**Národná koncepcia informatizácie~~a~~ verejnej správy**

**Strategická priorita 10 Kybernetická bezpečnosť**

verzia 2.1

Bratislava, 29. mája.2018

**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 nadrezortná informačná sieť

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

KIB kybernetická a informačná bezpečnosť

MISP Malware Information Sharing Platform (projekt NATO)

NASES Národná agentúra pre sieťové služby

NBÚ SR Národný bezpečnostný úrad

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

SANET Slovenská akademická sieť

SASIB Slovenská asociácia pre informačnú bezpečnosť

SR Slovenská republika

TLD top level domain

ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu

ÚPVS Ústredný portál verejnej správy

Obsah

1 [Úvod 5](#_Toc517357485)

[2 Ciele dokumentu 5](#_Toc517357487)

[3 Adresáti dokumentu 5](#_Toc517357488)

[4 Základné pojmy 6](#_Toc517357490)

[5 Súčasný stav v KIB 8](#_Toc517357525)

[5.1 Koncepcia a legislatíva EÚ v KIB 8](#_Toc517357526)

[5.2 KIB SR a ISVS 9](#_Toc517357528)

[5.2.1 Legislatívny rámec KIB v SR 9](#_Toc517357529)

[5.2.2 Kompetencie 11](#_Toc517357530)

[5.2.3 Koncepcie KIB a ich realizácia 11](#_Toc517357531)

[5.2.4 Hodnotenie stavu KIB SR podľa GSI 12](#_Toc517357533)

[5.2.5 Stav bezpečnosti ISVS podľa zistení CSIRT.SK 14](#_Toc517357534)

[5.2.6 Problémové oblasti z pohľadu bezpečnosti ISVS 15](#_Toc517357535)

[5.3 Zhrnutie stavu KIB v SR 15](#_Toc517357537)

[6 Navrhované riešenia 16](#_Toc517357538)

[6.1 Priority a princípy riešenia 16](#_Toc517357539)

[6.2 Koncepcia, legislatíva, kompetencie 17](#_Toc517357540)

[6.3 Riadenie a koordinácia zabezpečenia slovenského virtuálneho priestoru 17](#_Toc517357541)

[6.4 Zabezpečenie základnej úrovne ochrany virtuálneho priestoru VS 21](#_Toc517357543)

[6.5 Systematické zabezpečenie informačnej bezpečnosti vo verejnej správe 22](#_Toc517357544)

[6.5.1 Prevencia a riadenie KIB 22](#_Toc517357545)

[6.5.2 Reakcia na bezpečnostné incidenty 24](#_Toc517357546)

[6.5.3 Kontrolné mechanizmy a mechanizmy posúdenia bezpečnosti 25](#_Toc517357549)

[6.6 Budovanie odborných kapacít 26](#_Toc517357550)

[**6.7** **Vypracovanie metodického rámca pre riadenie KIB vo verejnej správe** 27](#_Toc517357572)

[**6.7.1** **Metodický rámec riadenia KIB vo verejnej správe** 27](#_Toc517357573)

[6.8 Budovanie bezpečnostného povedomia 30](#_Toc517357574)

[6.9 Vytvorenie rámca požiadaviek a postupov pre implementáciu a koordináciu požiadaviek GDPR regulácie vo verejnej správe 30](#_Toc517357575)

[6.10 Periodické vyhodnocovanie úrovne implementovaných bezpečnostných opatrení 31](#_Toc517357576)

[6.11 Zahraničná spolupráca 31](#_Toc517357577)

[6.12 Vytvorenie potrebného rámca na financovanie riadenia KIB v ISVS 32](#_Toc517357579)

[6.13 SWOT analýza navrhovaného riešenia 32](#_Toc517357581)

[7 Ďalšie kroky a odporúčané úlohy 34](#_Toc517357583)

[**7.1** **Organizačno-kompetenčné zabezpečenie riadenia KIB vo verejnej správe** 34](#_Toc517357584)

[**7.2** **Návrh potrebných krokov ÚPVII pre zlepšenie situácie v KIB ISVS v krátkodobom horizonte** 36](#_Toc517357585)

[**7.3** **Vytvorenie štandardných / referenčných postup v oblasti KIB pre ISVS** 38](#_Toc517357586)

[7.4 Vzdelávanie v KIB 40](#_Toc517357588)

[7.4.1 Zvyšovanie bezpečnostného povedomia pre občanov 42](#_Toc517357589)

[8 Prílohy 43](#_Toc517357590)

[8.1 Prehľad najdôležitejších dokumentov KIB SR 43](#_Toc517357592)

[8.2 Aktuálny zoznam zákonov a vykonávacích predpisov relevantných pre KIB ISVS 43](#_Toc517357593)

[8.3 Hodnotenie Slovenskej republiky na základe ITU indexu 44](#_Toc517357594)

[8.4 Poznatky CSIRT.SK o stave KIB vo verejnej správe (r. 2016) 48](#_Toc517357595)

[8.5 Procesný rámec COBIT-u a framework CSF 52](#_Toc517357596)

[8.5.1 Postup implementácie 54](#_Toc517357598)

# Úvod

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.

# Ciele dokumentu

Tento dokument sa sústreďuje na KIB 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 slovenského virtuálneho priestoru vo všeobecnosti a ISVS zvlášť.

Zaistenie dostatočnej úrovne KIB ISVS nie je možné bez toho, aby nebolo zabezpečené prostredie, v ktorom ISVS pôsobia. Tento dokument veľmi stručne popíše aj požiadavky/predpoklady na bezpečnostné okolie/prostredie ISVS. Dokument menovite

 vymedzí rozsah problémov KIB, ktoré bude potrebné riešiť na úrovni štátu;

 špecifikuje, čo je potrebné zaistiť v záujme zabezpečenia ISVS a úloh vyplývajúcich z NKIVS; t. j. stanoví ciele v oblasti KIB pre verejnú správu;

 opíše aktuálny stav KIB v ISVS a navrhne postupnosť krokov potrebných na naplnenie stanovených cieľov

stručne rozoberie existujúcu relevantnú legislatívu vyplývajúcu z postavenia SR v EÚ, vrátane aktuálnych materiálov, o ktoré by sa bolo možné oprieť,

 stručne popíše existujúce kompetencie,

 navrhne konkrétné úlohy a ďalšie kroky.

# Adresáti dokumentu

Dokument je odporúčaním ÚPVII a je určený šiestim kategóriám ľudí, ktorí požívajú, 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 štátnych inštitúcií 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 štátnych inštitúcií, ktoré prevádzkujú ISVS má dokument vysvetliť význam zabezpečenia IB a KB systémov v pôsobnosti organizácie, ktorú riadia, povinnosti ktoré im vyplývajú z legislatívy a rámcovo čo pre to musia robiť;

pracovníkom štátnych inštitúcií, 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.

# 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]](#footnote-2). 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.

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]](#footnote-3) 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 1. ideálny stav systému, organizácie, keď IKT fungujú bez narušenia a je zaručená dôvernosť, integrita, autentickosť a dostupnosť údajov, resp. služieb; 2. činnosť zameraná na dosiahnutie a udržanie požadovaného stavu IKT, 3. 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 forme. Široké chápanie kybernetickej bezpečnosti je konzistentnejšie, ale na zaistenie bezpečnosti systému/organizácie je potrebné chrániť aj netechnické a nemateriálne aktíva organizácie. Kybernetická bezpečnosť (v úzkom aj širokom zmysle) je podoblasťou informačnej bezpečnosti, obr. 1.



**Obr. 1. Vzťahy medzi informačnou a kybernetickou bezpečnosťou a inými oblasťami bezpečnosti[[3]](#footnote-4)**

# Súčasný stav v KIB

KIB je spoločenským problémom aj v globálnom meradle. Okrem objektívnych problémov spôsobených charakterom digitálnych IKT a spôsobom ich používania[[4]](#footnote-5), dramaticky stúpa rozsah a závažnosť cielených útokov na IKT a údaje, ktoré sa v nich spracovávajú. Podľa najnovšej Správy EÚ[[5]](#footnote-6) sa za necelých 5 rokov (2013-2017) zvýšil ekonomický dopad kybernetickej kriminality 5-násobne 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.

## Koncepcia a legislatíva EÚ v KIB

EÚ sa dlhodobo zaoberá KIB. V tomto dokumente nie je priestor na rozoberanie aktivít EÚ, preto uvádzame len najdôležitejšie legislatívne a koncepčné dokumenty EÚ týkajúce sa KIB[[6]](#footnote-7), 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
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.

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 najbližsom čase.

## 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. Technickou časťou okolia ISVS[[7]](#footnote-8) je slovenský kybernetický priestor (resp. globálny kybernetický priestor).

S výnimkou malého počtu izolovaných systémov sú takmer všetky ISVS pripojené na Govnet a teda pripojené na Internet buď prostredníctvom Govnet, alebo priamo.

### 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.. Ďalšími osobitnými predpismi, ktoré upravujú pôsobnosť vo vzťahu ku KIB** sú:

**Zákon č. 215/2004 Z. z.  o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov** - 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. 18/2018 Z. z. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Úrad na ochranu osobných údajov SR),** ktorýupravuje 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. s účinnosťou od 25.05.2018.

**Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov (Ministerstvo vnútra SR)** upravujeorganizáciu 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. 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. 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.

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

**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. 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 o.i. identifikáciu osôb a autentifikáciu osôb vo virtuálnom priestore.

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

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

**Výnos MVSR č. 525/2011 Z. z.** **o štandardoch pre elektronické informačné systémy na správu registratúry.**

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

Pre ISVS je najdôležitejší

**Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (MF SR, následne UPVII),** ktorý okrem iného upravuje práva a povinnosti povinných osôb v oblasti vytvárania, prevádzkovania, využívania a rozvoja informačných systémov verejnej správy, základné podmienky na zabezpečenie integrovateľnosti a bezpečnosti informačných systémov verejnej správy.

Podrobné bezpečnostné požiadavky na ISVS ustanovuje

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

V súčasnosti sa na ÚPVII pripravuje **Zákon o  informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov**, ktorý má nahradiť Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy. Pripravovaný zákon obsahuje aj ustanovenia relevantné pre bezpečnosť ISVS. Keďže tento zákon ešte nebol schválený, nemožno jeho ustanovenia zohľadňovať pri tvorbe tohto dokumentu ako záväzné.

### 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, elektonický podpis, osobné údaje, počítačová kriminalita) alebo po type systémov (ISVS, kritická infraštruktúra, telekomunikačné siete). Toto rozdelenie kompetencií sa utváralo historicky, postačovalo na riešenie bezpečnosti v špecifických oblastiach, ale nepostačuje na zaistenie bezpečnosti celého kybernetického priestoru SR, pretože

1. nepokrýva celý priestor,
2. nerieši úlohy, ktoré presahujú rámec jednej oblasti (vzdelávanie, výskum, štandardizácia, bezpečnosť nových technológií,...)
3. chýba koordinácia čiastkových aktivít,
4. nereflektuje nové globálne hrozby (sofistikovaný kybernetický zločin, globálne útoky na kybernetický priestor), resp. neumožňuje na ne dostatočne účinne reagovať.

V roku 2018 bol prijatý zákon, ktorý niektoré povinnosti zainteresovaných subjektov v oblasti kybernetickej oblasti explicitne špecifikoval. V súčasnosti NBÚ vykonáva činnosti potrebné na zabezpečenie slovenského kybernetického priestoru. Avšak ani tento zákon problematiku nerieši komplexne a primárne sa sústredí na kompetenčné a organizačné zabezpečenie riešenia bezpečnostných incidentov a implementáciu smernice NIS do slovenskej legislatívy.

V rámci zabezpečenia KIB UPVII v súlade so zákonom o kybernetickej bezpečnosti[[8]](#footnote-9) delimitoval vládnu jednotku CSIRT.sk a ďalej vyvíja aktivity na systematické zabezpečenie organizácií verejnej správy z pohľadu KIB.

### 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[[9]](#footnote-10) a Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020[[10]](#footnote-11). Obe koncepcie sa zhodli na rovnakých najdôležitejších prioritách.

MF SR, ktoré do roku 2015 riadilo a koordinovalo bezpečnosť ISVS[[11]](#footnote-12) 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), systematicky budovalo terminológiu informačnej bezpečnosti a pripravilo návrh zákona o informačnej bezpečnosti.

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[[12]](#footnote-13), NBÚ v roku 2016 zriadil Komisiu pre kybernetickú bezpečnosť.

Väčšina úloh, ktoré boli identifikované v koncepcii Kybernetickej bezpečnosti resp. v Akčnom pláne ku koncepcii kybernetickej bezpečnosti sú aj v roku 2018 nesplnené. 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 SASIB, 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.

### 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 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.

**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[[13]](#footnote-14), 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 |
| Dánsko | 0,617 | 34 | 18 |
| Česká republika | 0,609 | 35 | 19 |
|  |  |  |  |
| Slovensko | 0,362 | 81 | 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. V súčasnosti nám nie je známy index okrem GSI, ktorý by z hľadiska overovania informácií, metodiky spracovania a komplexnosti bol reprezentatívny. GSI je považovaný za referenčný index pri posudzovaní vyspelosti krajiny z hľadiska kybernetickej bezpečnosti.

Ani v rámci indexu GSI nedochádza ku komplexnému auditu stavu kybernetickej bezpečnosti v krajinách, v súčasnosti však z hľadiska komplexnosti a hĺbky analýzy je GSI najreprezentatívnejší index na porovnanie úrovne krajín z pohľadu kybernetickej bezpečnosti.

### 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[[14]](#footnote-15), súborné informácie o stave zabezpečenia ISVS chýbajú. Istý obraz o stave bezpečnosti ISVS dávajú výsledky CSIRT.SK[[15]](#footnote-16).

Špecializovaný útvar CSIRT.SK DataCentra MF SR je jednotka pre riešenie informačno-bezpečnostných incidentov, ktorá v súčasnosti vykonáva činnosti národnej jednotky CSIRT. CSIRT.SK rieši informačno-bezpečnostné incidenty v orgánoch verejnej správy 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[[16]](#footnote-17), informácií získaných z threat intelligence platformy implementovanej CSIRT.SK[[17]](#footnote-18), 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.

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 (!).

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. V prípade komplexných útokov  je pravdepodobné, že pokročilý útočník by mohol bez väčších problémov kompromitovať väčšinu organizácií verejnej správy.

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

### Problémové oblasti z pohľadu bezpečnosti ISVS

Kľúčovým problémom KIB je nedostatok kvalifikovaných odborníkov. Štát potrebuje špecialistov na informačnú/kybernetickú bezpečnosť nasledujúceho zamerania:

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.

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

## 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, podľa aktivít, ktoré vyvíjajú orgány zodpovedné za jednotlivé úlohy sa prevažná väčšina stanovených úloh ešte ani nezačala plniť.

**Legislatíva a kompetencie**. Vyvíjali sa historicky a málo koordinovane. Pokrývajú čiastkové oblasti kybernetického priestoru (podľa typu informácie, významu systémov, typu systémov), ale chýba jednotiaci zákon a štátny orgán, ktorý by KIB reálne koordinoval. NBÚ SR sa zaoberalo len vybranými aspektami kybernetickej bezpečnosti a na plnenie úloh v potrebnom rozsahu nemá potrebné odborné kapacity a kompetencie. Zákon o kybernetickej bezpečnosti je zameraný len na implementáciu smernice NIS[[18]](#footnote-19) a nerieši problémy informačnej bezpečnosti, špecifikované legistatívnym zámerom zákona o informačnej bezpečnosti.

**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.

# Navrhované riešenia

Stav KIB v SR je neuspokojivý a za takýchto podmienok (legislatíva, odborné kapacity, zdroje, úroveň bezpečnostného povedomia) štát nedokáže zabezpečiť adekvátnu ochranu svojho virtuálneho priestoru a teda ani 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 a bezpečnosti 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.

## Priority a princípy riešenia

Kybernetická bezpečnosť je jednou z priorít NKIVS a aj Operačný program integrovanej infraštruktúry obsahuje špecifický cieľ 7.9 Zvýšenie kybernetickej bezpečnosti v spoločnosti. Oba dokumenty sa odvolávajú 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 KIB by podľa NKIVS mali byť postavené na nasledovných princípoch:

štandardizácia riešení, založená na klasifikácii informácií a systémov,

stanovenie povinných minimálnych požiadaviek na ochranu systémov, (z dôvodu efektívnosti investícií, ako aj kvôli minimalizácii obmedzení vyplývajúcich z nasadených bezpečnostných opatrení),

stanovenie povinných minimálnych požiadaviek na riadenie informačnej bezpečnosti v organizáciách a na centrálnej úrovni

vybudovanie efektívneho systému na riešenie bezpečnostných incidentov, ich identifikáciu a systematické riešenie

dôsledné zamietnutie princípu „security by obscurity“, utajené a neprístupné budú iba nevyhnutné záležitosti,

systematická podpora používateľov pri bezpečnom používaní elektronických služieb,

dôsledne riešenie rizík prameniacich zo zdieľanej zodpovednosti za prevádzku integrovaného informačného systému verejnej správy

systematické ohodnocovanie dodržiavania povinností zo strany povinných osôb

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.“

## Koncepcia, legislatíva, kompetencie

V súčasnosti je legislatívou *lex generalis*  pre oblasť KIB v slovenskej legislatíve z**ákon č. 69/2018 Z. z. o kybernetickej bezpečnosti**. a pripravuje sa **zákon o výkone správy v oblasti informačných technológií.** Pripravovaný zákon o  informačných technológiách verejnej správy je zameraný len na IKT v pôsobnosti orgánov verejnej správy a jeho cieľom je definovať kompetencie ohľadne vedenia a riadenia bezpečnosti ISVS (pracovná skupina a aj tento dokument predpokladá, že kompetentným pre túto pre oblasť ISVS bude ÚPVII).

V dlhšom časovom horizonte bude potrebné analyzovať

Povinnosti v KIB, ktoré pre SR vyplývajú z právnych aktov EÚ,

Zákony a podzákonné normy SR, týkajúce sa KIB (ISVS a celého virtuálneho priestoru SR) a identifikovať nezrovnalosti, duplicity a iné nedostatky a navrhnúť ich zosúladenie;

Trvale bude potrebné systematicky sledovať legislatívu EÚ a udržiavať slovenskú legislatívu KIB konzistentnú a v súlade s európskou legislatívou.

## Riadenie a koordinácia zabezpečenia slovenského virtuálneho priestoru

Základným dôvodom nedostatočnej úrovne KIB ISVS je absencia centrálnej autority v tejto oblasti, ktorá by mala dostatočné právomoci pre presadzovanie strategických zámerov v tejto oblasti.

Súčasne s ralizáciou 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 vo verejnej správe a k tomu korešpondujúci inštitucionálny rámec.

Za týmto cieľom je potrebné vytvoriť organizáciu (Sekcia,/Odbor na ÚPVII), ktorá by metodicky zastrešovala riadenie KIB naprieč celou verejnou správou – pracovný názov: **Centrum pre kybernetickú a informačnú bezpečnosť**.

Na zaistenie ochrany a obrany slovenského virtuálneho priestoru je potrebné zaistiť súčinnosť štátnych orgánov, súkromného a akademického sektora a verejnosti čo pravdepodobne môže zabezpečiť len Vláda SR. Výkon rozsiahlej operatívy v oblasti KIB bude zabezpečovať (koordinovať, riadiť a vykonávať) ÚPVII, ktorý na výkon tejto činnosti zriadi hore uvedenú sekciu KIB. Toto riešenie umožní centrálne riadiť KIB v organizácií, efektívne riešiť bezpečnostné problémy, identifikovať bezpečnostné incidenty a efektívne ohodnocovať dodržiavanie legislatívnych požiadaviek, ako aj adekvátnu úroveň bezpečnosti ISVS.

**Vytvorenie centrálneho orgánu pre strategické riadenie KIB vo verejnej správe**

***Základné úlohy centrálneho orgánu:***

***Riadenie KIB vo verejnej správe***

Vytvorenie a presadzovanie stratégie KIB pre verejnú správu

Zavedenie jednotného, záväzného rámca bezpečnostných opatrení

Strategické vyhodnocovanie a reportovanie stavu kybernetickej bezpečnosti

Centralizovaná koordinácia bezpečnostných opatrení a ich optimalizácia

Šírenie osvety a zvyšovanie bezpečnostného povedomia

Komunikácia so zúčastnenými stranami

Vytváranie globálnej bezpečnostnej architektúry služieb e-Governmentu

Spolupráca s akademickou obcou, odbornou verejnosťou a profesijnými združeniami

Komunikácie so zahraničnými partnerskými organizáciami.

Plánovanie prostriedkov na rozvoj kybernetickej bezpečnosti

Predkladanie návrhov na legislatívne zmeny v oblasti kybernetickej bezpečnosti

Definovanie štandardov vo verejnej správe v oblasti KIB

Vytváranie inventáru aktív vo verejnej správe

Vytváranie analýzy rizík na národnej úrovni z pohľadu ISVS

Ohodnocovanie úrovne bezpečnosti ISVS

***Riešenie bezpečnostných incidentov a špecializované činnnosti***

Reakcia na bezpečnostné incidenty

Proaktívne služby na predchádzanie bezpečnostných incidentov

 Technologický dozor

 Vydávanie oznámení a varovaní

 Ohodnocovanie zraniteľností

 Bezpečnostné audity

 Penetračné testy

 Hardening infraštruktúr

 Tvorba postupov na riešenie bezpečnostných incidentov

 Bezpečnostné konzultácie

Reaktívne služby na systematické riešenie bezpečnostných incidnetov

 Riešenie bezpečnostných incidentov

 Vykonávanie forenzných analýz

 Analýza škodlivého kódu

 Analytické a  podporné činnosti pri riešení bezpečnostných incidentov

***Vykonávanie bezpečnostného dohľadu nad vybranými IS VS***

Služby SOC pre vybrané informačné systémy a infraštruktúry

Vytvorenie centrálneho orgánu je možné v rámci súčasnej a navrhovanej legislatívy bez potreby zmien.

Veľmi dôležitým poslaním tejto organizácie by mala byť aj postupná identifikácia tých aktivít a činností v procesoch riadenia KIB, ktoré je možné prevádzkovať pre viacero organizácií a inštitúcií spoločne, čím by bolo umožnené veľmi významné šetrenie nákladov, a taktiež dostupnosť aktivít a služieb pre organizácie, kde by to nebolo možné, alebo efektívne zrealizovať z finančných dôvodov (napr. zdieľanie monitorovacích centier tzv. SOC, centrálne bezpečnostné vzdelávanie, zálohovanie a pod.). Niektoré z uvedených aktivít je možné zrealizovať už v súčasnej dobe, avšak až po získaní celkového obrazu o stave KIB vo verejnej správe bude možné navrhnúť ďalšie optimalizácie opatrení.

Pre efektívny proces koordinácie KIB bude musieť byť vytvorený aj efektívny spôsob presadzovania bezpečnostných opatrení vo verejnej správe. Sankcionovanie formou finančných sankcií, nie je možné považovať za efektívny spôsob, ktorý sa v praxi neosvedčil. Ako účinné a logické sa napríklad javí podmienenie, alebo obmedzenie financovania projektov v prípade, že prostredie, do ktorého majú byť informačné systémy nasadené nie je bezpečné t.j. bezpečnostné opatrenia sú na neadekvátne nízkej úrovni.

Vzhľadom na veľmi blízku problematiku a pre zachovania efektívnosti vynaložených zdrojov by uvedená organizácia mala metodicky pokrývať aj koordináciu KIB v oblasti kritickej infraštruktúry. Výhradne sa však jedná iba o koordináciu KIB pri jednotlivých prvkoch kritickej infraštruktúry, čím sa nebude zasahovať do kompetencií ostatných orgánov vykonávajúcich správu kritickej infraštruktúry. Naopak, bude im poskytnutá odborná podpora pre výkon ich právomocí. Budovanie ďalších inštitúcií, ktoré by v podstate plnili veľmi podobné, ak nie rovnaké úlohy (aj keď s menšími právomocami) sa v tejto oblasti javí ako neefektívne a to aj vzhľadom na potrebu personálnych kapacít (je výhodnejšie mať odborníkov sústredených v jednej organizácii). Taktiež chýba prvok centrálneho vyhodnocovania KIB v kritickej infraštruktúre na celonárodnej úrovni. Okrem vyššie uvedeného je problematika KIB prvkov kritickej infraštruktúry vo veľkej miere rovnaká (t.j. rovnaké hrozby, rovnaké protiopatrenia). Rozdiely sú v špecifikách KIB pri priemyselných systémoch (ICS – Industrial Control Systems), t.j. informačných systémoch, ktoré riadia priemyselné procesy.

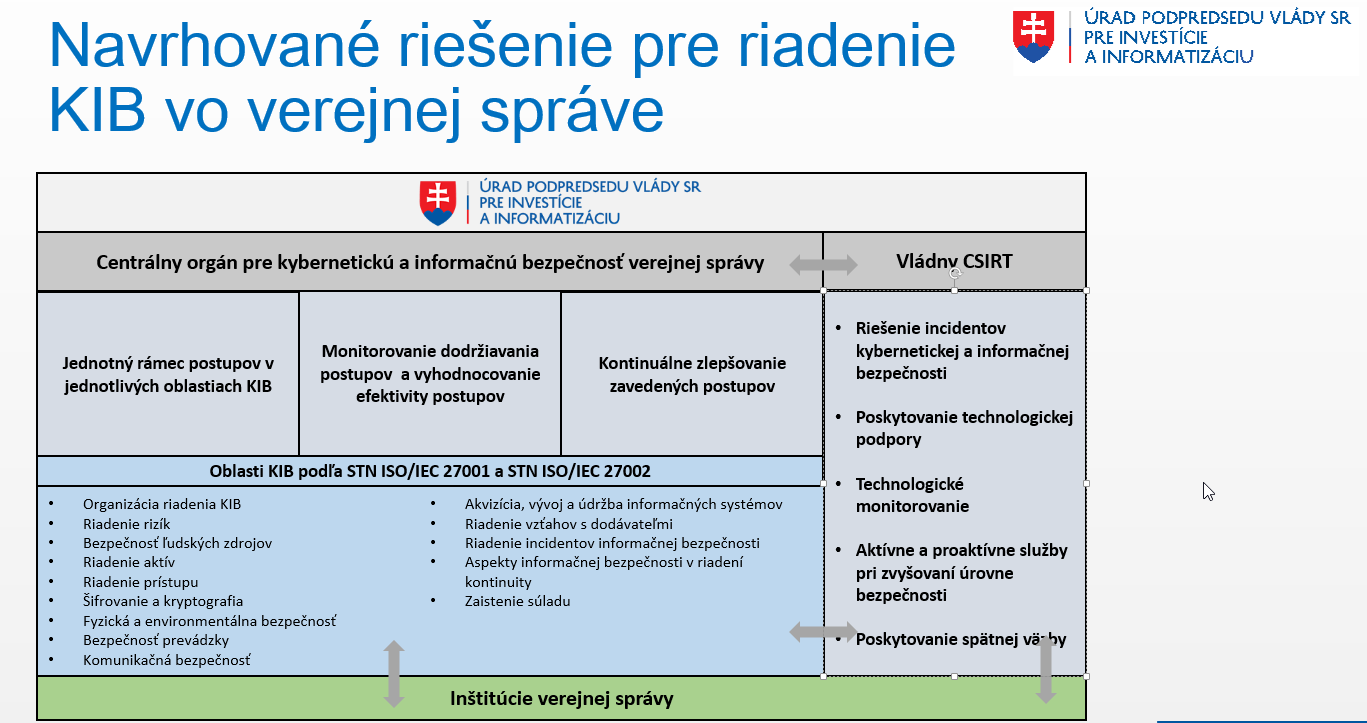


Figure Schéma fungovania Centra pre kybernetickú a informačnú bezpečnosť vo verejnej správe

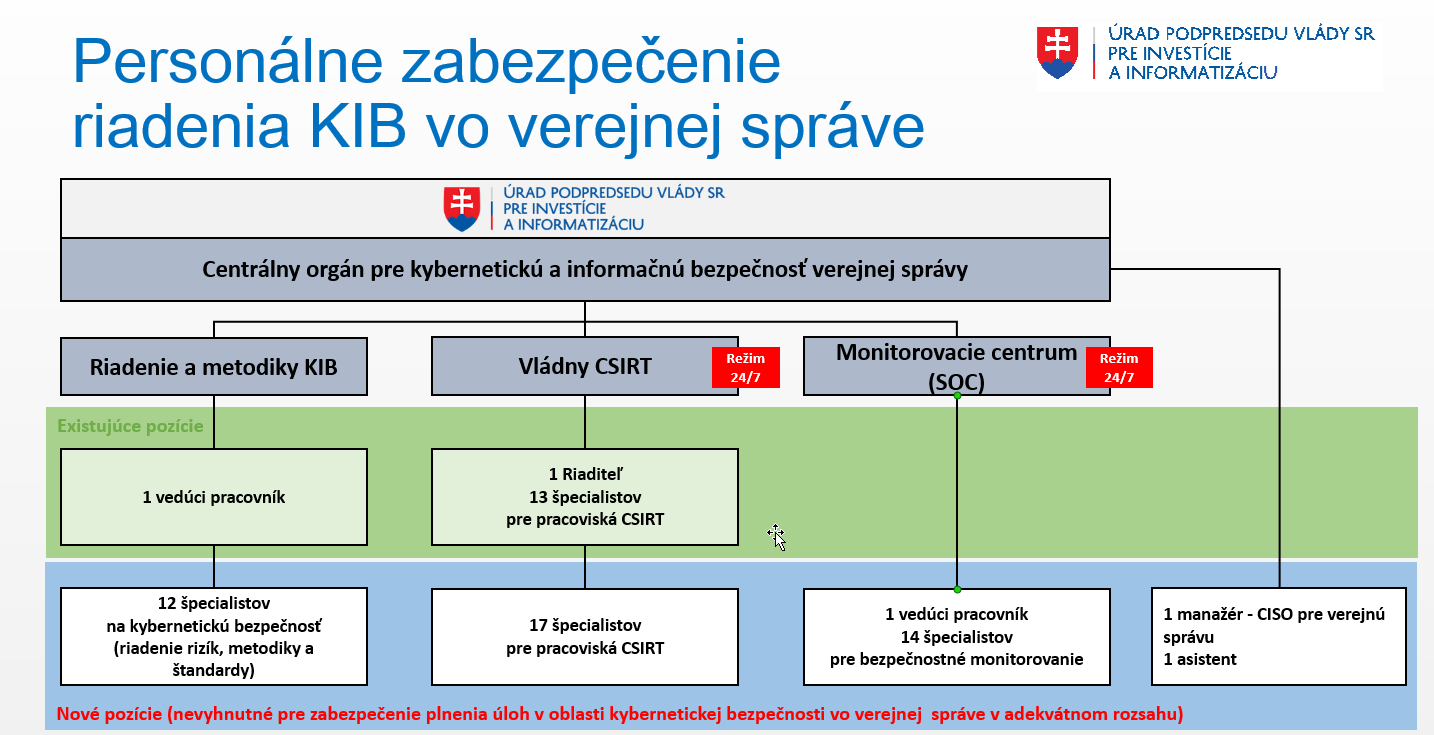


Figure Personálne zabezpečenie Centra pre kybernetickú a informačnú bezpečnosť vo verejnej správe

Vzhľadom na stav kapacít uvedených vyššie, je predpoklad, že ÚPVII popri sekcii KIB bude potrebovať zriadiť aj odborný koordinačno-koncepčno-výkonný orgán[[19]](#footnote-20) (pracovný názov – Komisia pre KIB) so zastúpením relevantných strán (štátne orgány, akademický sektor, súkromná sféra), ktorý by[[20]](#footnote-21)

mal prehľad o stave KIB v SR (spracovávanie dostupných informácií, časom vypracovanie metodiky na získavanie relevantných informácií a formu reportingu vedeniu ÚPVII)

 poskytoval odborné stanoviská pre Vládu SR (analógia vzťahu ENISA a Európskej komisie)

sledoval projekty a iné aktivity EÚ (v minulosti napr. FIDIS, epSOS, STORK; príprava direktív a nariadení, činnosť odborných komisií pri orgánoch EÚ a pod.), zastúpenie SR v odborných orgánoch EÚ,

rozvíjal/inicioval/podporoval odbornú činnosť v oblasti informačnej bezpečnosti zameranú na riešenie aktuálnych a perspektívnych problémov,

 zosúladil[[21]](#footnote-22) existujúcu legislatívu, sledoval konzistentnosť pripravovaných zákonov a podzákonných noriem, budoval konzistentnú terminológiu,

Vykonával pravidelnú analýzu stavu KIB vo verejnej správe, navrhoval strategické riešenia identifikovaných bezpečnostných problémov

posudzoval projekty a aktivity celoslovenského rozsahu zamerané na KIB.

Komisia pre KIB by mala mať aj stále odborné kapacity (pracovné skupiny) schopné riešiť dlhodobé úlohy. Momentálne existujú pracovné skupiny

 Výbor pre kybernetickú bezpečnosť pri Bezpečnostnej rade

 Komisia pre kybernetickú bezpečnosť Riaditeľa NBÚ

 pracovná skupina pre kybernetickú bezpečnosť pri ÚPVII

 pracovné skupiny pre kybernetický zločin, kritickú infraštruktúru (MV SR),

Tieto skupiny majú príbuznú problematiku, v niektorých pôsobia tí istí ľudia. Pre efektívne riadenie KIB je nevyhnutné zabezpečiť koordináciu týchto skupín, prípadne zlúčenie niektorých z nich.

Komisia by mala mať minimálne pracovné skupiny pre :

Bezpečnostnú architektúru

Štandardy pre informačnú bezpečnosť

Bezpečnosť e-Governmentu

Riadenie rizík vo verejnej správe v oblasti KB a IB.

## Zabezpečenie základnej úrovne ochrany virtuálneho priestoru VS

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

dohodnúť pokrytie čo najväčšieho počtu ISVS existujúcimi CSIRT-ami

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.

Úlohy a) a b) 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 navrhované v rámci Centra pre kyberneticku a informačnú bezpečnosť a tiež dostatočná odborná a personálna kapacita na ústrednom orgáne, ako aj v rámci jednotlivých ÚOŠS.[[22]](#footnote-23) Odporúčame použiť COBIT na mapovanie pre všetky procesy povinnej osoby, ale hlavne premostenie na argumentáciu v GAP analýze, čo chýba v štandardoch ISVS, kde:

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.

## Systematické zabezpečenie informačnej bezpečnosti vo verejnej správe

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

Prevencia - definícia bezpečnostných štandardov, definícia procesov a ich implementácia

Reakcia – riešenie bezpečnostných incidentov, proaktívne a reaktívne služby riešenia bezpečnostných incidentov

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.

### Prevencia a riadenie KIB

Pre štandardizáciu postupov v oblasti riadenia[[23]](#footnote-24) 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[[24]](#footnote-25) 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 ústrednom orgáne štátnej správy 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, sektorovej a národnej úrovni .

Implementovať systém riadenia informačnej bezpečnosti v organizácií (vrátane analýzy bezpečnostných rizík) a implementáciu bezpečnostných opatrení za účelom vytvorenia bezpečnostného baseline v organizácií.

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 VS 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 rodinu štandardov ISO 27000, špecialne štandardy ISO 27001:2013 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.[[25]](#footnote-26) 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.

### Reakcia na bezpečnostné incidenty

V rámci riešenia incidentov 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 alebo sektora
* 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 z hľadiska organizácie obsahuje minimálne nasledujúce kroky[[26]](#footnote-27) :

* 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 jasne určiť kompetencie a zabezpečiť efektívnu spoluprácu medzi jednotlivými zložkami pri riešení bezpečnostných incidentov. Ide o :

národný orgán pre kybernetickú bezpečnosť

VPA v zmysle zákona o kybernetickej bezpečnosti

Prevádzkovatelia prvkov kritickej infraštruktúry

Spravodajské služby

Národný CSIRT

Vládny CSIRT

Vojenský CSIRT

Ostatné CSIRTy

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

### 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[[27]](#footnote-28) .

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 informačnej bezpečnosti | Technické, procesné alebo dokumentačné posúdenie informačnej bezpečnosti | Posúdenie zhody informačnej bezpečnosti so štandardom alebo súlad s legislatívnymi, normatívnymi, regulačnými alebo zmluvnými požiadavkami. | Raz za tri roky musia byť auditované všetky IS a procesy, odporúča sa vykonávať čiastkové audity raz ročne | Stredná úroveň vyspelosti bezpečnostných opatrení, nezávislosť audítora na predmete auditu. | Analýza rizík, Posúdenie zraniteľností |
| Posúdenie zraniteľností | 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 |
| Penetračné 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 a národnej úrovni na komplexné posudzovanie informačnej bezpečnosti, ktoré je potrebné implementovať na získanie prehľadu o stave informačnej bezpečnosti v organizácií resp. rezorte/sektore resp. národnej úrovni.

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. Ďalším krokom pre efektívne zabezpečenie slovenského virtuálneho priestoru je vypracovanie systému klasifikácie informácií a systémov a návrh bezpečnostných požiadaviek a povinných súborov opatrení pre jednotlivé bezpečnostné kategórie systémov.

## 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

vybudovať centrum excelencie pre KIB (výskum, expertná činnosť, vzdelávanie)

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[[28]](#footnote-29), ale **najmä zaviesť do praxe** komplexný systém vzdelávania v KIB. Pre štátne organizácie z hľadiska KIB rozlišujeme štyri skupiny zamestnancov v štátnych inštitúciách, 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.

V rámci verejnej správy bude potrebné vybudovať (dobudovať) bezpečnostné a CSIRT tímy minimálne v nasledujúcom zložení :

vládny CSIRT tím (vládna jednotka CSIRT)

sektorové CSIRT tímy (v pôsobnosti VPA v zmysle zákona o KB)

vládny bezpečnostný tím

sektorové bezpečnostné tímy

Úlohy a povinnosti týchto typov tímov sú uvedené v Metodike pre spoločné postupy a podporu.

* 1. **Vypracovanie metodického rámca pre riadenie KIB vo verejnej správe**
     1. **Metodický rámec riadenia KIB vo verejnej správe**

Hlavnou úlohou Centra pre KIB by mala byť 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 ústredných orgánoch štátnej správy (tzv. maticový model, podobný už začína ÚPVII používať pri rozpočtovaní výdavkov na IT).

Vzhľadom na aktuálny stav bude musieť byť zadefinovaný modelová štruktúra riadenia KIB na ústrednom orgáne štátnej správy.

* + - 1. **Hlavné úlohy navrhovaného Centra pre KIB**

V navrhovanej organizačnej štruktúre by mala byť v prvom rade zadefinovaná rola Chief Information Security Officer (CISO) pre verejnú správu, ktorý by zodpovedal za riadenie a presadzovanie KIB vo verejnej správe ako hlavná autorita.

Úlohou CISO bude hlavne v spolupráci s 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.
* 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)

S pohľadu riešenia bezpečnostných incidentov je vhodné zachovať kontinuitu. Do organizačnej štruktúry Centra je možné začleniť CISRT.SK, ktorý by poskytoval technologickú podporu CISO, a to nie len pri riešení bezpečnostných incidentov. Začlenením CSIRT.SK do štruktúry centra by mohlo výrazne urýchliť jeho vytvorenie a efektívne fungovanie. V prípade začlenenia CSIRT.SK do centra je potrebné doplniť úlohy centra o úlohy ktoré plní CSIRT.SK. Avšak spolupráca s CSIRT.SK môže byť vykonávaná na obdobnej úrovni aj bez jeho začlenenia do štruktúry Centra.

* + - 1. **Organizačná štruktúra riadenia KIB na ÚOŠS**

Aktívne, kontinuálne a rutinné riadenie KIB by malo byť realizované na jednotlivých ÚOŠS. 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 informačnej bezpečnosti ktorý je vlastníkom procesu riadenia a zaisťovania KIB na ÚOŠS.
* Stanovenú zodpovednosť realizuje manažér informačnej bezpečnosti prostredníctvom:
  + organizačného útvaru „KIB“
  + organizačného útvaru „prevádzka IT“ (alebo obdobný útvar zodpovedný za prevádzku IT)
  + vedúcich zamestnancov organizačných ostatných útvarov a ich podriadených zamestnancov
* Na procese riadenia a udržiavania KIB sa podieľajú všetky jeho organizačné útvary v rozsahu svojej pôsobnosti.

Na základe skúseností z praxe odporúčame začlenenie manažéra informačnej bezpečnosti a organizačného útvaru KIB mimo organizačný útvar, ktorý má na starosti správu a prevádzku informačných technológií ( napr. iná sekcia). V opačnom prípade dochádza takmer vždy ku konfliktu záujmov. V takýchto prípadoch je väčšinou vždy uprednostnená prevádzka pred bezpečnosťou bez následného riešenia. Taktiež je pri takomto modeli vysoká možnosť zakrývania bezpečnostných rizík a nedostatkov. Z tohto pohľadu ako aj s pohľadu dosiahnutia celkovej efektivity riadenia KIB je potrebné toto opatrenie považovať za veľmi dôležité.

Vzťah manažér informačnej bezpečnosti k Centru pre KIB:

* manažér informačnej bezpečnosti bude metodicky riadený CISO pre verejnú správu (tzv. dotted line reporting).
* Centrum bude poskytovať manažérovi informačnej bezpečnosti metodickú podporu, odbornú podporu, podporu pri riešení bezpečnostných incidentov.
* Centrum bude slúžiť ako eskalačný subjekt
* manažér informačnej bezpečnosti bude zodpovedný za implementáciu stanovených bezpečnostných opatrení a ich reportovanie prostredníctvom portálu (self-assessment) Centra.
* Centrum bude oprávnené vykonávať kontrolné aktivity samostatne, alebo prostredníctvom tretích osôb (napr. audítorské spoločnosti).
* Centrum 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 ústredných orgánov štátnej správy s Centrom 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 informačnej bezpečnosti a  organizáciám podriadeným ústredným orgánom štátnej správy .

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 jednoznačnej správcu, ktorý bude vykonávať v oblasti riadenia KIB obdobné úlohy ako ústredné orgány štátnej správy (definovaná pozícia manažéra informačnej bezpečnosti), organizačný útvar KIB a pod.). V prípade potreby môžu byť tieto štruktúry vytvorené v Centre.

## 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 úlohy z Akčného plánu, ktoré boli pôvodne dané MF SR (odporúčanie pracovnej skupiny):



## Vytvorenie rámca požiadaviek a postupov pre implementáciu a koordináciu požiadaviek GDPR regulácie vo verejnej správe

Za účelom 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 Centrom 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.

## 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 Centra (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 (prípadne kritickej infraštruktúre). 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.

## Zahraničná spolupráca

Zahraničná spolupráca je pre zaistenie adekvátnej ochrany slovenského virtuálneho priestoru nevyhnutnosťou, nakoľko je otvoreným podpriestorom globálneho priestoru. Nízka úroveň zaistenia slovenského virtuálneho priestoru 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 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. Národná autorita (v spolupráci s MZV SR) bude musieť

identifikovať (pracovné) orgány EÚ, NATO, prípadne iných medzinárodných organizácií ktoré riešia KIB a v ktorých máme/mali by sme mať zastúpenie, zástupcov, ktorých SR v týchto orgánoch má a činnosť ktorú orgány/naši zástupcovia v nich vyvíjajú,

prezrieť medzinárodné zmluvy s informaticky vyspelými partnermi a zistiť, či na ich základe nie je možné nadviazať spoluprácu v oblasti KIB,

určiť, čo by sme od zahraničných partnerov potrebovali a čo im môžeme ponúknuť,

zaistiť účasť odborníkov v delegáciách, resp. na rokovaniach s potenciálnymi partnermi.

vyhodnocovať prínos zmlúv, Memoránd a dohôd pre KIB[[29]](#footnote-30).

## 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.

V úvodnej fáze vzniku centrálnej autority a zavádzania systému riadenia KIB vo verejnej správe je vhodné dočasne (1-2 roky) zamestnať odborníkov z komplexnými a viacročnými skúsenosťami v prípade potreby aj dodávateľskou formou (zmluvy s konkrétnymi osobami). Ich úlohou bude zaistiť plynulý nábeh prevádzky Centra a plnenia jeho základných úloh ako aj výber zamestnancov, ktorý zabezpečia jeho ďalšiu prevádzku. Pri výbere start-up tímu je potrebné zamerať sa na konkrétne skúsenosti jednotlivcov v uvedenej oblasti, ktorý reálne budú vykonávať úlohy a aktivity v mene organizácie. Ich základným poslaním bude vytvoriť funkčné tímy a organizačné jednotky, ktoré po úvodnej fáze dokážu existovať samostatne. Vypracovane rámca bezpečnostných opatrení ako aj dielčích metodík ich implementácie je možné realizovať dodávateľským spôsobom. Avšak v takom prípade je potrebné zabezpečiť efektívnu kontrolu kvality interným odborným personálom. Takýto postup je možným kandidátom na financovanie z OP EVS – analytické tímy.

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

## 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

Vytvorenie tímu pre riadenie KIB na úrade (Centrum) môže priniesť ďalšie rozpracovanie dokumentu a pokrytie niektorých oblastí detailnejší

Hrozby:

Nedohoda na prevzatí kompetencií v oblasti KIB ISVS úradom

Nejasné kompetencie na vyššej úrovni riadenie KIB v štáte

Nedostatok financií na navrhované opatrenia

Vznik národného českého centra pre kybernetickej bezpečnosti v Brne

# 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 úloha. 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.

* 1. **Organizačno-kompetenčné zabezpečenie riadenia KIB vo verejnej správe**

|  |  |
| --- | --- |
| **Ú.1 Organizačné a personálne zaistenie KIB na ÚPVII** | |
| Názov | Vytvorenie organizačnej štruktúry pre KIB bezpečnosť a jej personálne obsadenie na ÚPVII a upravenie jej postavenia aj zákonom. |
| Špecifikácia | Koordináciu riešení úloh na zaistenie KIB ISVS bude potrebné vytvoriť sekciu alebo odbor 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 | Úrad vlády |
| Termín |  |
| Zdroje | * návrh na organizačnú štruktúru, úlohy, počty a kvalifikáciu zamestnancov, harmonogram budovania útvaru, základné dokumenty útvaru * pracovné miesta * náklady na   + priestory   + technické vybavenie   + informačné zdroje   + cestovanie   + vzdelávanie |
| Kooperujúce orgány |  |
| Poznámka | Keďže kvalifikovaných odborníkov pre KIB nie je dostatok, môže byť problém naplniť stavy sekcie/odboru pre KIB na ÚPVII kompetentnými ľuďmi. Preto by namiesto definitívneho stavu mohla byť definovaná organizačná štruktúra, ktorá by sa postupne osadzovala 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[[30]](#footnote-31) 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 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. |

#### 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 ústredných orgánoch štátnej správy, 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 ústredných orgánoch štátnej správy kontrolovať, či pre dané kompetencie / procesy sú alokované potrebné zdroje.

Dôležitým faktorom pre nájdenie optimálneho modelu bude aj činnosť Centra, ktoré musí detailne rozpracovať opatrenia KIB pre informačné systémy verejnej správy a to do niekoľkých úrovní vyspelosti. Cieľom silnej metodickej podpory zo strany Centra 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 v medzinárodne uznávaných inštitúciách (napr. ISACA, SANS, ISC2 a pod.), 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 (CSIRT.SK, Centrum, PZ SR a pod.).

Všetky školenia a výukové aktivity vrátane interných musia byť finančne ohodnotené a vyčíslené. Zamestnanci pred ich absolvovaním budú musieť uzavrieť s Centrom 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 Centra 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 Centra.

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.

* 1. **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 na základe bezpečnostných požiadaviek na dôvernosť, integritu, dostupnosť a autentickosť informácie |
| 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 |  |
| Termín |  |
| Zdroje |  |
| Kooperujúce orgány | MV SR (kritická infraštruktúra), ÚOOÚ SR (osobné údaje), NBÚ SR (utajované skutočnosti a elektronický podpis) |
| Poznámka | existujú dve použiteľné riešenia, systém Grundschutz nemeckého BSI s rozsiahlymi katalógmi hrozieb, zraniteľností a opatrení a americké riešenie postavené na štandardoch FIPS 199 a FIPS 200 |

|  |  |
| --- | --- |
| **Ú.4. Audit** | |
| Názov | Vypracovať návrh systému auditu ISVS a monitorovania dodržiavania štandardov ISVS  Výkon auditu by mal pozostávať minimálne z overenia  a) súladu so štandardami ITVS  b) vhodnosti a dostatočnosti opatrení a prostriedkov na zabezpečenie požiadaviek KIB  c) súladu s podmienkami vnútorných predpisov v oblasti prevádzky ITVS, ktoré správca určil v súlade so všeobecne záväznými právnymi predpismi |
| Špecifikácia | Vypracovať požiadavky na audítorov, frekvenciu auditu, monitoring dodržiavania povinnosti auditu a aktualizáciu štandardov na základe skúseností z výstupov auditov. |
| Zdôvodnenie | Z analýzy súčasného stavu vyplýva, že porušenia, ktoré vedú k zlyhaniam pri penetračnom testovaní nasvedčujú, že sa nedodržiavajú ani existujúce štandardy ISVS. |
| Výstupy | Návrh procesov auditu na úrovni governance (ÚPVII, odvetvie/sektor, povinné osoby) ako aj pri všetkých etapách životného cyklu ISVS.  Určenie postupov pre minimálny rozsah auditu projektov súvisiacich s vznikom nových ISVS, monitorovaním prevádzky existujúcich ISVS a zaistením súladu požiadaviek na prevádzkovanie e-Government služieb a podmienok prevádzky ISVS, ktoré tieto služby podporujú. |
| Riešiteľ |  |
| Termín |  |
| Zdroje |  |
| Kooperujúce orgány |  |
| Poznámka | Mechanizmus, ktorý by mal byť súčasťou navrhovaného zákona o kybernetickej bezpečnosti sa bude týkať len tých ISVS, ktoré budú zaradené do systémov podporujúcich základné služby, nakoľko nie sú zatiaľ dané parametre, ktoré určia zaradenie do zoznamu základných služieb, nie je jasný ani záber tohto mechanizmu auditu. Na druhej strane, analýza ukázala, že nedostatky v zabezpečovaní bezpečnostných opatrení podľa súčasných štandardov ISVS sú enormné a systematický prístup k auditu má napomôcť tento stav zlepšiť. Naviac bezpečnosť ITVS môže narušiť aj malý nevýznamný systém tým, že sa pri súčasnej miere integrácie stane cestou pre kybernetický útok na iné systémy, s ktorými je prepojený alebo spolu sedia v jednom cloude. |

|  |  |
| --- | --- |
| **Ú.5 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 |  |
| Termín |  |
| Zdroje |  |
| Kooperujúce orgány |  |

* 1. **Vytvorenie štandardných / referenčných postup v oblasti KIB pre ISVS**

|  |  |
| --- | --- |
| **Ú. 6 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. |
| 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 |  |
| Termín |  |
| Zdroje |  |
| Kooperujúce orgány |  |
| **Ú.7 Štandardizácia oblasti KIB na Slovensku – preklad ISO 27032** | |
| Názov | Preklad ISO 27032 |
| Špecifikácia | Preklad ISO 27032 ako podkladu pri príprave na vypracovanie nového slovenského štandardu pre KB v oblasti ISVS |
| Zdôvodnenie | Z indexu ITU je zrejmé, že SR nemá pozitívne hodnotenie v oblasti štandardizácie. Absencia slovenského textu najdôležitejších štandardov z oblasti KIB v rámci STN nepodporuje rozvoj povedomia a prenos najlepšej praxe do slovenského prostredia. |
| Výstupy | Preklad ISO 27032 |
| Riešiteľ | PS/ TK 37 |
| Termín |  |
| Zdroje | ÚPVII |
| Kooperujúce orgány | ÚNMS |

|  |  |
| --- | --- |
| **Ú.8 Návrh slovenského štandardu KIB** | |
| Názov | Vypracovať návrh slovenského štandardu KIB |
| Špecifikácia | Vypracovať návrh slovenského štandardu KIB |
| Zdôvodnenie | Z indexu ITU je zrejmé, že SR nemá pozitívne hodnotenie v oblasti štandardizácie. Prínosom aplikácie najdôležitejších štandardov z oblasti KIB v rámci STN do vlastného štandardu by umožnila zahrnúť špecifiká ISVS a potrieb slovenského prostredia. |
| Výstupy | Návrh novej STN pre oblasť KIB |
| Riešiteľ |  |
| Termín |  |
| Zdroje |  |
| Kooperujúce orgány |  |

|  |  |
| --- | --- |
| **Ú. 9 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)  ministerstvá, ústredné orgány (NBÚ SR, MV SR, MS SR SIS,...) |
| Zdôvodnenie | Získanie a udržanie prehľadu o stave, problémoch a trendoch v KIB ISVS/alebo SR. Bude sa využívať pre riadenie aktivít na zaistenie KIB ISVS alebo celej SR |
| Výstupy | Osnova prehľadu (kvôli zabezpečeniu spolupráce ostatných štátnych orgánov)  správa (v slovenčine aj angličtine) |
| Riešiteľ | ÚPVII (komunikácia s respondentami CSIRTami a štátnymi orgánmi |
| 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 | Budeme zverejňovať celú správu, alebo bude mať utajenú časť?  nebudeme niektoré časti správy robiť každý rok? |

|  |  |
| --- | --- |
| **Ú.10 Prehľad legislatívy EÚ** | |
| Názov | Vypracovať prehľad legislatívy EÚ relevantnej z hľadiska KIB |
| Špecifikácia | Prehľad by mal identifikovať úlohy, ktoré SR z európskych právnych aktov vyplývajú, spôsob, akým boli príslušné právne akty implementované do slovenského právneho systému, ktoré štátne orgány sú za ich plnenie zodpovedné, prípadne koho ďalšieho sa tieto úlohy týkajú a tiež závislosti medzi európskymi právnymi aktmi a závislosti medzi úlohami. |
| Zdôvodnenie | Získanie a udržanie prehľadu o povinnostiach, ktoré SR má v KIB vo vzťahu k EÚ, podklad pre slovenskú legislatívu, aj koordináciu aktivít štátnych orgánov SR |
| Výstup | Základný prehľad,  raz mesačne informácie o prijatých eu dokumentoch (stručná charakteristika dokumentu, úlohy pre SR, termíny, nadväznosti, ktorých štátnych orgánov sa úlohy týkajú)  raz ročne súborná kapitola v správe o stave KIB v SR |
| Riešiteľ | buď právnici z ÚPVII, alebo úloha pre PraF UK, príp. externá právna kancelária |
| Termín | 1 rok |
| Zdroje | odhadovaná zložitosť 1000 hodín práce na počiatočnú analýzu  240 hodín ročne |
| Kooperujúce orgány | MZV SR, Zastúpenie EK v SR |
| Poznámka | cieľom tejto aktivity je včas zachytiť dokumenty, z ktorých pre SR vyplývajú nejaké povinnosti v KIB a zistiť, ktorých štátnych orgánov sa týkajú. Na základe prehľadu bude možné vybrať dokumenty, ktoré sa majú analyzovať detailne. |

## Vzdelávanie v KIB

|  |  |
| --- | --- |
| **Ú.11 Vzdelávanie v KIB** | |
| Názov | Vypracovanie systému vzdelávania a pilotný projekt vzdelávania v KIB pre verejnú správu |
| Špecifikácia | Prehodnotiť získané poznatky a materiály vypracované v rámci projektu vzdelávania v IB 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 IB. 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 |  |
| Doba trvania | 2 roky |
| Zdroje |  |
| Kooperujúce orgány | Ministerstvo školstva, UPVII |
| Poznámka | Ide o základné kurzy v rozsahu 40 (vedúci pracovníci a laici) a 80 hodín (informatici, špecialisti v IB/KB a lektori IB/KB) a výberové bloky v rozsahu 20 (vedúci pracovníci a laici) a 40 hodín ostatní. Na základné vzdelávanie by malo nadväzovať špecializačné pre informatikov a špecialistov v IB, kde by mali získať aj praktické zručnosti, čo si však vyžaduje vybudovanie laboratórií a časovo náročnejšiu prácu v malých skupinách. |

|  |  |
| --- | --- |
| **Ú. 12**  **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 ÚVPII a povinných osôb |
| Riešiteľ | UPVII v spolupráci s univerzitami |
| Termín | 1 rok (kurzy a doplnkové vysokoškolské štúdium) |
| 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. 13**  **Budovanie bezpečnostného povedomia zamestnancov verejnej správy a verejnosti** | |
| Názov | Budovanie bezpečnostného povedomia zamestnancov a verejnosti |
| Špecifikácia | Vypracovanie systému školení zameraných na budovanie bezpečnostného povedomia zamestnancov verejnej správy (forma, frekvencia, obsah)  Organizácia aktivít, podporujúcich bezpečnostné povedomie verejnosti  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 | CSIRTy, Ministerstvo školstva, MV SR, Úrad vlády |

### Zvyšovanie bezpečnostného povedomia pre občanov

Pre zvyšovanie bezpečnostného povedomia občanov bude mierne modifikovaný obsah sprístupnený multimediálnou formou bez e-learningových funkcionalít zdarma na stránkach Centra / ÚPVII. Na uvedenej webovej stránke 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.

# Prílohy

## 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](http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24695), schválená uznesením vlády SR č. 334/2015.
* Akčný plán realizácie Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020

## Aktuálny zoznam zákonov a vykonávacích predpisov relevantných pre KIB ISVS

**Základný legislatívny rámec 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. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom
* trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) 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. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
* zákon č. 185/2015 Z. z. Autorský zákon 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 neskorších predpisov,
* zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* 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 SR na preskúmavanie rozhodnutí Národného bezpečnostného úradu,
* zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov 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 v znení neskorších predpisov,
* zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších právnych predpisov,
* nariadenie vlády SR č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností,
* výnos č. 55/2014 Z. z. Ministerstva financií SR zo 4. marca 2014 o štandardoch pre informačné systémy verejnej správy
* zákon 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
* Zbierka zákonov č. 525/2011 Výnos Ministerstva vnútra SR z 12. decembra 2011 o štandardoch pre elektronické informačné systémy na správu registratúry
* Zbierka zákonov č. 164/2013, Vyhláška Úradu na ochranu osobných údajov SR z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení
* Zbierka zákonov č. 117/2014, Vyhláška Úradu na ochranu osobných údajov SR z 24. apríla 2014, ktorou sa mení a dopĺňa vyhláška Úradu na ochranu osobných údajov č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení
* Zbierka zákonov č. 165/2013, Vyhláška Úradu na ochranu osobných údajov SR z 13. júna 2013, ktorou sa ustanovujú podrobnosti o skúške fyzickej osoby na výkon funkcie zodpovednej osoby
* Vyhláška č. 132/2016 Z. z. zo dňa 23. 03. 2016 Úradu pre verejné obstarávanie, ktorou sa ustanovujú podrobnosti o postupe certifikácie systémov na uskutočnenie elektronickej aukcie

Vyhlášky Národného bezpečnostného úradu upravujúce ochranu utajovaných skutočností sú:

* 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. 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.

## 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[[31]](#footnote-32) 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.



Týchto 5 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. |



## 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[[32]](#footnote-33), informácií získaných z tzv. „threat intelligence“ platformy implementovanej CSIRT.SK[[33]](#footnote-34), 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



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

Uvádzané zraniteľnosti sú iba zraniteľnosti, ktoré bolo možné získať na základe informácií z otvorených zdrojov (napríklad SHODAN, a informácií o zraniteľnostiach, ktoré boli doručené CSIRT.SK v rámci threat intelligence). Nejedná sa teda o všetky zraniteľnosti na uvedených IP rozsahoch nakoľko v súčasnosti CSIRT.SK nemá možnosť vykonávať proaktívne skenovanie IP adries na zistenie zraniteľností okrem dohôd o vykonaní penetračných testov. Výsledky z penetračných testov sú uvedené v ďalšej časti tohto dokumentu.

Vo verejnej správe okrem incidentov získaných ako threat intelligence boli riešené bezpečnostné incidenty nahlásené organizáciami samotnými, alebo sa jednalo o obzvlášť závažné bezpečnostné incidenty identifikované v rámci činnosti CSIRT.SK.

Obrázok Závažné bezpečnostné incidenty vo verejnej správe

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[[34]](#footnote-35) 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 Kybernetické 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 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[[35]](#footnote-36):

* **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 [[36]](#footnote-37) a preto v súčasnosti v mnohých organizáciách chýbajú základné prvky zabezpečenia infraštruktúr, sú nesprávne nasadené alebo nakonfigurované.
* **Nedostatky v operačnej 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.

Pri obmedzených externých penetračných testoch[[37]](#footnote-38) bolo pri viac ako 90 percent penetračných testoch identifikovaná aspoň jedná závažná[[38]](#footnote-39) a/alebo kritická[[39]](#footnote-40) 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)

## 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[[40]](#footnote-41) 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.

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)



### Postup implementácie

CSF poskytuje nielen rámec pre kybernetickú bezpečnosť ale aj základný návod[[41]](#footnote-42) na jeho implementáciu a to v 7 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

**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 5 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 (detekuj) — 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.



Záver:

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. [↑](#footnote-ref-2)
2. niekedy sa uvádzajú len tri - confidentiality, integrity, availability, tzv. CIA, pričom integrita zahŕňa aj autentickosť [↑](#footnote-ref-3)
3. obrázok je prevzatý z normy ISO/IEC 27032:2012 [↑](#footnote-ref-4)
4. Internet Security Threat Report 2017, <https://www.symantec.com/security-center/threat-report> [↑](#footnote-ref-5)
5. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017 [↑](#footnote-ref-6)
6. podrobnejší zoznam na <http://cordis.europa.eu/search/result_en?q=cybersecurity> obsahuje 165 položiek [↑](#footnote-ref-7)
7. s výnimkou systémov, ktoré sú izolované, alebo zapojené len do vyhradených sietí [↑](#footnote-ref-8)
8. Zákon č. 68/2018 Z.z. [↑](#footnote-ref-9)
9. Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008. [↑](#footnote-ref-10)
10. schválená uznesením vlády SR č. 328/2015 [↑](#footnote-ref-11)
11. § 4, ods. 2), písm. f) zákona č. 275/2006 Z .z. [↑](#footnote-ref-12)
12. § 10b zákona č. 110/2004 Z. z. [↑](#footnote-ref-13)
13. GSI 2017, International Telecommunication Union (ITU) 2017, s.20 Methodology [↑](#footnote-ref-14)
14. Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike, MF SR, 2013 [↑](#footnote-ref-15)
15. https://www.csirt.gov.sk [↑](#footnote-ref-16)
16. IP adresy pridelené subjektom v Slovenskej republike, webové portály a služby v rámci TLD domény .sk [↑](#footnote-ref-17)
17. 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. [↑](#footnote-ref-18)
18. 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. [↑](#footnote-ref-19)
19. blízko k tomu má podľa štatútu Komisia pre kybernetickú bezpečnosť riaditeľa NBÚ, ale v nej chýba zastúpenie štátnych orgánov, pracovné skupiny, finančné a organizačné zabezpečenie činnosti, reálny záujem NBÚ na jej činnosti [↑](#footnote-ref-20)
20. úlohy podobného zamerania a rozsahu zabezpečoval v minulosti odbor informačnej bezpečnosti, legislatívy a štandardov sekcie informatizácie spoločnosti MF SR [↑](#footnote-ref-21)
21. analyzoval a pripravil návrh na zosúladenie [↑](#footnote-ref-22)
22. Katalóg hrozieb, zraniteľností a opatrení Spolkového úradu pre informačnú bezpečnosť má niekoľko tisíc strán [↑](#footnote-ref-23)
23. Rozpracované v kapitole 6.8 [↑](#footnote-ref-24)
24. 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 [↑](#footnote-ref-25)
25. https://www.csirt.gov.sk/aktualne-7d7.html?id=120 [↑](#footnote-ref-26)
26. Jednotlivé kroky sú podrobne rozpísané v Metodike pre spoločné postupy a podporu [↑](#footnote-ref-27)
27. Uvedené mechanizmy je možné nahradiť ekvivalentnými mechanizmami v prípade, že ich súčasťou budú výstupy špecifikované nižšie. [↑](#footnote-ref-28)
28. Stále je aktuálny Systém vzdelávania v informačnej bezpečnosti, schválený Vládou SR v roku 2009 [↑](#footnote-ref-29)
29. majú sa na mysli zmluvy zahŕňajúce spoluprácu v KIB [↑](#footnote-ref-30)
30. bezpečnostný tím môže v malej organizácii tvoriť zamestnanec vykonávajúci povinnosti bezpečnostného manažéra na čiastočný úväzok [↑](#footnote-ref-31)
31. GCI 2017, International Telecommunication Union (ITU) 2017, s. 17 CGI Pillars and Sub-pillars [↑](#footnote-ref-32)
32. IP adresy pridelené subjektom v SR, webové portály a služby v rámci TLD domény .sk [↑](#footnote-ref-33)
33. 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. [↑](#footnote-ref-34)
34. Pozn. rok 2016, je potrebné prepočítať za predchádzajúce obdobie [↑](#footnote-ref-35)
35. [↑](#footnote-ref-36)
36. Analýza rizík je iba formálna alebo chýba úplne [↑](#footnote-ref-37)
37. S vylúčením útoku na celý perimeter organizácie pri testovaní iba konkrétnej služby, projektu alebo časti perimetra [↑](#footnote-ref-38)
38. 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. [↑](#footnote-ref-39)
39. Kritická zraniteľnosť je zneužiteľná zraniteľnosť, ktorej zneužitím je možné kompromitovať celý informačný systém, alebo infraštruktúru organizácie, alebo informačné systémy napojené na tento informačný systém. [↑](#footnote-ref-40)
40. Control Objectives for Information and Related Technology, ISACA [↑](#footnote-ref-41)
41. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, National Institute of Standards and Technology, February 12, 2014 [↑](#footnote-ref-42)