatrení.	Posúdenie zraniteľností, Red Teaming

Uvedené mechanizmy sú minimálnou množinou kontrolných mechanizmov na úrovni organizácie, rezortu/sektora úrovni na komplexné posudzovanie informačnej bezpečnosti, ktoré je potrebné implementovať na získanie prehľadu o stave informačnej bezpečnosti v organizácií resp. rezorte/sektore.

Špecialne audit bezpečnosti informačných systémov je bežne používaným nástrojom kontroly dodržiavania štandardov, pri ktorom sa dajú dobre využiť externí audítori. Bude však potrebné špecifikovať požiadavky na audit, ako aj požiadavky na kvalifikáciu audítorov. Tento krok bude implementovaný prostrednítvom vytvorenia vzorových / šablónových riešení pre organizácie verejnej správy tam kde je to možné, tak aby tieto vzorové riešenia boli s minimálnymi nárokmi na čas, spôsobilosti a peniaze interpretované a využiteľné v podmienkach organizácií verejnej správy. Tieto riešenia budú založené na medzinárodných normách ISO a NIST .

3.5 Budovanie odborných kapacít

Nakoľko bez kvalifikovaných odborníkov sa KIB nedá zaistiť, ide o prvoradú a kľúčovú úlohu. Viacero koncepčných, metodických aj realizačných problémov riešilo v minulosti MF SR a jeho výsledky sa po prehodnotení a aktualizácii budú dať využiť. Niektoré aktivity (ak na to budú k dispozícii potrebné kapacity) bude možné spustiť súčasne. ÚPVII pre budovanie odborných kapacít zabezpečí

- identifikovanie potrieb (koľko a akých odborníkov SR/štátna sféra potrebuje),
- špecifikáciu potrebných znalostí, zručností a schopností pre jednotlivé špecializácie (neskôr aj formálnu definíciu špecializácií),
- identifikácia nositeľov potrebného know-how použiteľných na školiacu činnosť, možné školiace kapacity v zahraničí (pre oblasti, kde nemáme dostatočne kvalifikovaných vlastných ľudí),
- stanovenie priorít – akých ľudí potrebujeme vyškoliť najskôr,

- spustenie projektu vzdelávania zameraného na vybudovanie výučbových kapacít a spustenie vzdelávania v KIB (revízia študijných materiálov MF SR a vydanie opraveného a doplneného vydania, terminologický slovník v informačnej bezpečnosti).

Súčasne s týmito aktivitami je možné

- riešiť stabilizáciu odborníkov na KIB v štátnych inštitúciách,
- podporovať vzdelávanie v KIB v rámci existujúcich programov na vysokých školách (informatici, manažéri, právnici), nové špecializácie, postgraduálne vzdelávanie, celoživotné vzdelávanie.

Neskôr je možné vypracovať[19], ale **najmä zaviesť do praxe** komplexný systém vzdelávania v KIB KIB vo verejnej správe v spolupráci s NBÚ. Pre verejnú správu z hľadiska KIB rozlišujeme štyri skupiny zamestnancov, a to vedúci pracovníci, manažéri KIB, informatici a laickí používatelia. V projekte MF SR boli vypracované a na pomerne širokej skupine účastníkov aj prakticky overené materiály a metodika pre tieto skupiny a v priebehu cca jedného roka je možné spustiť vzdelávanie pre vedúcich pracovníkov a manažérov KIB. Ďalším dôležitým krokom by malo byť nastavenie potrebnej úrovne vzdelávania v oblasti KIB pre všetkých pracovníkov verejnej správy (podobne, ako je to pri BOZP).

3.6 Vypracovanie metodického rámca pre riadenie KIB vo verejnej správe

3.6.1 Metodický rámec riadenia KIB vo verejnej správe

Kybernetická a informačná bezpečnosť v podsektore informačných systémov verejnej správy je riadená sektorovým ústredným orgánom ÚPVII. V rámci ÚPVII má KIB na zodpovednosť sekcia kybernetickej bezpečnosti ÚPVII (ďalej len „Sekcia“).

Hlavnou úlohou Sekcie je revízia, aktualizácia, dopracovanie metodiky riadenia informačnej bezpečnosti na všetkých úrovniach verejnej správy ako aj jej exekúcia. Systém riadenia KIB by mal byť centralizovaný s metodickým riadením bezpečnostných pracovníkov na jednotlivých ÚOŠS (tzv. maticový model, podobný už začína ÚPVII používať pri rozpočtovaní výdavkov na IT).

Vzhľadom na aktuálny stav bude musieť byť zadefinovaná modelová štruktúra riadenia KIB na ÚOŠS.

3.6.1.1 Hlavné úlohy Sekcie v oblasti ISVS

Generálny riaditeľ Sekcie je zároveň Chief Information Security Officer (CISO) pre ISVS, ktorý zodpovedá za riadenie a presadzovanie KIB vo verejnej správe ako hlavná autorita. CISO stojí na čele Sekcie, ktorá metodicky riadi všetkých manažérov informačnej bezpečnosti v organizáciách verejnej správy.

Úlohou Sekcie bude hlavne v spolupráci s NBÚ a ostatnými orgánmi verejnej správy:

- definovanie stratégie KIB vo verejnej správe,
- vytvorenie a exekúcia formálneho rámca riadenia KIB vo verejnej správe,
- definovanie opatrení KIB pre informačné systémy verejnej správy a ich detailné metodologické rozpracovanie,

[19] Stále je aktuálny Systém vzdelávania v informačnej bezpečnosti, schválený vládou SR v roku 2009.

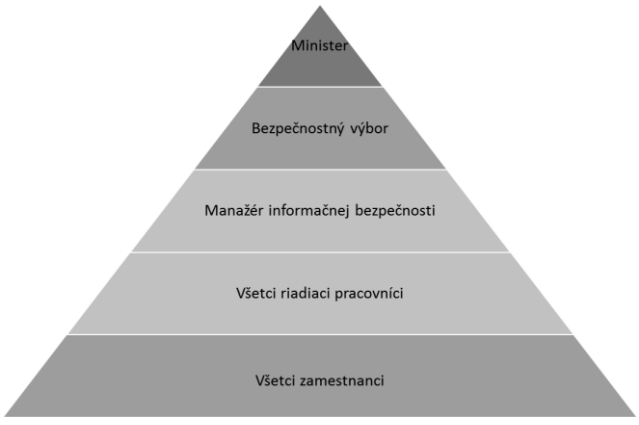
- monitorovanie úrovne implementácie definovaných opatrení KIB vo verejnej správe,
- vyhodnocovanie efektivity definovaných opatrení KIB vo verejnej správe,
- pravidelné vyhodnocovanie a reportovanie stavu KIB vo verejnej správa,
- optimalizácia a kontinuálne zlepšovanie úrovne opatrení KIB vo verejnej správe,
- vypracovávanie odborných analýz a podkladov pre rozhodovanie vo veciach, alebo v prípade rozporov o oblasti KIB vo verejnej správe,
- vyjadrovanie sa, schvaľovanie významných projektov týkajúcich sa KIB vo verejnej správe,
- komunikácia so zúčastnenými stranami, verejnosťou a výrobcami bezpečnostných technológií,
- spolupráca s akademickou obcou, odbornou verejnosťou a profesijnými združeniami,
- komunikácie so zahraničnými partnerskými organizáciami,
- plánovanie prostriedkov na rozvoj KIB vo verejnej správe,
- predkladanie návrhov na legislatívne zmeny.

Taktiež bude potrebné definovať jednotlivých špecialistov a oblasti, v ktorých budú vykonávať svoje aktivity. Pozície by mali byť špecializované hlavne na nasledovné oblasti:

- riadenie rizík
- metodickú činnosť
- analytickú činnosť
- osveta a bezpečnostné vzdelávanie
- komunikáciu
- špecialisti pre ochranu osobných údajov
- technologický špecialisti (virtualizácia, operačné systémy, aplikácie, databázy, sieťové technológie a pod.)
- technologický špecialisti na priemyselné systémy (Industrial Control Systems).

3.6.1.2 Organizačná štruktúra riadenia KIB na ÚOŠS

Aktívne, kontinuálne a rutinné riadenie KIB by malo byť realizované na jednotlivých ÚOŠS, na podriadených organizáciách verejnej správy je riadenie organizované analogicky. Riadenie KIB musí mať hierarchickú štruktúru ako je uvedené na nasledovnom obrázku.



Pri organizácii riadenia KIB na ÚOŠS musia byť uplatnené nasledovné základné zásady:

- vrcholný orgánom pre riadenie KIB na ÚOŠS je minister (prípadne iný štatutár),
- bezpečnostnú stratégiu definuje a riadi bezpečnostný výbor (alebo iný kolektívny orgán), ktorý je zároveň poradným a iniciatívnym orgánom ministra,

- za riadenie a koordináciu informačnej bezpečnosti, určovania zásad, tvorbu, aktualizáciu a presadzovanie bezpečnostnej politiky zodpovedá manažér kybernetickej bezpečnosti ktorý je vlastníkom procesu riadenia a zaisťovania KIB na ÚOŠS,
- manažér kybernetickej bezpečnosti musí byť nezávislý od riadenia prevádzky a vývoja služieb informačných technológii
- na procese riadenia a udržiavania KIB sa podieľajú všetky jeho organizačné útvary v rozsahu svojej pôsobnosti.

Vzťah manažér kybernetickej bezpečnosti k Sekcii:

- manažér kybernetickej bezpečnosti bude metodicky riadený CISO pre ISVS (tzv. dotted line reporting),
- Sekcia bude poskytovať manažérovi kybernetickej bezpečnosti metodickú podporu, odbornú podporu, podporu pri riešení bezpečnostných incidentov,
- Sekcia bude slúžiť ako eskalačný subjekt,
- manažér kybernetickej bezpečnosti bude zodpovedný za implementáciu stanovených bezpečnostných opatrení a ich reportovanie prostredníctvom portálu (self-assessment) Sekcie,
- Sekcia bude oprávnená vykonávať kontrolné aktivity samostatne, alebo prostredníctvom tretích osôb (napr. audítorské spoločnosti),
- Sekcia bude aj posudzovať a schvaľovať všetky významné projekty v oblasti KIB za účelom zaistenia ich súladu s celkovou stratégiou KIB vo verejnej správe.

Základným cieľom spolupráce ÚOŠS so Sekciou je poskytovanie metodickej podpory, zdieľanie znalostí a skúseností medzi jednotlivými inštitúciami verejnej správy navzájom, riešenie problémov nadrezortného charakteru s cieľom postupného zvyšovania celkovej úrovne KIB vo verejnej správe. Účelom kontrolných opatrení však bude primárne zisťovanie úrovne porozumenia metodike, úrovne efektivity stanovených opatrení v praxi ako ďalší prostriedok pre získanie spätnej väzby a až v druhom rade iba ich striktné vynucovanie.

Podobná hierarchia v riadení KIB bude uplatňovaná aj vo vzťahu manažér kybernetickej bezpečnosti a organizáciám podriadeným ÚOŠS .

Pre nadrezortné informačné systémy, t.j. informačné systémy verejnej správy, ktoré hierarchicky integrujú spoločné časti jednotlivých informačných systémov verejnej správy, ktoré sú v pôsobnosti iných správcov, do hierarchicky vyššieho informačného systému verejnej správy bude potrebné určiť jednoznačného správcu, ktorý bude vykonávať v oblasti riadenia KIB obdobné úlohy ako ÚOŠS (definovaná pozícia manažéra informačnej bezpečnosti), organizačný útvar KIB a pod.). V prípade potreby môžu byť tieto štruktúry vytvorené v Sekcii.

3.7 Budovanie bezpečnostného povedomia

Každý, kto prichádza do styku s ISVS (digitálnymi IKT vo všeobecnosti) by mal mať aspoň základné vedomosti o KIB, dostatočné na to, aby svojou činnosťou nepoškodil systémy, s ktorými pracuje, neohrozil iných ľudí a neporušil zákony a pravidlá pre prácu s danými systémami. Základné princípy KIB sú univerzálne, ale spôsob práce a obmedzenia na používanie konkrétnych systémov špecifické. Budovanie bezpečnostného povedomia má z obsahového hľadiska dve zložky – základnú (všeobecnú) a špecifickú. Štát (národná autorita) môže posilňovať z centrálnej úrovne všeobecnú zložku bezpečnostného povedomia (povinné školenia zamestnancov verejnej správy, propagácia, kampane, cvičenia,...), zabezpečiť preškolenie učiteľov stredných a základných škôl (pilotný projekt) zaradenie základných poznatkov KIB do výučby na stredných a základných školách (príprava e-learningových

materiálov), prípadne vydávať metodické materiály KIB pre dospelých. Konkrétne školenia zamestnancov v IB/KB, musia robiť lokálni manažéri KIB (alebo lektori), aby vo vzdelávaní dokázali aplikovať všeobecné princípy na konkrétne podmienky organizácie.

ÚPVII by si mal pre plnenie úloh v tejto oblasti prevziať vybrané úlohy z Akčného plánu, ktoré boli pôvodne dané MF SR v oblasti ISVS (odporúčanie pracovnej skupiny):

Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
1.9 Vytvoriť nadrezortný program „Ochrana kybernetického priestoru Slovenskej republiky“	V rámci priorít vlády SR predložiť na rokovanie vlády SR program „Ochrana kybernetického priestoru Slovenskej republiky“ v horizonte do roku 2025 obsahujúci súhrn projektov, aktivít, prác, činností a dodávok vykonávaných na splnenie zámerov a cieľov podľa rozpočtových pravidiel.	NBÚ	MF SR ÚV SR	2/2016
4.4 Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti	Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti, ktoré zabezpečí vzdelávanie a dosiahnutie aspoň základnej úrovne kompetencií v oblasti kybernetickej bezpečnosti všetkých pedagogických zamestnancov v regionálnom školstve, inovovať praktickú prípravu budúcich učiteľov.	MŠVVaŠ SR	MF SR	6/2017
4.5 Systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti	Navrhnúť a zaviesť systematické šírenie osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy.	MF SR		6/2017
4.6 Zabezpečiť školenie o kybernetickej bezpečnosti	Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o oblasti kybernetickej bezpečnosti a zabezpečiť jej realizáciu.	MF SR		2017
6.3 V rámci stredoeurópskeho priestoru rozvíjať spoluprácu	Aktívne sa podieľať, rozvíjať a podporovať spoluprácu Stredoeurópskej platformy kybernetickej bezpečnosti (Central Europe Cyber Security Platform, CECSP)	NBÚ	MF SR MO SR NASES	

3.8 Vytvorenie rámca požiadaviek a postupov pre implementáciu a koordináciu požiadaviek GDPR regulácie v systémoch ISVS

Na účely zabezpečenia ochrany osobných údajov a implementácie požiadaviek nariadenie EPaR č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „regulácia “), ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) budú rovnako vypracované opatrenia a metodické postupy.

Implementácia opatrení pre ochranu osobných údajov vo verejnej správe by mala byť špecificky koordinovaná a vyhodnocovaná Sekciou rovnakým spôsobom ako úroveň implementovaných bezpečnostných opatrení.

Osobné údaje budú zaradené do adekvátnej klasifikačnej triedy, kde budú stanovené povinné bezpečnostné opatrenia, ktoré budú musieť byť aplikované. Potreby regulácie GDPR budú musieť byť zohľadnené aj pri definovaní bezpečnostných opatrení pre informačné systémy verejnej správy.

3.9 Periodické vyhodnocovanie úrovne implementovaných bezpečnostných opatrení

Periodické vyhodnocovanie úrovne implementovaných bezpečnostných opatrení je nevyhnutným predpokladom pre ich presadzovanie ako aj monitorovanie celkovej úrovne KIB a taktiež pre zabezpečenie ich kontinuálneho zlepšovania.

Vylúči sa tým nežiadúci stav, kde sú určené povinné bezpečnostné opatrenia no v mnohých prípadoch nie sú implementované, alebo sú implementované iba formálne, alebo na veľmi nízkej úrovni (tzv. „na papieri“) resp. sú deklarované, ale v podstate sa neprevádzkujú. Rovnako je potrebné monitorovať ich implementáciu a periodicky vyhodnocovať ich stav, ako aj zabezpečiť podporu Sekcie (eskalácia) v prípadoch, že implementácia nevyhnutných opatrení nie je vedením organizácie dostatočne podporovaná.

Cieľom nie je sankcionovanie, ale dosiahnutie reálneho stavu implementovaných opatrení, a tým adekvátnu úroveň KIB vo verejnej správe. Významným prínosom bude taktiež ich neustále vylepšovanie paralelne s vývojom situácie v kybernetickej bezpečnosti, ako aj v súlade s meniacimi sa požiadavkami praxe nakoľko bude existovať spätná väzba.

Implementácia jednotlivých bezpečnostných opatrení bude odstupňovaná do niekoľkých úrovní podľa rôznych kritérií, tak, aby odrážali efektivitu a merateľnosť uvedeného opatrenia.

3.10 Zahraničná spolupráca

Zahraničná spolupráca je pre zaistenie adekvátnej ochrany. Nízka úroveň zaistenia virtuálneho priestoru v oblasti ISVS ohrozuje aj lepšie chránené systémy v zahraničí, pretože útočník môže viesť útok zo slabo zabezpečeného slovenského systému, nad ktorým prevzal kontrolu. Druhým dôvodom je nekompatibilnosť (legislatívy, štandardov, technických a bezpečnostných riešení), ktorá vylučuje alebo obmedzuje možnosti prepojenia našich a zahraničných systémov a využívania služieb, ktoré sa pomocou nich poskytujú. Tretím dôvodom je zložitosť a dynamický vývoj KIB, rozsah a stúpajúca frekvencia kybernetických útokov. SR ale ani väčšie a informaticky vyspelejšie krajiny nemajú na to, aby na všetky problémy vytvárali vlastné riešenia (drahé, nekompatibilné). Preto je nevyhnutné dohodnúť sa na spoločných riešeniach (princípoch, štandardoch) a kooperácii. Nedostatok odborných kapacít v štátnej správe spôsobuje, že sa SR len v minimálnej miere zapája do odborných projektov, resp. podieľa na práci pracovných skupín EÚ, čím sa okrem iného ochudobňujeme o možnosť poznať v predstihu pripravované opatrenia EÚ, ktorým sa budeme musieť prispôsobiť. určiť, čo by sme od zahraničných partnerov potrebovali a čo im môžeme ponúknuť,

3.11 Vytvorenie potrebného rámca na financovanie riadenia KIB v ISVS

Pre dosiahnutie a udržiavanie adekvátnej úrovne KIB vo verejnej správe (prípadne aj kritickej infraštruktúre) je potrebné vytvorenie inštitucionálneho rámca (podmienky, riadenie, monitorovanie, kontrola) pre financovanie, alebo spolufinancovanie implementácie bezpečnostných opatrení v relevantných operačných programoch napríklad OPII a OP EVS, prípadne OP VaI.

Financovanie školení a vzdelávania špecialistov KIB môže byť financované z iných operačných programov (okrem OP EVS aj OP ĽZ), kde je potrebné vytvoriť priestor a štruktúru pre túto aktivitu.

Pre zabezpečenie financovania bezpečnostných tímov u povinných osôb – ÚPVII má kompetenciu vyjadrovať sa k rozpočtom jednotlivých ÚOŠS správy a preto je potrebné, aby začal sledovať separátne rozpočet na KIB.

3.11.1 Aktuálny stav financovania KIB v ISVS

Na základe vyššie uvedených zámerov sú aktuálne realizované mechanizmy pre financovanie kľúčových aktivít riadenia KIB v ISVS z OPII.

Kľúčové aktivity pre ktoré boli vytvorené mechanizmy financovania z OPII sú:

- Zvýšenie schopnosti reakcie na bezpečnostné incidenty
- Zvýšenie úrovne detekcie a prevencie vzniku bezpečnostných incidentov
- Vzdelávanie špecialistov pre KIB

Zvýšenie schopnosti reakcie na bezpečnostné incidenty

Pre zaistenie efektívnej reakcie na bezpečnostné incidenty ako aj pre poskytovanie niektorých preventívnych služieb (v zmysle § 15 zákona o kybernetickej bezpečnosti pre podsektor ISVS) bol realizovaný národný projekt s názvom „**Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe**“.

Hlavným cieľom národného systému riadenia incidentov kybernetickej bezpečnosti vo VS je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej aj „jednotky CSIRT“) pre podsektor ISVS. Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe predstavuje prvú strategickú fázu budovania celonárodného systému riadenia incidentov kybernetickej bezpečnosti. Prostredníctvom tejto fázy budovania celonárodného systému budú pokryté preventívne a reaktívne služby pre podsektor ISVS.

Zvýšenie úrovne detekcie a prevencie vzniku bezpečnostných incidentov

Za účelom financovania zlepšenia úrovne detekcie a prevencie vzniku bezpečnostných incidentov v ISVS ÚPVII pripravil dopytovú výzvu s názvom „**Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v podsektore IS VS**“.

Cieľom dopytovej výzvy je najmä zvýšenie úrovne zavedených postupov a opatrení týkajúcich sa KIB u prevádzkovateľov ISVS, kde je potreba vybudovať novú, resp. konsolidovať existujúcu bezpečnostnú architektúru. Výzva umôžňuje implementáciu nových, alebo inováciou existujúcich bezpečnostných nástrojov a procesov v nasledovných oblastiach:

- ochrana pred útokmi z externého prostredia,
- detekcia škodlivých aktivít a bezpečnostných incidentov,
- ochrana dát, dátových prenosov a komunikácie,
- budovanie bezpečnostného povedomia.

Vzdelávanie špecialistov pre KIB

Zabezpečenie potrebného počtu špecialistov KIB s adekvátnymi odbornými znalosťami je dôležitým aspektom riadenia KIB v ISVS. Z uvedeného dôvodu ÚPVII v spolupráci s NBÚ ralizuje národný projekt „**Vybudovanie centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti** “ . Jeho úlohou bude Vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti (ďalej len “ Centra”) je reakcia na aktuálny nárast potreby

prehlbovania kvalifikácie a vzdelávania v oblasti kybernetickej bezpečnosti a nutnosť zvyšovania kvalifikácie odborníkov na naplnenie požiadaviek vyplývajúcich zo Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorým sa implementuje smernica EP a rady EÚ 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Centrum bude zamerané na vzdelávanie, výskum, vývoj a tvorbu unikátnych IT prostredí pre analýzu bezpečnostných hrozieb smerujúcich na informačné systémy a simuláciu podmienok v čase kybernetického ohrozenia štátu. Bude možné v ňom simulovať rozsiahle počítačové siete, služby a aplikácie takým spôsobom, aby bolo možné skúmať šírenie kybernetických hrozieb a ich dopady. Prostredie Centra bude možné aktívne využívať na realizáciu vzdelávania v oblasti informačnej a kybernetickej bezpečnosti a nadobúdanie zručností bezpečnostných špecialistov a tímov v sektore verejnej správy.

SWOT analýza navrhovaného riešenia

Silné stránky:

- koncepčný prístup „zhora – nadol“, ktorý pokrýva väčšinu problémových oblastí a navrhuje proces pre riešenie zostávajúcich, ktoré neboli bližšie analyzované / adresované,
- stratégia pre ISVS v tejto oblasti je zasadená do predpokladaného rámca / stratégie, ktorá vzniká v príprave zákona o kybernetickej bezpečnosti (t.j. je použiteľná aj v prípade jeho schválenia, aj neschválenia),
- komplexný návrh, ktorý pokrýva oblasti procesov, ľudí, organizácie a financovania a aj návrh konkrétnych úloh.

Slabé stránky:

- nepokrýva niektoré špecifické oblasti v detaile (Cloud, eGov služby),
- nie je obsahovo takmer nijako prepojená s detailnými cieľmi iných priorít NKIVS (ani s už ukončenými, ani s tými rozpracovanými),
- neobsahuje žiadne výpočty / odhady nákladov potrebných na implementáciu.

Možnosti:

- obsahové prepojenie rozpracovaných dokumentov NKIVS v rámci procesov úradu (t.j. aj úprava tohto) môže viesť k ich zlepšeniu,

Hrozby:

- nedostatok financií na navrhované opatrenia ,
- vznik národného českého centra pre kybernetickú bezpečnosť v Brne.

4 Ďalšie kroky a odporúčané úlohy

Aby boli navrhované riešenia v predchádzajúcej kapitole úspešne uvedené do praxe a dosiahli požadovaný cieľ / účinok, sú upravené do konkrétnych krokov a potrebných úloh. Kde bolo možné, PS uviedla aj odhady nákladov / časový rozsah. V prípade schválenia tohto dokumentu internými vlastníkmi na ÚPVII, bude potrebné všetky potrebné údaje / odhady do navrhovaných úloh doplniť.

4.1 Organizačno-kompetenčné zabezpečenie riadenia KIB vo verejnej správe

Ú.1 Organizačné a personálne zaistenie KIB na ÚPVII	
Názov	Posilnenie organizačnej štruktúry pre Sekcie a jej personálne obsadenie na ÚPVII.
Špecifikácia	Koordináciu riešení úloh na zaistenie KIB ISVS bude potrebné doplniť personálne Sekciu KIB a zabezpečiť jej osadenie odborne dostatočne kvalifikovanými ľuďmi.
Zdôvodnenie	ÚPVII má v oblasti KIB množstvo úloh. Väčšinu z nich budú riešiť externé subjekty, ale časť bude musieť riešiť ÚPVII priamo vlastnými silami a aj tie, ktoré zadá externým subjektom, bude musieť kontrolovať a koordinovať.
Výstupy	• špecifikácia úloh, ktoré má navrhovaný organizačný útvar plniť, • organizačná štruktúra , • pozície so špecifikáciou úloh, ktoré pracovník na danej pozícii má plniť, požadovanými odbornými predpokladmi, špeciálnymi požiadavkami (napr. bezpečnostná previerka), forma zamestnania, navrhované finančné ohodnotenie.
Riešiteľ	ÚPVII
Termín	
Zdroje	• návrh na organizačnú štruktúru, úlohy, počty a kvalifikáciu zamestnancov, harmonogram budovania útvaru, základné dokumenty útvaru, • pracovné miesta, • náklady na o priestory o technické vybavenie o informačné zdroje o cestovanie o vzdelávanie
Kooperujúce orgány	
Poznámka	Keďže kvalifikovaných odborníkov pre KIB nie je dostatok, môže byť problém naplniť stavy Sekcie na ÚPVII kompetentnými ľuďmi. Preto by namiesto definitívneho stavu mohla byť definovaná organizačná štruktúra, ktorá by sa postupne obsadzovala ľuďmi. ÚPVII má podpísané memorandum o spolupráci s vysokými školami, ktoré by mu mohli pripravovať potrebných ľudí, resp. dovzdelávať existujúcich podľa potrieb.

Ú.2 Organizačné a personálne zabezpečenie KIB u povinných osôb	
Názov	Vytvorenie bezpečnostných tímov[20] u povinných osôb
Špecifikácia	Zistiť, čo (minimálne) rôzne typy organizácií (z hľadiska ich rozsahu, druhu činnosti a dôležitosti) potrebujú na zaistenie KIB, navrhnúť pre jednotlivé typy organizácií minimálnu organizačnú štruktúru a podľa

[20] Bezpečnostný tím môže v malej organizácii tvoriť zamestnanec vykonávajúci povinnosti bezpečnostného manažéra na čiastočný úväzok.

	nej v organizáciách vytvoriť bezpečnostné tímy. Identifikovať medzery v požadovaných znalostiach a zabezpečiť doplnenie požadovaného vzdelania.
Zdôvodnenie	Aj povinné osoby budú potrebovať na zaistenie potrebnej úrovne svojich IKT (a plnenie ďalších úloh v KIB) odborné personálne kapacity. V závislosti od veľkosti organizácie, IKT ktoré používa a úloh ktoré pomocou IKT plní, budú organizácie potrebovať minimálne manažéra KIB (na plný alebo čiastočný úväzok), prípadne (primerane potrebám a úlohám organizácie) aj bezpečnostný tím.
Výstupy	• identifikovanie základných typov organizácie z hľadiska ich bezpečnostných potrieb, • rámcový návrh organizačnej štruktúry na zabezpečenie KIB v organizáciách jednotlivých typov, • špecifikácia znalostných, organizačných a iných požiadaviek na členov tímov, • vytvorenie tabuľkových miest s primeraným platovým ohodnotením u povinných osôb (príp. centrálne – Úrad vlády SR).
Riešiteľ	ÚPVII, Úrad vlády SR povinné osoby
Termín	1 rok
Zdroje	
Kooperujúce orgány	
Poznámka	Aj u povinných osôb bude rozumnejšie budovať bezpečnostné tímy postupne, poverením pracovníka organizácie funkciou bezpečnostného manažéra, ktorý dostane metodickú podporu UPVII a odborne sa dovzdeláva, aby bol schopný okrem iného vyhľadať vhodných ľudí na bezpečnostné pozície a riadiť KIB v organizácii.

4.1.1.1 Riešenie personálneho obsadenia odborných pozícií

Všetky uvedené pozície si vyžadujú odborne kvalifikovaný personál. Pre zamestnávanie kvalifikovaného personálu v oblasti KIB vo verejnej správe je potrebné v prvom rade vytvoriť základnú schému.

Je potrebné vytvoriť priestor pre adekvátne ohodnotenie vybraných špecialistov v rámci existujúcich mechanizmov, alebo vytvorením nových mechanizmov pre odmeňovanie, ktorý by umožnili adekvátne ohodnotenie (nie nadhodnotené). Uvedené si pravdepodobne vyžiada dôkladnú analýzu súčasných foriem pracovnoprávnych vzťahov s cieľom nájdenia optimálneho modelu.

V jednotlivých ÚOŠS, prípadne iných inštitúciách verejnej správy (povinné osoby) je potrebné vytvorenie organizačných útvarov zabezpečujúcich úlohy KIB (kde neexistujú) a jednoznačné definovanie ich úloh podľa vyššie uvedených princípov. Pre plnenie týchto úloh bude potrebné vytvorenie junior a senior pozícií. Pre vytvorené pozície zadefinovať pracovnú náplň. Na základe pracovnej náplne budú identifikované kľúčové požiadavky na odborné znalosti a skúsenosti pre plnenie vyžadovaných úloh. Rovnako budú stanovené aj požiadavky na minimálny rozsah znalostí.

Pre stimulovanie motivácie je nevyhnutné aby vyššie platové ohodnotenie zamestnancov nebolo dostupné automaticky. Bezpečnostným špecialistom by bolo umožnené iba po splnení transparentne stanovených kvalifikačných, výkonnostných prípadne iných parametrov. Medzi vyhodnocované

parametre by mali patriť najmä odborná úroveň, proaktívny prístup, inovatívnosť, tímová spolupráca a pod. Uvedený princíp je možné uplatniť pri diferenciácii junior a senior pozícií. ÚPVII môže prostredníctvom svojej koordinačnej roly v príprave IT rozpočtov jednotlivých ÚOŠS kontrolovať, či pre dané kompetencie / procesy sú alokované potrebné zdroje.

Dôležitým faktorom pre nájdenie optimálneho modelu bude aj činnosť Sekcie, ktorá musí detailne rozpracovať opatrenia KIB pre informačné systémy verejnej správy a to do niekoľkých úrovní vyspelosti. Cieľom silnej metodickej podpory zo strany Sekcie bude minimalizácia potreby vynaloženého úsilia pre implementáciu a prevádzku opatrení na úrovni manžéra informačnej bezpečnosti a organizačných zložiek, t.j. výkonných zložiek riadenia KIB. Tým sa do určitej miery ovplyvní aj potreba množstva vysoko kvalifikovaného personálu.

Pre získanie odborných znalosti potrebných pre definované pozície bude potrebné vytvoriť schému interných a externých profesionálnych školení a certifikácií, ktoré budú špecialistom k dispozícii pre ich komplexný rozvoj resp. získanie potrebných odborných znalostí. Kurzy môžu byť realizované elektronicky aj osobnými školeniami, univerzitami ako aj vlastnými zamestnancami špecializovaných odborných útvarov verejnej správy (SK-CERT (NBÚ), CSIRT.SK, Sekcia, PZ SR a pod.).

Všetky školenia a výukové aktivity vrátane interných musia byť finančne ohodnotené a vyčíslené. Zamestnanci pred ich absolvovaním budú musieť uzavrieť so Sekciou zmluvu, kde sa zaviažu po absolvovaní kurzu odpracovať určité obdobie (napr. 5 rokov), alebo v opačnom prípade uhradiť celú výšku nákladov na kurz.

Veľký význam má v tejto oblasti spolupráca s akademickou obcou. Spolupráca s akademickou obcou na úrovni Sekcie by mohla byť realizovaná priamym zapojením talentovaných študentov do riešenia konkrétnych technologických, alebo iných problémov KIB vo verejnej správe. Z pohľadu študentov by sa im naskytla možnosť získavania cenných praktických skúseností pričom by boli ich kapacity využité na riešenie konkrétnych problematických, alebo málo rozvinutých oblastí KIB vo verejnej správe. Taktiež by študenti po skončení štúdia mali možnosť začať ich profesijný rast v oblasti KIB práve vo verejnej správe. Z tohto pohľadu pripadá do úvahy aj vytvorenie centier pre výskum a vývoj v oblasti KIB v spolupráci s univerzitami priamo s účasťou Sekcie.

Na základe vyššie uvedených princípoch bude možné vypracovanie kariérneho rebríčka pre bezpečnostných špecialistov vo verejnej správe (junior, senior, manažér, CERT a pod.) a tak z časti eliminovať fluktuáciu špecialistov.

4.2 Návrh potrebných krokov ÚPVII pre zlepšenie situácie v KIB ISVS v krátkodobom horizonte

Ú 3. Klasifikácia informácií a systémov	
Názov	Vypracovať návrh systému klasifikácie informácií a systémov v rámci podsektora ISVS na základe bezpečnostných požiadaviek na dôvernosť, integritu, dostupnosť a autentickosť informácie a ich zjednotenie do kompaktného a kompatibilného celku v súlade s vyhláškou Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
Špecifikácia	Navrhovaný spôsob klasifikácie musí • rešpektovať existujúce kompetencie pri ochrane informácií a systémov (utajované skutočnosti, osobné údaje, kritická infraštruktúra),

	• umožniť definovať malý počet bezpečnostných tried (3-5), pre ktoré bude možné definovať ucelené súbory opatrení postačujúce na dosiahnutie danej úrovne KIB, • umožňovať úpravy súborov opatrení, rozšírenie bezpečnostných požiadaviek.
Zdôvodnenie	Je potrebné zaistiť základnú úroveň KIB u veľkého počtu systémov, pre ktoré nie je z kapacitných/ekonomických dôvodov možné robiť individuálnu analýzu rizík. Klasifikácia umožňuje kategorizáciu systémov a vypracovanie štandardných súborov opatrení pre jednotlivé kategórie systémov. Na druhej strane pre systémy, pre ktoré nebudú postačovať štandardné opatrenia bude možné rozšíriť navrhovaný súbor alebo spraviť analýzu rizík a prijať opatrenia presahujúce základnú úroveň KIB.
Výstupy	• systém klasifikácie informácií a systémov založený na bezpečnostných požiadavkách na dôvernosť, integritu, autentickosť a dostupnosť, • metodika klasifikácie, • návrh štandardu ISVS.
Riešiteľ	ÚPVII
Termín	Bez termínu
Zdroje	Zladenia sa s dokumentom NBÚ
Kooperujúce orgány	ÚOOÚ SR (osobné údaje)
Poznámka	

Ú.4 Odporúčania pre sprostredkovateľský orgán (OP II, PO7): odsúhlasiť financovanie len pri dodržaní požiadaviek na bezpečnosť	
Názov	Stanoviť povinnosť pri písaní štúdií realizovateľnosti všetkých programov a projektov Podporiť pripájanie systémov ISVS na SIEM podľa výsledku klasifikácie systémov a s ohľadom na možnú optimalizáciu (t.j. nie 1:1, ale pre skupiny) Vyžadovať správu nezávislého audítora bezpečnosti IT pre každý ukončený projekt.
Špecifikácia	
Zdôvodnenie	
Výstupy	• spracovať metodiku pre minimálne bezpečnostné parametre bezpečnostnej architektúry, • zabezpečiť aktualizáciu postupov pri posudzovaní IT rozpočtov (projekty, organizácie) aby boli nutnou podmienkou splnené požiadavky na IT bezpečnosť, • zabezpečiť aktualizáciu Príručky pre prijímateľa.
Riešiteľ	ÚPVII
Termín	priebežne
Zdroje	

Kooperujúce orgány	partneri priojektov

4.3 Vytvorenie štandardných / referenčných postupovv oblasti KIB pre ISVS

Ú. 5 Procesy a postupy	
Názov	Vypracovať návrh procesného modelu v oblasti KIB
Špecifikácia	Vypracovať procesný model pre oblasti KIB, ktorý by slúžil ako návod pre všetky povinné osoby a zároveň umožňoval ďalšie štandardizovanie minimálnej úrovne zabezpečenia KIB ISVS. Procesný model musí byť v súlade so zákonom 69/2018 o kybernetickej bezpečnosti a vyhláškou NBÚ 362/2018 ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
Zdôvodnenie	KIB nie je možné zabezpečiť bez zapojenia všetkých úrovní riadenia. Procesy s implementáciou overených skúseností uznávamých frameworkov zakotvené v povinnostiach pri zabezpečovaní činností (nielen pre KIB) umožnia prístup na báze nadväznosti na plnenie účelu služieb e-Govermentu, ktorý povinné osoby ovlyvňujú prevádzkou ISVS.
Výstupy	Návrh procesného modelu na základe COBIT a CSFs využitím best practices a existujúcich skúseností.
Riešiteľ	ÚPVII
Termín	Q4/2020
Zdroje	
Kooperujúce orgány	

Ú.6 Príprava a udržiavanie šablón dokumentov	
Názov	Pripraviť a udržiavať vzorové šablóny dokumentov pre štruktúru bezpečnostnej dokumentácie požadovanej vyhlaškou 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
Špecifikácia	Pripraviť a udržiavať vzorové šablóny riešenia dokumentov pre štruktúru bezpečnostnej dokumentácie. Ide najmä o nasledovné: • dokument bezpečnostnej politiky • katalóg hrozieb pre IS verejnej správy • šablóna pre vykonanie analýzy rizík • katalóg štandardizovaných bezpečnostných opatrení • bezpečnostné smernice • dokumentácia súvisiaca s riadením kontinuity prevádzky, najmä havarijné plány. Tieto riešenia budú jednotlivými OVM iba jednoducho interpretované, alebo upravené pre vlastnú situáciu a potreby.
Zdôvodnenie	
Výstupy	Šablonové riešenia

Riešiteľ	ÚPVII
Termín	/09/2020
Zdroje	
Kooperujúce orgány	NBÚ

Ú. 8 Prehľad stavu KIB vo verejnej správe SR	
Názov	Raz za dva roky vypracovať prehľad stavu KIB ISVS
Špecifikácia	Prehľad bude založený na viacerých informačných zdrojoch: • dotazníkom rozposielaným orgánom/organizáciám VS sa bude zisťovať stav zabezpečenia ISVS, organizácia a riadenie kybernetickej a informačnej bezpečnosti v organizácii/rezorte, vlastné hodnotenie úrovne KIB v organizácii • CSIRT-y (zraniteľnosti, bezpečnostné incidenty, trendy, činnosť) • ÚOŠS (NBÚ SR, MV SR, MS SR), SIS
Zdôvodnenie	Získanie a udržanie prehľadu o stave, problémoch a trendoch v KIB ISVS. Bude sa využívať pre riadenie aktivít na zaistenie KIB ISVS.
Výstupy	Osnova prehľadu (kvôli zabezpečeniu spolupráce ostatných štátnych orgánov) správa (v slovenčine aj angličtine)
Riešiteľ	ÚPVII (komunikácia s respondentami)
Termín	1 rok
Zdroje	• dotazníky • podklady zo štátnych orgánov • podklady z CSIRT-ov • financie – spracovanie dotazníka 10.000 eur, ostatné závisí od rozsahu a zložitosti analýzy
Kooperujúce orgány	NBÚ SR, CSIRT-y, SIS
Poznámka	

4.4 Vzdelávanie v KIB

Ú.9 Vzdelávanie v KIB	
Názov	Vypracovanie systému vzdelávania v ISVS a pilotný projekt vzdelávania v KIB pre verejnú správu
Špecifikácia	Prehodnotiť získané poznatky a materiály vypracované v rámci projektu vzdelávania v informačnej bezpečnosti MF SR. Stanoviť požadované znalosti a zručnosti pre laikov, vedúcich pracovníkov, informatikov, špecialistov v informačnej bezpečnosti a lektorov. Vypracovať metodiku, obsah a organizáciu vzdelávania. Napísať a vydať základnú učebnicu informačnej bezpečnosti. Realizovať a vyhodnotiť pilotný projekt vzdelávania v KIB pre vyššie uvedené kategórie používateľov IKT.
Zdôvodnenie	Na zaistenie požadovanej úrovne KIB vo verejnej správe sú potrební kvalifikovaní ľudia, ktorých verejná správa nemá a nie sú ani v súkromnom sektore. Riešením je

	využitie existujúcich odborníkov na urýchlenú prípravu zamestnancov verejnej správy v rolách laikov, vedúcich pracovníkov, informatikov, špecialistov v informačnej bezpečnosti a lektorov. MF SR v rokoch 2012-2014 realizovalo projekt vzdelávania v IB, ktorého sa zúčastnilo vyše 1000 ľudí z rôznych inštitúcií verejnej správy. Pre potreby vzdelávania boli vytvorené učebnice, metodické materiály, sylaby, prezentácie. MF SR projekt obsahovo neuzavrelo a tak je potrebné posúdiť aktuálnosť materiálov, doplniť chýbajúce časti a overiť ich v pilotnom projekte. Výsledky pilotného projektu riešitelia vyhodnotia, zapracujú a pripravia dlhodobý projekt postgraduálneho vzdelávania v IB/KB.
Výstupy	Metodika, sylaby, študijné programy pre jednotlivé kategórie používateľov IKT, formy skúšania, učebnice, prezentácie, e-learningové materiály, skúšobné testy, 4 skupiny (200-400) absolventov.
Riešiteľ	UPVII, NBÚ
Doba trvania	2 roky
Zdroje	
Kooperujúce orgány	
Poznámka	

Ú. 10 Vzdelávanie manažérov KIB povinných osôb a pracovníkov Sekcie KIB ÚPVII	
Názov	Doškoľovanie nových pracovníkov v KIB
Špecifikácia	Vytvorenie systému na doškoľovanie nových manažérov KIB povinných osôb a pracovníkov sekcie KIB ÚPVII. Porovnanie znalostí pracovníka s odbornými požiadavkami na pozíciu, ktorú má zastávať, návrh foriem vzdelávania vhodných na doplnenie chýbajúcich vedomostí a zručností, doškolenie a preskúšanie.
Zdôvodnenie	Pri vytváraní sekcie, resp. budovaní útvarov KIB u povinných osôb, neskôr pri obmene zamestnancov bude nutné pracovať aj s ľuďmi, ktorí nemajú dostatočné vzdelanie. Cieľom je rýchle a efektívne doplniť potrebné vedomosti, aby bol daný človek použiteľný pre riešenie úloh pracoviska.
Výstupy	• metodika, testy, výsledky testov, študijné programy • vyškolení zamestnanci ÚPVII a povinných osôb
Riešiteľ	ÚPVII
Termín	1 rok
Zdroje	• príprava testov, • testovanie, vyhodnocovanie a návrh študijných programov pre jednotlivých zamestnancov, • štandardná výučba na vysokých školách, • náklady (učebnice, miestnosti, prednášajúci) na štandardný kurz KIB, • záverečné testovanie,
Kooperujúce orgány	CSIRT-y a štátne orgány s fungujúcimi pracoviskami KIB na špecializované vzdelávania.
Poznámka	Čas a náklady na doškolenie zamestnancov ÚPVII a manažérov KIB bude závisieť od ich predbežných vedomostí a tiež od toho, či už bude možné použiť učebnice a metodiku vzdelávania z úlohy **Vzdelávanie v KIB.**

Ú. 11 Budovanie bezpečnostného povedomia zamestnancov verejnej správy	
Názov	Budovanie bezpečnostného povedomia zamestnancov a verejnosti
Špecifikácia	Vypracovanie systému školení zameraných na budovanie bezpečnostného povedomia zamestnancov verejnej správy (forma, frekvencia, obsah) Sledovanie úspešných foriem budovania bezpečnostného povedomia v zahraničí, spracovanie metodík, materiálov a školení pre bezpečnostných manažérov organizácií a učiteľov SŠ a ZŠ. vytvorenie a aktualizácia webovej stránky
Zdôvodnenie	KIB závisí nielen od špecialistov, ale od všetkých používateľov IKT. Každý z nich by mal vedieť, čo s IKT môže robiť, čo nesmie a čo robiť v prípade, ak nastane problém, ktorý nevie sám riešiť. Všeobecné bezpečnostné povedomie, ktoré sa dá budovať a upevňovať z centra (médiá, videá, bezpečnostné kampane, súťaže, sociálne siete,...) je potrebné doplniť formami zohľadňujúcimi konkrétne podmienky, v ktorých používateľ pôsobí. U zamestnancov by školenie o KIB malo byť súčasťou prijímacieho procesu a je potrebné zvážiť či stanoviť povinné periodické preškoľovanie (ako BOZP) alebo podľa potreby alebo kombinovať periodické a aktualizačné školenia
Výstupy	• obsah potrebných znalostí z KIB pre laických používateľov IKT, • návrh štandardu ISVS, metodiky, • študijné materiály a školenia pre učiteľov, lektorov, bezpečnostných manažérov, • webová stránka úradu zameraná na KIB, kampane, súťaže, propagačné a osvetové akcie.
Riešiteľ	ÚPVII, bezpečnostní manažéri povinných osôb
Termín	trvale
Zdroje	
Kooperujúce orgány	NBÚ, CSIRTy, MŠVVŠ SR, MV SR, Úrad vlády SR

4.4.1 Zvyšovanie bezpečnostného povedomia pre občanov

Pre zvyšovanie bezpečnostného povedomia občanov bude mierne modifikovaný obsah sprístupnený multimediálnou formou bez e-learningových funkcionalít zdarma na stránkach Sekcie / ÚPVII a SK-CERT (NBÚ). Na uvedených webových stránkach si bude môcť každý občan, ktorý bude mať záujem, pozrieť multimediálny obsah zameraný na jednotlivé oblasti (napr. ako vytvoriť bezpečné heslo, bezpečnosť v sociálnych sieťach apod.).

Ďalšou možnosťou je aj sprístupnenie e-learnigovej platformy zvyšovania bezpečnostného povedomia aj podnikateľským subjektom (napr. za nákladovú cenu) a tak im umožniť vzdelať svojich zamestnancov najmä ak pracujú s osobnými údajmi, alebo inými citlivými dátami.

Z dôvodu efektívneho využívania zdrojov bude možné použiť rovnaký, alebo mierne upravený obsah. Obsah bude potrebné prispôsobovať aktuálnym trendom (doplnenie min. 1-2 krát ročne) v prípade potreby aj vo veľmi krátkom časovom období.

5 Záver

Tento dokument vznikol v otvorenom a participantovom procese odborníkov z verejnej správy a komerčného sektora. Dokumentu sa stáva platným a účinným jeho schválením v Rade vlády SR pre digitalizáciu verejnej správy a jednotný digitálny trh. Rozsahom sa dokument zameral na detailnejšie rozpracovanie principiálnych tém v oblasti kybernetickej bezpečnosti vo verejnej správe SR, ktoré boli uvedené v NKIVS.

Z pohľadu aktuálneho stavu v KIB bolo konštatované, že:

- Aktuálnu štátnu stratégiu predstavuje Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020, rozpracovaná v Akčnom pláne realizácie Koncepcie kybernetickej bezpečnosti. Štátnym orgánom zodpovedným za kybernetickú bezpečnosť je NBÚ SR. Oficiálna správa o plnení úloh Akčného plánu zatiaľ nebola zverejnená.
- Štát nemá dostatočné odborné kapacity na riešenie potrebných úloh na centrálnej a rezortnej úrovni, ale ani výkonných pracovníkov na zabezpečenie ochrany vlastných systémov. Potrebných odborníkov (počtom a zameraním) nemá ani súkromná sféra, ani akademický sektor. Bezpečnosť štátu nemožno postaviť na externých spolupracovníkoch.

Vychádzajúc z poznania stavu, kritických problémov a disponibilných zdrojov a zohľadňujúc problémy s realizáciou predchádzajúcich koncepcií, navrhujeme na riešenie globálneho stavu KIB v SR a zvlášť bezpečnosti ISVS nasledujúci postup:

- rýchle riešenie kritických problémov KIB v štáte a v ISVS (v rámci platnej legislatívy, prostredníctvom vzdelávania, štandardizácie, koordinácie činnosti, medzinárodnej spolupráce, podporou existujúcich pracovísk),
- priebežne upresňovanie údajov o stave KIB a bezpečnosti ISVS v SR (monitorovanie a vyhodnocovanie bezpečnostných incidentov, inventarizácia odborných kapacít, možných zdrojov, analytická činnosť, cielený vedecký výskum),
- stanovenie priorít pre systematické riešenie KIB a bezpečnosti ISVS (závisí od zdrojov a malo by sa prehodnocovať raz ročne na úrovni Vlády SR,

Aby boli navrhované riešenia úspešne uvedené do praxe a dosiahli požadovaný cieľ / účinok, sú upravené do konkrétnych krokov a potrebných úloh uvedených v kapitole Ďalšie kroky a odporúčané úlohy. Kde bolo možné, PS uviedla aj odhady nákladov / časový rozsah.

6 Prílohy

6.1 Prehľad najdôležitejších dokumentov KIB SR

- Národná stratégia pre informačnú bezpečnosť v SR, schválená uznesením vlády SR č. 570/2008,
- Návrh systému vzdelávania v oblasti KIB v SR, schválený uznesením vlády SR č. 391/2009,
- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v SR – CSIRT.SK, schválený uznesením vlády SR č. 479/2009,
- Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v SR schválený uznesením vlády SR č. 46/2010,
- Legislatívny zámer zákona o informačnej bezpečnosti, schválený uznesením vlády SR č. 136/2010,
- Správy o plnení úloh z Národnej stratégie pre informačnú bezpečnosť v SR a Akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády SR,
- Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020 (ďalej len „Koncepcia“), schválená uznesením vlády SR č. 328/2015,
- Správa o plnení úloh vyplývajúcich z materiálu Príprava SR na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí SR, schválená uznesením vlády SR č. 334/2015.
- Akčný plán realizácie Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020

6.2 Aktuálny zoznam zákonov a vykonávacích predpisov relevantných pre KIB ISVS

Základný legislatívny rámec kybernetickej a informačnej bezpečnosti súčasnej právnej úpravy SR:

- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,
- Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov,
- Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. v znení neskorších predpisov,
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Nariadenie vlády Slovenskej republiky č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností,
- Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov,
- Ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu,
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov,
- Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Zákon č. 392/2011 Z. z. o obchodovaní s výrobkami obranného priemyslu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

- Výnos Ministerstva vnútra Slovenskej republiky č. 525/2011 o štandardoch pre elektronické informačné systémy na správu registratúry,
- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov,
- Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov,
- Zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov,
- Vyhláška Úradu pre verejné obstarávanie č. 132/2016 Z. z., ktorou sa ustanovujú podrobnosti o postupe certifikácie systémov na uskutočnenie elektronickej aukcie,
- Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom
- trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách),
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
- Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 o postupe pri posudzovaní vplyvu na ochranu osobných údajov,
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,

Vyhlášky Národného bezpečnostného úradu upravujúce ochranu utajovaných skutočností sú:

- Vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky Národného bezpečnostného úradu č. 315/2006 Z. z.,
- Vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní v znení vyhlášky Národného bezpečnostného úradu č. 314/2006 Z. z.,
- Vyhláška Národného bezpečnostného úradu č. 339/2004 Z. z. o bezpečnosti technických prostriedkov,
- Vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií,
- Vyhláška Národného bezpečnostného úradu č. 314/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní,
- Vyhláška Národného bezpečnostného úradu č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti,
- Vyhláška Národného bezpečnostného úradu č. 453/2007 Z. z. o administratívnej bezpečnosti,
- Vyhláška Národného bezpečnostného úradu č. 301/2013 Z. z. o priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa,
- Vyhláška Národného bezpečnostného úradu č. 134/2016 Z. z. o personálnej bezpečnosti,
- Vyhláška Národného bezpečnostného úradu č. 135/2016 Z. z. o skúške bezpečnostného zamestnanca,
- Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
- Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,

- 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.

6.3 Hodnotenie Slovenskej republiky na základe ITU indexu

Metóda zberu dát

GCI obsahuje 25 indikátorov a 157 otázok. Indikátory používané na výpočet GCI zohľadňujú kritériá:

- Relevancia pre 5 GCI kľúčových oblastí[21] a ich príspevku pre ciele GCI
- Dostupnosť a kvalita dát
- Možnosť krížového porovnania

Zloženie indexu je postavené na 5 základných pilieroch:

1. Právny: meria sa na základe existencie právnych rámcov a zodpovednosti inštitúcií zaoberajúcimi sa kybernetickou bezpečnosťou a zločinom.

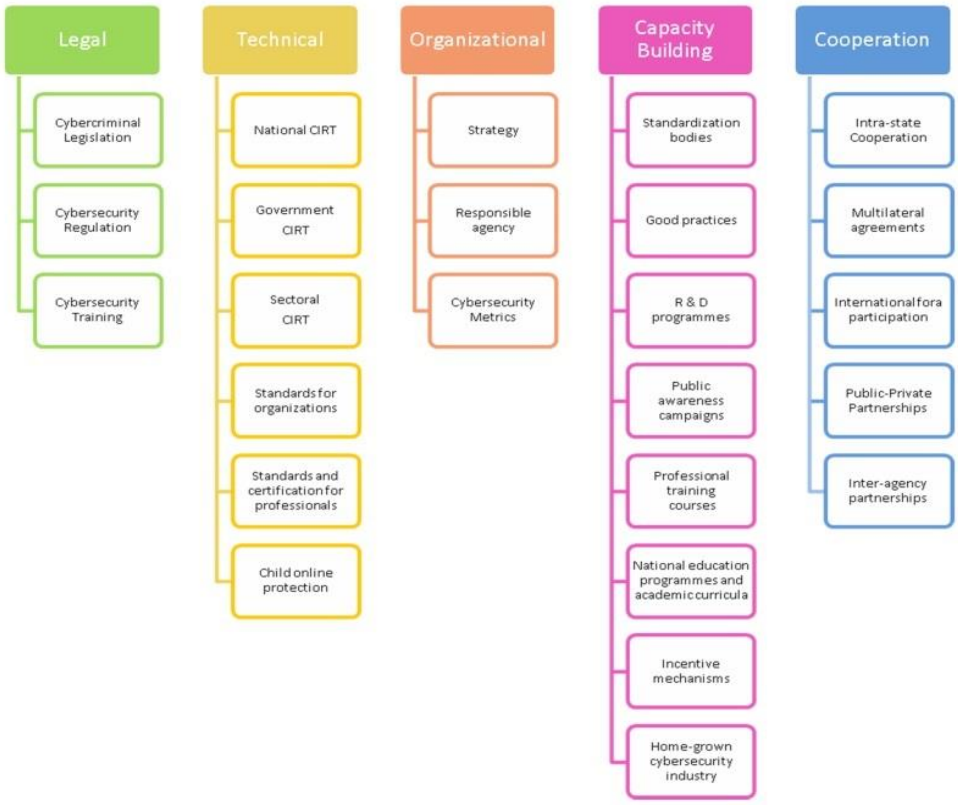
2. Technický: meria sa na základe existencie technických rámcov a zodpovednosti inštitúcií zaoberajúcimi sa kybernetickou bezpečnosťou.

3. Organizačný: meria sa na základe existencie politiky koordinácie inštitúcií a stratégií pre kybernetickú bezpečnosť s ohľadom na rozvoj na národnej úrovni.

4. Budovania kapacít: meria sa na základe existencie výskumu a vývoja, vzdelávania a školiacich programov, certifikácie profesionálov a existencie agentúr verejného sektora podporujúcich budovanie kapacít v oblasti kybernetickej bezpečnosti.

5. Kooperácie: meria sa na základe existencie partnerstiev a rámcov spolupráce a výmeny informácií v oblasti kybernetickej bezpečnosti.

[21] GCI 2017, International Telecommunication Union (ITU) 2017, s. 17 CGI Pillars and Sub-pillars.



Týchto päť oblastí tvorí základ indexu a sú kritickými pri meraní národnej spôsobilosti v oblasti kybernetickej bezpečnosti, ktorej budovanie vyžaduje úsilie na politickej, ekonomickej aj sociálnej úrovni.

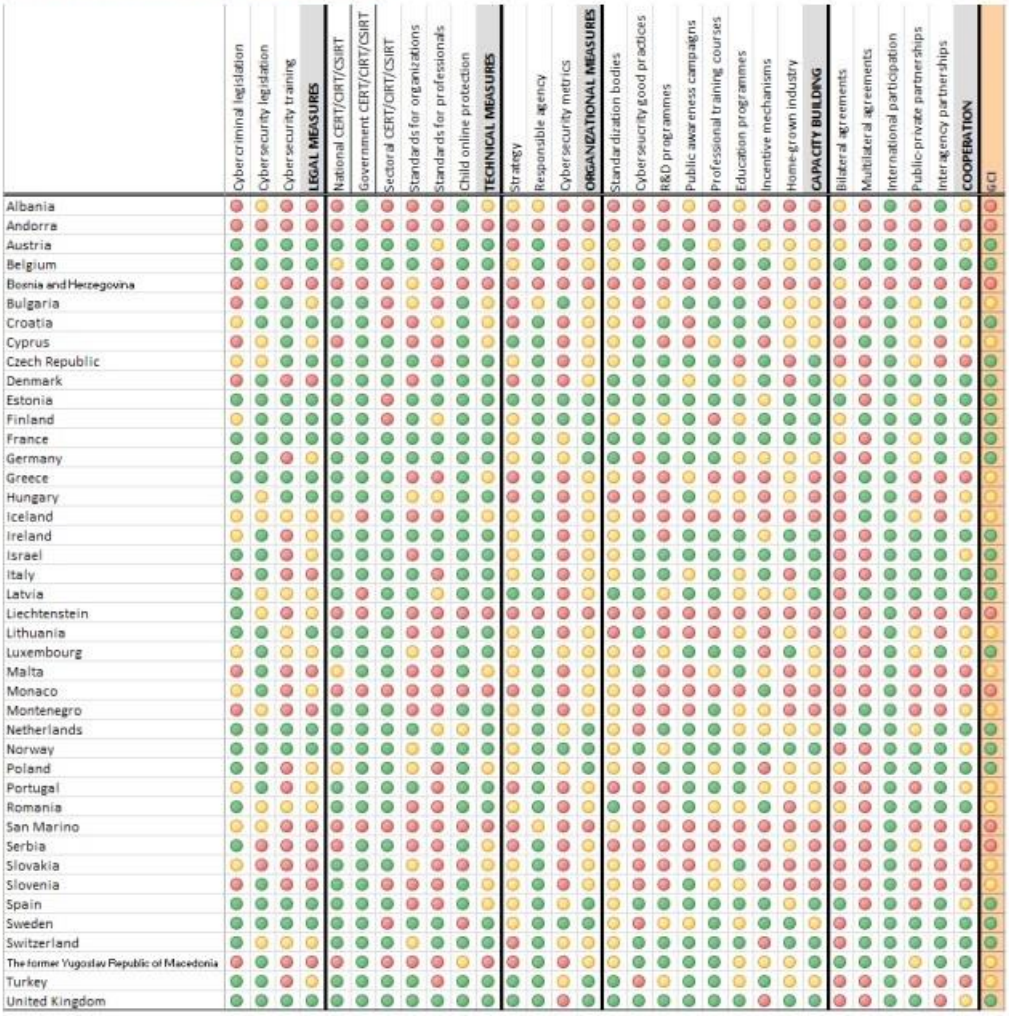
Kategórie a indikátory výkonnosti v rámci 5 základných pilierov

Pilier	**Kategória**	**Indikátory vstupujúce do hodnotenia**
Právny	Právo v oblasti počítačového zločinu	Hodnotenie čiastočnej implementácie: v práve je počítačový zločin len povsúvaný ako doplnenie v existujúcich zákonoch, hodnotenie úplnej implementácie je pri prijatí komplexných zákonov zaoberajúcich sa počítačovým zločinom.
	Regulácia v oblasti počítačového zločinu	Ochrana dát, oznamovanie narušenia, požiadavky na štandardizáciu a certifikáciu sú súčasťou právneho systému.
	Príprava profesionálov v oblasti počítačového zločinu	Profesionáli v oblasti vynucovania práva (policajti, sudcovia, právnici a i.) sú trénovaní v oblasti kybernetickej bezpečnosti.
Technický	Národný CERT/CIRT/CSIRT	Existencia a zákonné vynucovanie existencie týchto inštitúcií
	Vládny CERT/CIRT/CSIRT	
	Sektorový	
	Štandardy a implementačné rámce pre organizácie v oblasti kybernetickej bezpečnosti	Existencia vládou vyžadovaného štandardizovaného rámca pre kybernetickú bezpečnosť vo verejnom sektore alebo implementácia medzinárodne uznávaného

		rámca a jeho vynucovanie dodržiavania vo verejnom sektore a kritickej infraštruktúre aj keď je v súkromnom vlastníctve.
	Štandardy a certifikačné schémy pre profesionálov v oblasti kybernetickej bezpečnosti	Existencia vládou vyžadovaného štandardizovaného rámca pre certifikáciu profesionálov v oblasti KB vo verejnom sektore alebo implementácia medzinárodne uznávaného rámca a jeho vynucovanie dodržiavania voči profesionálom pracujúcim vo verejnom sektore a kritickej infraštruktúre. Hodnotí sa vytvorený národný rámec certifikácie a akreditácie pracovníkov vo verejnom sektore.
	Online ochrana detí	Existencia národného orgánu pre online ochranu práv detí.
Organizačný	Stratégia	Existencia stratégie, kompetencií pridelených orgánom a governance modelu v oblasti kybernetickej bezpečnosti. Politika má stanoviť jasné zodpovednosti za všetky aspekty kybernetickej bezpečnosti a nastaviť jasné smerovanie k ochrane práv občanov v oblasti KB vrátane podpory pre súkromný sektor.
	Zodpovedný orgán	Stanovenie zodpovedného orgánu na implementáciu stratégie.
	Metriky kybernetickej bezpečnosti	Zavedenie benchmarkingu a sledovania dosahovania očakávanej sektorovej bezpečnosti.
Budovanie kapacít KB	Orgán štandardizácie	Existencia národného orgánu na podporu štandardizácie v oblasti KB.
	Best practices	Hodnotí sa existujúci výskum a publikovanie v oblasti postupov najlepšej praxe (best practices) v KB, ktorá sú priamo previazané na úspech v oblasti KB.
	Vývoj a rozvojové projekty	Hodnotí sa existencia vývojových a rozvojových projektov v oblasti KB v súkromných, akademických, vládnych alebo nevládnych organizáciách. Hodnotí sa existencia národného orgánu, ktorý tieto projekty podporuje a monitoruje.
	Verejné kampane na budovanie povedomia	Hodnotí sa vykonávanie kampaní na budovanie verejného bezpečnostného povedomia v oblasti KB.
	Školenia a tréning profesionálov	Hodnotí sa existencia tréningových a školiacich programov.
	Národné vzdelávacie programy a akademické curricula	Hodnotí sa podpora vzdelávania na národnej úrovni pri získavaní zručností v školskom vzdelávacom systéme od základných po vysoké školy vrátane postgraduálneho vzdelávania.
	Mechanizmy podpory	Hodnotí sa existencia národných podporných mechanizmov na rozvoj kapacít v oblasti KB

		vo forme daňových úľav, grantov, pôžičiek alebo finančných stimulov.
	Domáci priemysel v oblasti KB	Vznik domáceho priemyslu v oblasti KB je pozitívnym dôsledkom účinného dvíhania povedomia, ktorý podporuje rozvoj trhu s produktami v oblasti KB.
Kooperácie	Bilaterálne zmluvy	Hodnotí sa existencia a záväznosť zmlúv.
	Multilaterálne zmluvy	
	Účasť na medzinárodných fórach	Hodnotí sa aktívna participácia a podpora účasti na národnej úrovni.
	Public-Private partnerstvá	Hodnotí sa zdieľanie vedomostí, profesionálov a zdrojov pri spolupráci ako aj počty partnerstiev.
	Partnerstvá medzi agentúrami	Hodnotia sa oficiálne partnerstvá medzi verejnými orgánmi a inštitúciami v rámci štátu.

Figure 6.6.2: Europe region scorecard



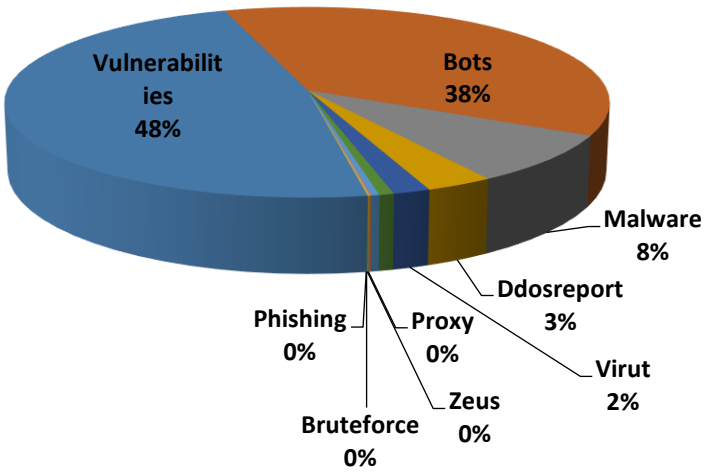
6.4 Poznatky CSIRT.SK o stave KIB vo verejnej správe (r. 2016)

CSIRT.SK rieši informačno-bezpečnostné incidenty v orgánoch verejnej správy a vykonáva aj penetračné testovanie (hľadanie zraniteľností, ktoré umožňujú útočníkovi preniknúť do systému).

Zistenia CSIRT.SK sú postavené na riešení bezpečnostných incidentov vo verejnej správe a IP adresnom priestore SR[22], informácií získaných z tzv. „threat intelligence" platformy implementovanej CSIRT.SK[23], vykonaných bezpečnostných auditoch organizácií vo verejnej správe a vykonaných penetračných testov. CSIRT.SK až do schválenia zákona o kybernetickej bezpečnosti vykonáva činnosti vládnej a národnej jednotky typu CSIRT.

Stav informačnej bezpečnosti vo verejnej správe - štatistiky

Vo verejnej správe boli v roku 2016 na základe informácií z threat intelligence platformy CSIRT.SK identifikované nasledujúce incidenty:



Typ incidentu	Počet
Vulnerabilities	5 126
Bots	4 035
Malware	902
Ddosreport	343
Virut	188
Defacement	75
Malwareurl	40
Citadel	7
Proxy	7
Zeus	4
Bruteforce	2
Phishing	2
Celkom	**10 731**

Do verejnej správy sú zaradené všetky inštitúcie verejnej správy vrátane samosprávy a organizácií, ktoré na základe známych informácií patria do zriaďovateľskej pôsobnosti nejakej organizácií verejnej správy alebo samosprávy. Nakoľko niektoré organizácie verejnej správy nemali informácie o všetkých verejných IP adresách používaných nimi, alebo organizáciami v ich zriadovateľskej pôsobnosti, uvedený zoznam s najväčšou pravdepodobnosťou nie je kompletný. Súčasne uvedené informácie zahŕňajú iba informácie o detegovaných incidentoch prostredníctvom automatizovaných riešení. Problémom je to najmä pri škodlivom kóde, kde sú zaznamenané iba škodlivé kódy, ktoré kontaktujú známe kontrolné servery. Napriek tomu uvedené čísla čiastočne reprezentujú stav informačnej

[22] IP adresy pridelené subjektom v SR, webové portály a služby v rámci TLD domény .sk.

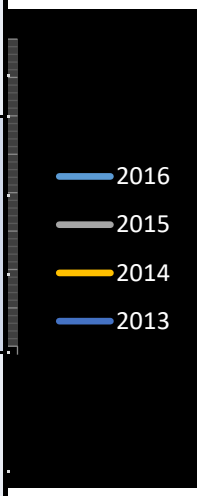
[23] Systém založený na systéme Malicious Domain Manager, ktorý zbiera a vyhodnocuje informácie z verejných zdrojov threat intelligence a informácie získané od zahraničných partnerov týkajúce sa detegovaných bezpečnostných incidentov najčastejšie na základe SinkHole serverov pre škodlivý kód.

bezpečnosti vo verejnej správe nakoľko sa jedná o počet unikátnych bezpečnostných incidentov, prípadne bezpečnostných incidentov, ktoré boli organizáciám viacnásobne nahlasované.

Typ útočníka	Predpokladané technické znalosti útočníka	Ciele útočníka
Aktivista/ hacktivista	Nízke až mierne pokročilé	•Zviditeľnenie sa v médiách, útoky typu defacement, DDoS •Krádeže údajov •Poškodenie dobrého mena SR alebo EU
Zločinci / zločinecké skupiny	Nízke až pokročilé	•Krádež a/alebo modifikácia údajov •Ovládnutie infraštruktúru s cieľom získať kontrolu •Finančný prospech
Národné štáty / hackerské skupiny	Vysoko pokročilé	•Diskreditácia SR a EU / Politické ciele •Krádež a/alebo modifikácia údajov •Ovládnutie infraštruktúry s cieľom získať kontrolu
Teroristické organizácie	Pokročilé až veľmi pokročilé	•Útoky na kritickú infraštruktúru s cieľom sabotáže •Krádež a/alebo modifikácia údajov

ácií
ručené
ných IP
anie IP adries
etračných

pečnostné
pečnostné



Jedným z najzávažnejších identifikovaných typov bezpečnostných incidentov je pokus o prienik, alebo prienik do informačných systémov. V rámci identifikovaných bezpečnostných incidentov bolo identifikovaných cca 10 percent[24] incidentov typu prienik, alebo pokus o prienik do informačných systémov.

Prehľad typov útočníkov a ich cieľov je uvedený v tabuľke č.1. Útočníci a útoky zaznamenané v SR sú zvýraznené červenou farbou.

Tabuľka 1Kybernetické útoky v SR

Stav informačnej bezpečnosti vo verejnej správe – bezpečnostné povedomie

Pre účely praktického overenia úrovne bezpečnostného povedomia zamestnancov štátnej správy CSIRT.SK v roku 2013 počas národného cvičenia na ochranu kritickej infraštruktúry SISE 2013 simuloval phishingový útok prostredníctvom emailu adresovaného jednotlivým rezortom. Text phishingového emailu bol pripravený na základe zaznamenaných útokov v SR aj v zahraničí a využíval viaceré psychologické prvky na dosiahnutie vyššej úspešnosti. Email pod zámienkou prístupu k lákavému obsahu (návrh finančného ohodnotenia zamestnancov) nabádal adresátov, aby navštívili stránku Úradu práce, ktorá však smerovala na zdanlivo podobný, avšak fiktívny Úrad práce. Následne

[24] Pozn. rok 2016, je potrebné prepočítať za predchádzajúce obdobie.

bolo od návštevníkov tejto stránky vyžadované ich meno a heslo do domény, resp. pracovného počítača. Ukázalo sa, že približne každý tretí adresát (31,32%) z celkového počtu navštívil podvodnú stránku a približne každý desiaty adresát emailu (10,04%) skutočne zadal svoje prihlasovacie údaje. Tieto hodnoty sú mimoriadne vysoké, najmä vzhľadom na to, že **pri skutočnom útoku by na úspešnú kompromitáciu celej organizácie stačil jeden používateľ**, ktorý by podvodnú stránku navštívil. Zadaním mena a hesla by útočníkom kompromitáciu iba zjednodušil, nie je to však nevyhnutne nutné pre úspešný útok.

Stav informačnej bezpečnosti vo verejnej správe – penetračné testy

Špecializovaný útvar CSIRT.SK DataCentra MF SR vykonal počas svojej existencie viac ako 150 interných a externých penetračných testov a retestov (v roku 2016 bolo vykonaných celkovo 55 penetračných testov z toho 33 testov a 22 retestov), počas ktorých simuloval správanie sa útočníkov a ich útok na konkrétne časti infraštruktúry a vybrané služby poskytované organizáciami verejnej správy.

Identifikované nedostatky v organizáciách verejnej správy možno rozdeliť najmä do nasledujúcich oblastí:

- **Nedostatočná alebo nesprávna bezpečnostná architektúra infraštruktúry**. Informačné systémy v mnohých organizáciách sa implementujú a integrujú do infraštruktúr ad-hoc, chýba bezpečnostné posúdenie vhodnosti zvoleného riešenia, alebo je iba formálne. V organizáciách pri návrhu infraštruktúry nie sú brané do úvahy bezpečnostné potreby organizácie [25] a preto v súčasnosti v mnohých organizáciách chýbajú základné prvky zabezpečenia infraštruktúr, sú nesprávne nasadené alebo nakonfigurované.
- **Nedostatky v prevadzkovej bezpečnosti.** Organizácie nemajú implementovaný manažment zmien a manažment záplat. Dôraz sa kladie na funkčnosť a používateľskú jednoduchosť riešenia aj za cenu nedostatočnej úrovne bezpečnosti. Administrátori v organizáciách verejnej správy (vrátane outsourcovaných kapacít) nemajú dostatočnú úroveň technických spôsobilostí na správu väčšieho množstva používaných technológií a pri správe systémov sú prijímané mnohé bezpečnostné kompromisy z dôvodu nedostatočnej znalosti spravovaných technológií. Súčasne na mnohých pozíciách správcov systémov, bezpečnostných špecialistov a manažérov informačnej bezpečnosti sa nachádzajú nekvalifikované a/alebo nedostatočne kvalifikované osoby.
- **Chýbajúce personálne kapacity.** V organizáciách nie sú dostupné interné kapacity na zabezpečenie infraštruktúry. V prípade externých kapacít chýba kontrola nad výkonom ich činnosti. Externé kapacity súčasne často minimalizujú svoju činnosť v prípadoch, že neexistujú interné kapacity ktoré technicky kontrolujú vykonávanie ich činnosti.
- **Nedostatočné bezpečnostné povedomie zamestnancov a administrátorov (vrátane administrátorov tretích strán).** Zamestnanci a administrátori často nemajú dostatočné vedomosti z oblasti kybernetickej bezpečnosti, nepoznajú riziká, príznaky útokov, neuvedomujú si závažnosť dopadov. Administrátori často nemajú dostatočné znalosti a skúsenosti so zabezpečovaním spravovaných systémov, najmä nepoznajú a nevyužívajú pokročilejšie bezpečnostné mechanizmy implementované vo viacerých v súčasnosti používaných systémoch.

[25] Analýza rizík je iba formálna alebo chýba úplne.

Pri obmedzených externých penetračných testoch[26] bolo pri viac ako 90 percent penetračných testoch identifikovaná aspoň jedná závažná[27] a/alebo kritická[28] zraniteľnosť. Zraniteľnosti z týchto penetračných testov je možné rozdeliť najmä do nasledujúcich kategórií :

- Zraniteľné webové servery
  - **SQL injection** (cca 10 percent)
  - XSS a nedostatočne ošetrené vstupy (cca 90 percent)
  - Command injection (cca 5 percent)
  - Neaktuálne verzie nainštalovaného softvéru so známymi zraniteľnosťami (cca 90 percent)
  - Iné závažné zraniteľnosti webových serverov a podkladovej infraštruktúry (cca 40 percent)
- Zraniteľnosti v súvislosti s autentifikáciou a zabezpečením dôvernosti/integrity/dostupnosti prenášaných údajov
  - Nedostatočne nakonfigurované SSL/TLS alebo jeho neprítomnosť (viac ako 90 percent)
  - Slabé heslá používateľov a administrátorov (viac ako 90 percent)
- Dostupné (a často aj zraniteľné) služby poskytované do siete Internet
  - Databázy (neaktuálne zraniteľné verzie)
  - Dostupné administračné rozhrania z prostredia Internetu
  - Mail (povolená enumerácia, povolené odosielanie mailov v mene organizácie)
  - VPN (často IPsec v agresívnom móde)

6.5 Procesný rámec COBIT-u a framework CSF

Pri analýzach potrieb, návrhu a implementácii riešení KIB je nevyhnutne použitie procesného rámca, v ktorom sú definované nutné minimálne procesy a aktivity, ich vstupy a výstupy rovnako ako pridelená zodpovednosť za ich realizáciu. V rámci procesného modelu je celosvetovo uznávaný procesný rámec v rámci COBIT[29] a v oblasti kybernetickej bezpečnosti vychádzame z uznávaného frameworku CSF.

CSF (Cybersecurity Framework) vznikol na základe nariadenia EO (Executive Order) 13636 z roku 2013 vydaného americkým prezidentom Obamom na zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry USA. CSF vyvinul NIST (National Institute of Standards and Technology) v spolupráci prevádzkovateľmi americkej národnej kritickej infraštruktúry a medzinárodnými partnermi avšak stal sa uznávaným rámcom na využívanie aj v iných spoločnostiach, nie len u prevádzkovateľov kritickej infraštruktúry, aj vďaka tomu, že poskytuje prístup na báze rizík s rýchlym dosahovaním výsledkov a jasnými krokmi na zvyšovanie zrelosti v oblasti kybernetickej bezpečnosti.

[26] S vylúčením útoku na celý perimeter organizácie pri testovaní iba konkrétnej služby, projektu alebo časti perimetra.

[27] Závažná zraniteľnosť je zneužiteľná zraniteľnosť, ktorej zneužitím je možné kompromitovať menšiu časť informačného systému (najčastejšie webový server, alebo nejaký konkrétny server alebo službu), narušiť dôvernosť, integritu alebo dostupnosť spracovávaných ukladaných, alebo prenášaných dát, alebo kompromitovať klienta tejto služby.

[28] Kritická zraniteľnosť je zneužiteľná zraniteľnosť, ktorej zneužitím je možné kompromitovať celý informačný systém, alebo infraštruktúru organizácie, alebo informačné systémy napojené na tento informačný systém.

[29] Control Objectives for Information and Related Technology, ISACA.

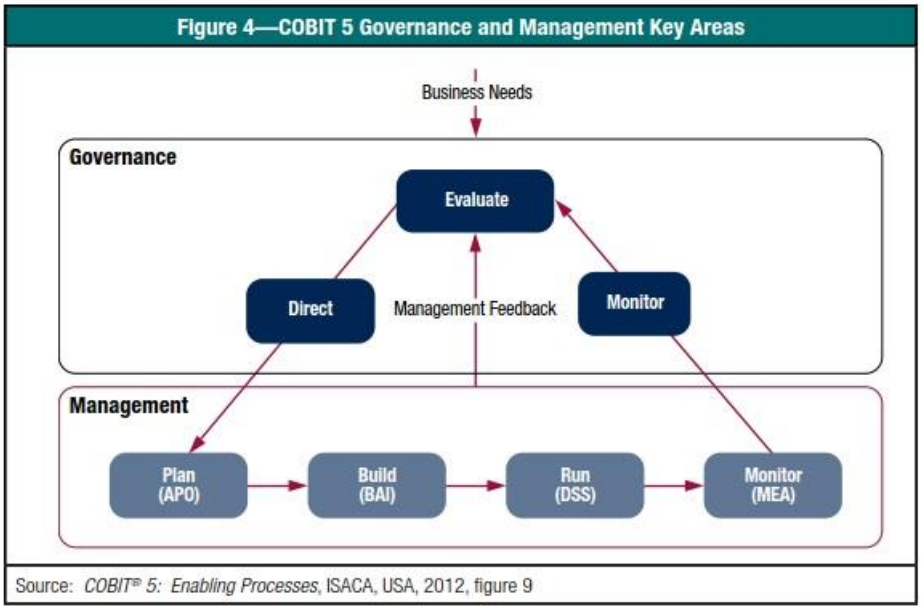
Keďže ISACA spolupracovala pri tvorbe CSF a zároveň tento rámec úzko nadväzuje na princípy governance a manažmentu, pri implementácii CSF sa využíva procesný model COBIT.

CSF poskytuje odkazy na zásadné opatrenia informačnej bezpečnosti, implementačný rámec COBITu ich pomáha aplikovať v rámci kaskády cieľov COBIT5. COBIT 5 je komplexným modelom, ktorý pomáha pri dosahovaní cieľov rámci governance a manažmentu IT (GEIT).

Framework COBIT 5 zásadne rozlišuje governance a manažment. Tieto dve úrovne zahŕňajú rôzne typy aktivít, vyžadujú rozličnú úroveň organizačnej štruktúry a slúžia odlišným cieľom.

COBIT5 rozlišuje tieto dve úrovne nasledovne:

- Governance—Governance zaisťuje potreby zainteresovaných strán, vyhodnocuje a dáva do rovnováhy podmienky a možnosti, v súlade s odsúhlasenými cieľmi, dáva usmernenia voči prioritizácii a pri rozhodovaní a monitoruje výkon a súlad voči odsúhlasenému smerovaniu a cieľom,
- Manažment – manažment plánuje, buduje, prevádzkuje a monitoruje aktivity v súlade so smerovaním danom na úrovni governance na dosiahnutie cieľov.



Procesy COBIT pokrývajú obe úrovne (governance aj manažment) a sú ďalej rozpracované do domén:

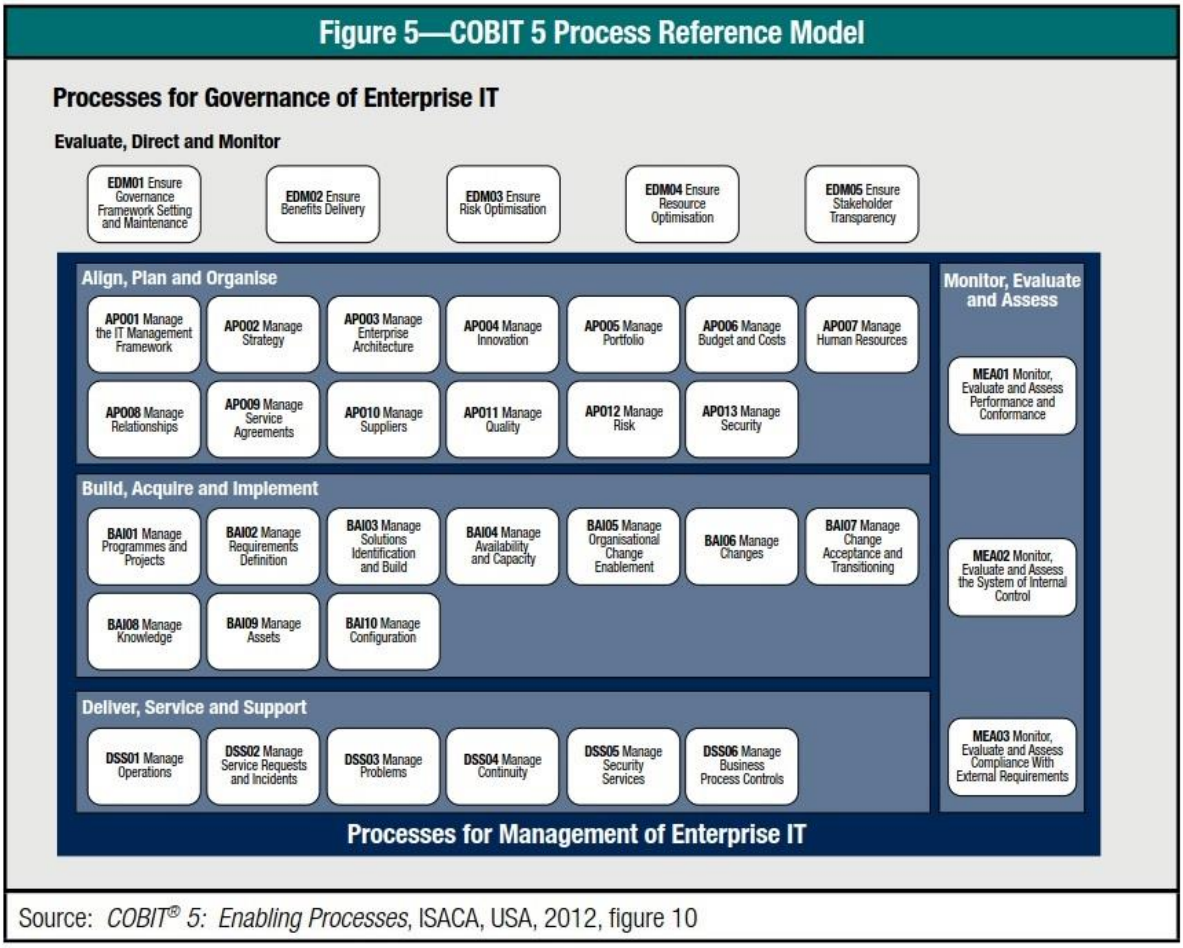
Governance: EDM (Evaluate, Direct, Monitor)

Manažment: APO (Allign, Plan, Organize),

BAI (Build, Acquire, Implement),

DSS (Deliver, Service, Support),

MEA (Monitor, Evaluate, Assess)



Source: *COBIT® 5: Enabling Processes*, ISACA, USA, 2012, figure 10

6.5.1 Postup implementácie

CSF poskytuje nielen rámec pre kybernetickú bezpečnosť ale aj základný návod[30] na jeho implementáciu a to v siedmych krokoch:

Krok 1: Prioritizuj a definuj rozsah - vyžaduje, že organizácie identifikuje rozsah a prioritizuje svoje ciele a priority najvyššej úrovne. Táto informácia umožní organizácii urobiť strategické rozhodnutia ohľadne rozsahu systémov a aktív, ktoré podporujú identifikované procesy

Krok 2: Orientuj sa – poskytuje organizácii príležitosť pre identifikáciu hrozieb, zraniteľností systémov identifikovaných v Kroku 1.

Krok 3: Vytvor súčasný profil – identifikuje požiadavku na definíciu súčasného stavu kybernetickej bezpečnosti organizácie

Krok 4: Vykonaj analýzu rizík – očakáva od organizácie vyhodnotenie rizík

Krok 5: Vytvor cieľový profil – umožňuje organizácii vytvoriť cieľový profil na báze analýzy rizík naprieč všetkými kategóriami CSF a subkategóriami popisujúc žiaduci cieľový výstup kybernetickej bezpečnosti

[30] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, February 12, 2014

Krok 6: Urči, analyzuj a prioritizuj rozdiely – organizácia vytvorí gap analýzu (analýzu rozdielov) na stanovenie príležitostí na zlepšenie súčasného stavu. Rozdiely sú identifikované pomocou porovnávania výstupov krokov 3 a 5 (súčasný a cieľový profil).

Krok 7: Implementuj akčný plán – po identifikácii rozdielov a ich prioritizácii sú vybrané nutné činnosti na ich vyriešenie a smerovanie k cieľovému stavu.

CSF popisuje päť kľúčových funkcií nasledovne (preklad uvádzame len pre lepšie pochopenie, na zachovanie prehľadnosti používame originálne označenia v ďalšom texte):

- Identify (Identifikuj) — vytvoriť v organizácii pochopenie s cieľom riadiť riziká pre systémy, aktíva, dáta a spôsobilosti. Pochopenie kontextu biznis procesov organizácie, zdrojov, ktoré podporujú kritické funkcie a súvis s rizikami kybernetickej bezpečnosti umožní sústredenie sa a prioritizáciu úsilia v súlade so stratégiou ošetrenia rizík a potrebami biznisu.
- Typickým výstupom v tejto kategórii sú: riadenie aktív, governance, hodnotenie rizík.
- Protect (chráň) — vytvoriť a implementovať primerané opatrenia na zaistenie dodávky kritických služieb. Funkcia Protect podporuje schopnosť eliminovať dopady kybernetického incidentu.
- Typickým výstupom v tejto kategórii sú Riadenie prístupov, školenia a povedomie, ochrana dát, procesy ochrany informácií, údržba.
- Detect (deteguj) — vytvoriť a implementovať primerané činnosti na identifikáciu výskytu kybernetického incidentu. Funkcia Detect umožňuje včasné odhalenie incidentu.
- Typickým výstupom v tejto kategórii sú anomálie a udalosti, kontinuálny monitoring bezpečnosti a procesy detekcie incidentov.
- Respond (reaguj) — vytvoriť a implementovať primerané činnosti v prípade detekcie kybernetického incidentu Funkcia Respond podporuje schopnosť eliminovať dopad potenciálneho incidentu

  Typickým výstupom v tejto kategórii sú plán odozvy, analýzy, eliminácie a zlepšenia.

- Recover (obnov) — vytvoriť a implementovať primerané činnosti na udržiavanie plánov na odolnosť a obnovu všetkých spôsobilostí služieb, ktoré boli zasiahnuté kybernetickým incidentom. Funkcia Recover podporuje včasný návrat k normálnej prevádzke a redukciu dopadov incidentu.
- Typickým výstupom v tejto kategórii sú plán obnovy a ich zlepšenia.

Figure 12—Framework Core Identifiers and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Information
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, USA, 2014, Table 1

Príloha č. 4

N á v r h

na zmenu a doplnenie Štatútu Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

Čl. I

Štatút Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh, schválený uznesením vlády Slovenskej republiky č. 364 z 30. 8. 2016 sa mení a dopĺňa takto:

1. V čl. 4 ods. 1 sa vypúšťajú slová „a nestáli“.

2. V čl. 4 sa vypúšťa odsek 2.
   Doterajšie odseky 3 až 11 sa označujú ako odseky 2 až 10.

3. V čl. 4 ods. 4 písm. g) sa slová „informatizácie spoločnosti“ nahrádzajú slovami „informačných technológií verejnej správy“.

4. V čl. 4 sa odsek 4 dopĺňa písmenami q) až u), ktoré znejú:
   „q) vedúci Úradu podpredsedu vlády SR pre investície a informatizáciu,

   r) štátny tajomník Ministerstva spravodlivosti Slovenskej republiky,

   s) štátny tajomník Ministerstva kultúry Slovenskej republiky,

   t) štátny tajomník Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky,

   u) zástupca Úradu na ochranu osobných údajov.“.

5. V čl. 4 sa vypúšťa odsek 5.
   Doterajšie odseky 6 až 10 sa označujú ako odseky 5 až 9.

Čl. II

Podľa tejto zmeny a doplnenia štatútu sa postupuje odo dňa jeho schválenia vládou.

Príloha č. 5

D o d a t o k č . 1

k

Rokovaciemu poriadku Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh

Čl. I

Rokovací poriadok Rady vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh sa mení a dopĺňa takto:

6. V čl. 4 ods. 3 sa vypúšťa veta „Nestáli členovia rady sú prizývaní len na zasadnutia rady, na ktorých sú prerokúvané materiály týkajúce sa otázok jednotného digitálneho trhu a ich hlasovacie právo sa vzťahuje len na materiály týkajúce sa otázok jednotného digitálneho trhu.“.

7. V čl. 5 ods. 5 sa vypúšťajú slová „oprávnených hlasovať v predmetnej veci“.

8. V čl. 6 ods. 5 sa vypúšťa veta „Nestáli členovia rady zasielajú svoje pripomienky len k časti zápisnice zo zasadnutia rady, ku ktorej majú hlasovacie právo podľa čl. 4 ods. 3 rokovacieho poriadku.“.

Čl. II

Tento dodatok nadobúda účinnosť dňom jeho schválenia radou.