**Národná koncepcia informatizácia verejnej správy**

**Strategická priorita 10 Kybernetická bezpečnosť**

verzia 1.7

Bratislava, 09.10.2017

**Document Information**

|  |  |
| --- | --- |
| Project name | Rozpracovanie NKIVS |
| Person responsible | Peter Poliak |
| Authors | Daniel Olejár, Lenka Gondová, Lukáš Hlavička, Peter Poliak |
| Document name | 10. prioritná oblasť NKIVS, Kybernetická bezpečnosť |
| Status | **in process** | submitted to QA | accepted by QM | approved |

**History of Alteration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | | Date | Type of editing | Editorial |
| 1.0 | 15/09/17 | | Návrh štruktúry a obsahu dokumentu | Daniel Olejár |
| 1.1 | 18/09/17 | | vloženie materiálov vypracovaných pre predchádzajúcu WG do štruktúry dokumentu  rozpracovanie obsahu prvých troch kapitol  Formálne úpravy | Daniel Olejár |
| 1.2 | 19/09/17 | | kapitoly 4, 5 a prílohy | Daniel Olejár |
| 1.3 | 25/09/17 | | kapitoly 1-4, doplnená časť 5.1.1 a 2 | Daniel Olejár |
| 1.4 | 01/10/17 | | doplnená časť 5.2.5 a príloha 9.6  dopracované kapitoly 5 a 6,  doplnené prílohy 9.3, 9.4, 9.5, 9.9 a 9.10 | Lenka Gondová  Daniel Olejár  Daniel Olejár |
| 1.5 | 01/10/17 | | doplnená časť 4.2, príloha audit, zapracované pripomienky LG | Daniel Olejár, Lenka Gondová |
| 1.6 | 06/10/17 | | doplnená časť 5.2.6 | Daniel Olejár, Lukáš Hlavička |
| 1.7 | 09/10/17 | | zapracovaná časť pripomienok, štylistické úpravy, doplnenie častí 4.1. (pojmy) a 7.1. ciele/úlohy, obrázku 1 | Daniel Olejár |
| 1.8 | 09/10/17 | | Editácia, úprava štruktúry dokumentu a doplnenie cieľov /úloh, Riešenia | Peter Poliak, Richard Kiškováč |

Obsah

[1 Úvod 6](#_Toc495308307)

[2 Ciele dokumentu 6](#_Toc495308308)

[3 Adresáti dokumentu 6](#_Toc495308309)

[4 Základné pojmy a označenia 7](#_Toc495308310)

[4.1 Základné pojmy 7](#_Toc495308311)

[4.2 Skratky 9](#_Toc495308312)

[5 Súčasná situácia v IB/KB 10](#_Toc495308313)

[5.1 Koncepcia a legislatíva EÚ v kybernetickej bezpečnosti 10](#_Toc495308314)

[5.2 Informačná a kybernetická bezpečnosť SR a ISVS 11](#_Toc495308315)

[5.2.1 Legislatívny rámec IB/KB v SR 12](#_Toc495308316)

[5.2.2 Kompetencie 13](#_Toc495308317)

[5.2.3 Koncepcie informačnej a kybernetickej bezpečnosti a ich realizácia 13](#_Toc495308318)

[5.2.4 Hodnotenie stavu informačnej/kybernetickej bezpečnosti Slovenska podľa GSI 14](#_Toc495308319)

[5.2.5 Stav ochrany ISVS podľa zistení CSIRT.SK 16](#_Toc495308320)

[5.2.6 Problémové oblasti z pohľadu bezpečnosti ISVS 16](#_Toc495308321)

[5.3 Zhrnutie stavu informačnej a kybernetickej bezpečnosti v SR 18](#_Toc495308322)

[6 Priority 18](#_Toc495308323)

[6.1 Kybernetická bezpečnosť v Národnej koncepcii informatizácie verejnej správy Slovenskej republiky 18](#_Toc495308324)

[6.2 Kybernetická bezpečnosť v Operačnom programe integrovaná infraštruktúra 19](#_Toc495308325)

[6.3 Ciele (návrh PS) 20](#_Toc495308326)

[7 Riešenia 20](#_Toc495308327)

[7.1 Koncepcia, legislatíva, kompetencie 20](#_Toc495308328)

[7.2 Predpokladané riadenie/koordinácia zabezpečenia slovenského virtuálneho priestoru 21](#_Toc495308329)

[7.3 Zabezpečenie základnej úrovne ochrany virtuálneho priestoru SR 22](#_Toc495308330)

[7.4 Budovanie odborných kapacít 22](#_Toc495308331)

[7.1 Zavedenie systému pre riadenie kybernetickej a informačnej bezpečnosti (Security Governance) vo verejnej správe 23](#_Toc495308332)

[7.2 Vypracovanie metodického rámca pre riadenie kybernetickej a informačnej bezpečnosti vo verejnej správe 24](#_Toc495308333)

[7.2.1 Metodický rámec riadenia kybernetickej a informačnej bezpečnosti vo verejnej správe 24](#_Toc495308334)

[7.3 Budovanie bezpečnostného povedomia 27](#_Toc495308335)

[7.4 Zahraničná spolupráca 27](#_Toc495308336)

[7.5 Kritické faktory úspechu 28](#_Toc495308337)

[8 Ďalší postup / úlohy 28](#_Toc495308338)

[Ú.Leg.3. Štandardy IB/KB 28](#_Toc495308339)

[9 Prílohy 30](#_Toc495308340)

[9.1 Malý výkladový slovník 30](#_Toc495308341)

[9.2 Prehľad najdôležitejších dokumentov Informačnej a kybernetickej bezpečnosti SR (pracovný názov) 30](#_Toc495308342)

[9.3 Aktuálny zoznam zákonov a vykonávacích predpisov relevantných pre informačnú a kybernetickú bezpečnosť ISVS 31](#_Toc495308343)

[9.5 Úlohy Akčného plánu na realizáciu Koncepcie kybernetickej bezpečnosti 33](#_Toc495308344)

[9.6 Kapacity SR v IB/KB 43](#_Toc495308345)

[9.6.1 Na riešenie incidentov informačnej bezpečnosti 43](#_Toc495308346)

[9.6.2 Organizácie 43](#_Toc495308347)

[9.6.3 Súkromné spoločnosti 43](#_Toc495308348)

[9.6.4 Vzdelávacie inštitúcie 43](#_Toc495308349)

[9.7 Hodnotenie Slovenskej republiky na základe ITU indexu 44](#_Toc495308350)

[9.8 Poznatky CSIRT.SK o stave informačnej/kybernetickej bezpečnosti vo verejnej správe 48](#_Toc495308351)

[9.9 Klasifikácia informácie a systémov 52](#_Toc495308352)

[9.9.1 Význam a podstata klasifikácie informácií a kategorizácie  systémov 52](#_Toc495308353)

[9.9.2 Realizácia 53](#_Toc495308354)

[9.10 Zoznam bezpečnostných rolí a kvalifikačné požiadavky na jednotlivé roly 53](#_Toc495308355)

[9.11 Systém vzdelávania v IB/KB 53](#_Toc495308356)

[9.12 Návrh postupu systematického riešenia informačnej/kybernetickej bezpečnosti v SR 55](#_Toc495308357)

[9.12.1 národná/štátna úroveň 55](#_Toc495308358)

[9.12.2 CSIRT 56](#_Toc495308359)

[9.12.3 Ministerstvá a im na roveň postavené štátne orgány 56](#_Toc495308360)

[9.12.4 Štátne inštitúcie (stredná a nižšia úroveň) 56](#_Toc495308361)

[9.12.5 Špeciálne systémy a aplikácie 56](#_Toc495308362)

[9.12.6 Systémy ktoré nie sú ISVS 57](#_Toc495308363)

# Úvod

Existencia súčasnej spoločnosti v podstatnej miere závisí od spoľahlivého fungovania digitálnych informačných a komunikačných technológií (IKT), ktoré sa používajú na spracovanie informácií vo všetkých oblastiach života spoločnosti; na 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 nutnou podmienkou informatizácie verejnej správy; t. j. aj nutnou podmienkou na dosiahnutie cieľov, ktoré si kladie NKIVS. Vzhľadom na charakter IKT (rozšírenosť a vzájomná prepojenosť) si zaistenie kybernetickej a informačnej bezpečnosti vyžaduje spoluprácu všetkých zainteresovaných; 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 Kybernetickú bezpečnosť NKIVS. Jeho základným cieľom je identifikovať/stanoviť úlohy

1. ktoré štát potrebuje vyriešiť na to, aby zaistil primeranú úroveň bezpečnosti ISVS a ich bezpečnostného okolia;
2. ktoré majú jednotlivé kategórie zainteresovaných pri zaisťovaní primeranej úrovne ochrany slovenského virtuálneho priestoru vo všeobecnosti a ISVS zvlášť.

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

1. vymedzí rozsah problémov informačnej a kybernetickej bezpečnosti (IB&KB), ktoré bude potrebné riešiť na úrovni štátu;
2. špecifikuje, čo je potrebné zaistiť v záujme zabezpečenia ISVS a úloh vyplývajúcich z NKIVS; t.j. stanoví ciele v oblasti kybernetickej a informačnej bezpečnosti pre verejnú správu;
3. opíše aktuálny stav KB&IB v SR a navrhne postupnosť krokov potrebných na naplnenie stanovených cieľov
4. stručne rozoberie existujúcu relevantnú legislatívu, EU aj slovenskú, vrátane aktuálnych materiálov, o ktoré by sa bolo možné oprieť
5. popíše existujúce kompetencie,
6. popíše spôsob správy tohto dokumentu
7. zhrnie kľúčové úlohy v Akčnom pláne?

# Adresáti dokumentu

Dokument je odporúčaním ÚPVII a je určený šiestim kategóriám čitateľov; jeho spoločným cieľom pre každú kategóriu čitateľov je vysvetliť  podstatu a úlohu kybernetickej a informačnej bezpečnosti; pre jednotlivé kategórie potom špeciálne

1. 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;
2. 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;
3. pracovníkom štátnych inštitúcií, ktorí sú zodpovední za zaistenie ochrany ISVS: ako rozpracovať všeobecné úlohy vyplývajúce zo zákonov do systematického riešenia kybernetickej a informačnej bezpečnosti; kde nájsť na to potrebné podrobnejšie informácie a na ktoré štátne inštitúcie sa obrátiť v prípade problémov;
4. dodávateľom IKT, služieb pre štátne inštitúcie: požiadavky na ochranu ISVS a podmienky, ktoré musia dodávané IKT a služby spĺňať;
5. prevádzkovateľom systémov komunikujúcich s ISVS – podmienky, ktoré musia ich systémy spĺňať, aby ich bolo možné pripojiť k ISVS bez rizika kompromitácie ISVS;
6. používateľom ISVS a občanom pristupujúcim k ISVS základné zásady, ktoré musia dodržiavať pri využívaní elektronických služieb verejnej správy.

# Základné pojmy a označenia

V tejto časti uvádzame najdôležitejšie pojmy a skratky, ktoré sa v dokumente používajú, aby sme čitateľovi uľahčili porozumenie dokumentu.

## Základné pojmy

Terminológia informačnej, resp. kybernetickej bezpečnosti 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; stručný výkladový slovník základných pojmov je uvedený v prílohe XXX Terminológia

*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-1). Čokoľvek, čo má pre organizáciu cenu (a vyžaduje si ochranu) predstavuje *aktívum organizácie*. Aktívami organizácie sú napr. technické zariadenia, budovy, informácie, ľudia, dobré meno organizácie a pod. Objektívne existujúca možnosť narušenia štandardného chodu systému (organizácie, podpriestoru) sa nazýva *hrozba*. (Hrozbou je napríklad technická porucha, blesk, požiar, ľudská chyba, omyl, škodlivý kód, útok hackera a i.) Hrozba môže zasiahnuť jedno alebo viacero aktív systému alebo organizácie. 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-2) na bezpečnosť informácií sú základom pre zaistenie potrebnej ochrany systémov. Organizácia analyzuje hrozby voči aktívam organizácie, odhaduje riziká, ktoré z hrozieb voči aktívam vyplývajú a prijíma opatrenia (technické organizačné, personálne a iné riešenia), ktorých cieľom je eliminovať riziká alebo aspoň znížiť hodnotu rizík na akceptovateľnú úroveň. *Informačná bezpečnosť* je 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-3)**

## Skratky

AKOB Akademická obec

AKOBZaA Akademická obec, združenia a asociácie

APZ Akadémia policajného zboru

BR SR Bezpečnostná rada SR

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

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

IB informačná bezpečnosť

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

JA SR Justičná akadémia

JRI jednotka pre riešenie incidentov

KB kybernetická 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

SNAS Slovenská národná akreditačná služba

STN Slovenská technická norma

TLD top level domain

ÚNMS Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky

ÚOŠS Ústredný orgán štátnej správy

ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu

ÚPVS Ústredný portál verejnej správy

ÚV Úrad vlády

VPA vecne príslušná autorita

# Súčasná situácia v IB/KB

Informačná a kybernetická bezpečnosť je problémom aj v globálnom meradle. Okrem objektívnych problémov spôsobených charakterom digitálnych IKT a spôsobom ich používania[[4]](#footnote-4), dramaticky stúpa rozsah a závažnosť cielených útokov na IKT a údaje, ktoré sa v nich spracovávajú. Podľa najnovšej Správy EÚ[[5]](#footnote-5) 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, ale závažné kybernetické útoky vedú štáty, organizácie, teroristické skupiny, niekedy aj jednotlivci a ich cieľom je často kritická infraštruktúra štátu ba dokonca aj narušenie základných demokratických procesov nevyhnutných pre fungovanie štátu. Využívanie prínosov informačnej spoločnosti bude možné len vtedy, ak sa na potrebnej úrovni podarí komplexne zaistiť (informačnú a) kybernetickú bezpečnosť; t.j. vypracovať, prijať a implementovať komplexnú Stratégiu kybernetickej bezpečnosti, vytvoriť potrebné kapacity na jej presadzovanie, zaistiť potrebný počet kvalifikovaných odborníkov a udržiavať potrebnú úroveň bezpečnostného povedomia širokej verejnosti.

## Koncepcia a legislatíva EÚ v kybernetickej bezpečnosti

EÚ sa dlhodobo zaoberá informačnou a kybernetickou bezpečnosťou. V tomto dokumente nie je priestor na rozoberanie aktivít, preto uvádzame len najdôležitejšie legislatívne a koncepčné dokumenty EÚ týkajúce sa kybernetickej bezpečnosti[[6]](#footnote-6), 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. 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.
3. 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
4. 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).
5. Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016
6. 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.
7. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.
8. 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).
9. Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.
10. 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
11. Regulation (EU) 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
12. 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 (poradným, metodickým) orgánom Európskej komisie je Agentúra ENISA. Pripravuje sa nariadenie na posilnenie jej postavenia

1. 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'')

Tieto (a ďalšie) dokumenty sa premietli do slovenskej legislatívy, resp. budú do nej zapracované. Definujú povinnosti, ktoré by SR mala plniť – má o tom niekto prehľad?

## Informačná a kybernetická bezpečnosť 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 (ešte niekto)?

Podstatnú časť systémov vo vlastníctve štátu predstavujú ISVS. Infraštruktúra, na ktorú sú ISVS pripojené a iné systémy, s ktorými ISVS komunikujú, ako aj 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-7) je slovenský kybernetický priestor (resp. globálny kybernetický priestor).

S výnimkou malého počtu izolovaných systémov sú takmer všetky ISVS pripojené na Govnet a prostredníctvom Govnet alebo priamo pripojené na Internet. (Čo špeciálne siete, budeme ich spomínať?)

### Legislatívny rámec IB/KB v SR

Ochrana systémov, sietí a informácií je predmetom úpravy viacerých zákonov, ale jednotiaci *lex generalis* pre oblasť informačnej/kybernetickej bezpečnosti v slovenskej legislatíve chýba. Najdôležitejšie zákony relevantné pre IB&KB a inštitúcie zodpovedné za príslušnú oblasť aktuálne sú

**Zákon č. 215/2004 Z. z. Zákon 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. 122/2013 Z. z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Úrad na ochranu osobných údajov SR),** ktorý **upravuje** ochranu práv fyzických osôb pred neoprávneným zasahovaním do ich súkromného života pri spracúvaní ich osobných údajov, práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb, postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky.

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

**Zákon č. 272/2016 Z. z. Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (Národný bezpečnostný úrad SR)** 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. Zákon o elektronických komunikáciách ()** 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 ()** okrem iného upravuje trestné činy z oblasti počítačovej kriminality.

**Zákon č. 211/2000 Z. z. Zákon o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) ()** 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. Zákon o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente),** ktorý upravuje o.i. identifikáciu osôb a autentifikáciu osôb vo virtuálnom priestore.

**Zákon č. 395/2002 Z. z. Zákon o archívoch a registratúrach a o doplnení niektorých zákonov (MV SR),** ktorý o.i. upravuje elektronický záznam (informácií).

**Zákon č. 575/2001 Z. z.** o organizácii činnosti vlády a organizácii ústrednej štátnej správy.

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

**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. Zákon o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (MF SR, UPVII),** ktorý o.i. 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 stanovuje

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

V súčasnosti sa na ÚPVII pripravuje Zákon o výkone správy v oblasti informačných technológií a o zmene a doplnení niektorých zákonov, ktorý má nahradiť (?) Zákon č. 275/2006 Z. z. Zákon 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

Informačná a kybernetická bezpečnosť je nutným prepokladom fungovania akýchkoľvek systémov postavených na digitálnych IKT a ochrana takýchto systémov vychádza z rovnakých základných princípov. Kompetencie v informačnej a kybernetickej bezpečnosti (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 Slovenskej republiky, 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 2015 boli síce kompetencie NBÚ SR rozšírené o kybernetickú bezpečnosť, ale k reálnemu naplneniu týchto kompetencií nedošlo, lebo zatiaľ nebol prijatý zákon, ktorý by povinnosti zainteresovaných subjektov v oblasti kybernetickej oblasti explicitne špecifikoval (zákon je v medzirezortnom pripomienkovaní a predpokladá sa jeho prijatie do konca roku 2017).

### Koncepcie informačnej a kybernetickej bezpečnosti 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[[8]](#footnote-8) a Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020[[9]](#footnote-9). Obe koncepcie sa zhodli na rovnakých najdôležitejších prioritách.

MF SR, ktoré do roku 2015 riadilo a koordinovalo bezpečnosť ISVS[[10]](#footnote-10) vypracovalo systém vzdelávania v informačnej bezpečnosti a realizovalo rozsiahly dvojročný projekt vzdelávania pracovníkov verejnej správy, vytvorilo CSIRT.sk, harmonizovalo bezpečnostné štandardy ISVS s medzinárodnými, urobilo dva prieskumy stavu informačnej bezpečnosti v SR (2011 a 2013), systematicky budovalo terminológiu informačnej bezpečnosti a pripravilo návrh zákona o informačnej bezpečnosti. (Príloha)

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 (Príloha). Pri BR SR bol zriadený Výbor pre kybernetickú bezpečnosť[[11]](#footnote-11), NBÚ v roku 2016 zriadil Komisiu pre kybernetickú bezpečnosť a pripravil návrh Zákona o kybernetickej bezpečnosti. Nie je známo oficiálne hodnotenie plnenia úloh Akčného plánu (predložil NBÚ správu do Vlády?), podľa informácií od zainteresovaných subjektov sa však väčšina úloh ešte ani nezačala riešiť.

### Hodnotenie stavu informačnej/kybernetickej bezpečnosti Slovenska podľa GSI

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 Slovenska**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rok** | **Skóre** | **Globálne poradie** | **Poradie v Európe** |
| 2014 | 0,618 | 8 | 5 |
| 2017 | 0,362 | 81 | 34 (8. od konca) |

Aj keď metódy zberu informácií nie sú pre roku 2014 a 2017 úplne totožné[[12]](#footnote-12), 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 Slovenska v poslednom období.

**Výsledky vybraných krajín v roku 2017**



V rámci regiónu zostáva za Slovenskom 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 xxx

### Stav ochrany 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[[13]](#footnote-13), súborné informácie o stave zabezpečenia ISVS chýbajú. Istý obraz o stave bezpečnosti ISVS dávajú výsledky CSIRT.SK[[14]](#footnote-14).

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[[15]](#footnote-15), informácií získaných z threat intelligence platformy implementovanej CSIRT.SK[[16]](#footnote-16), vykonaných bezpečnostných auditoch organizácií vo verejnej správe a vykonaných penetračných testov.

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.

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 neobmedzených penetračných testov (cca 15 percent celkového počtu), v ktorých bola dosiahnutá 100% úspešnosť kompromitácie v intervale 3-48 hodín[[17]](#footnote-17), CSIRT.SK dospel k záveru, že pokročilý útočník by mohol bez väčších problémov kompromitovať väčšinu testovaných organizácií verejnej správy.

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

### Problémové oblasti z pohľadu bezpečnosti ISVS

Kľúčovým problémom informačnej a kybernetickej bezpečnosti je nedostatok kvalifikovaných odborníkov. Štát potrebuje špecialistov na informačnú/kybernetickú bezpečnosť nasledujúceho zamerania

1. informatikov (bezpečnostní správcovia systémov a sietí, vývojári bezpečnostných riešení, operátori bezpečnostných systémov, analytici, členovia CSIRT-ov,...)
2. manažérov (bezpečnostní manažéri rôznych úrovní)
3. audítorov (audítorov bezpečnosti informačných systémov)
4. informaticky vzdelaných právnikov (európska a slovenská legislatíva, vnútorná legislatíva organizácií, ochrana osobných údajov, autorké práva, počítačová kriminalita, vyšetrovatelia, prokurátori, advokáti a sudcovia a i.)
5. učiteľov/lektorov informačnej/kybernetickej bezpečnosti pre žiakov, študentov stredných a vysokých škôl a dospelých,
6. výskumníkov pracujúcich v informačnej a kybernetickej bezpečnosti (kryptológia, informačné systémy, vzdelávanie detí a dospelých, siete, právne vedy, psychológia, sociológia, a i.)
7. novinárov.

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 IB a KB, 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, 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 IB&KB, ochrana vlastných systémov, vnútorná legislatíva, školenia pracovníkov, budovanie bezpečnostného povedomia a špeciálne úlohy závisiace od poslania organizácie).

U vyššie uvedených špecialistov na IB/KB 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 informačnej/kybernetickej bezpečnosti štátu mimoriadne dôležité, ale takýchto ľudí nie je možné pripravovať štandardným spôsobom.

Ucelený prehľad o potrebách, súčasnom počte a rozmiestnení odborníkov na informačnú/kybernetickú bezpečnosť nie je k dispozícii. Centrálne potreby nezávisia od veľkosti štátu a dajú sa orientačne odhadnúť na základe porovnania s podobnými organizáciami v zahraničí, napr. nemeckým Spolkovým úradom pre informačnú bezpečnosť, ktorý 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 (pozrieť presnú citáciu) odhaduje, že v roku 2020 bude potrebovať 350.000 špecialistov na IB/KB. 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 IB MF SR a činnosti CSIRT.SK, na Slovensku je nedostatok kvalifikovaných špecialistov na IB/KB 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. Prehľad kapacít je v prílohe (kapacity)

## Zhrnutie stavu informačnej a kybernetickej bezpečnosti v SR

**Dlhodobá stratégia a jej realizácia.** Aktuálnu štátnu stratégiu predstavuje Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020, rozpracovaná v Akčnon 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 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 informačnú/kybernetickú bezpečnosť reálne koordinoval. NBÚ SR sa zaoberalo len vybranými aspektami kybernetickej bezpečnosti a na plnenie úloh v potrebnom rozsahu nemá potrebné odborné kapacity a kompetencie. Návrh zákona o kybernetickej bezpečnosti je zameraný len na implementáciu Smernice NIS[[18]](#footnote-18) a nerieši problémy informačnej bezpečnosti, špecifikované legistatívnym zámerom zákona o informačnej bezpečnosti. Bez takého zákona nie je možné skoordinovať činnosť štátnych orgánov a zabezpečiť potrebnú súčinnosť majiteľov neštátnych systémov a sietí. Legislatíva taktiež nezohľadňuje to, že v kybernetickom priestore prebiehajú aktivity rozsahom a charakterom pripomínajúce vojenské operácie a že je potrebné zosúladiť ochranu (civilnú) a obranu (vojenskú) slovenského kybernetického priestoru.

**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.

**Vzdelávanie a výskum.**

**Zahraničná spolupráca.**

# Priority

## Kybernetická bezpečnosť v Národnej koncepcii informatizácie verejnej správy Slovenskej republiky

Kybernetická bezpečnosť je uvedená ako jedna z priorít informatizácie verejnej správy. V Národnej koncepcii informatizácie verejnej správy Slovenskej republiky (ďalej len „NKIVS“) je medzi požiadavkami na rozvoj informatizácie verejnej správy aj požiadavka centrálnej správy kybernetickej bezpečnosti nasledovne:

Z pohľadu bezpečnosti je dôraz kladený v prvom rade na zavedenie centrálnej a jednotnej správy kybernetickej bezpečnosti a zavedenia výkonu kybernetickej bezpečnosti na všetkých úrovniach a v rámci všetkých organizácií verejnej správy.

Ako priorita je kybernetická bezpečnosť popísaná ako:

Zaistenie ochrany národného kybernetického priestoru tvoreného prepojenými informačnými a komunikačnými systémami, časťami riadiacich a prevádzkových systémov, inteligentnými zariadeniami (v rámci IoT) naprieč celým spektrom vybudovanej technologickej infraštruktúry štátu predstavuje dlhodobý kľúčový cieľ, osobitne zohľadnený aj v rámci programového obdobia 2014-2020. Všetky základné ciele stanovené pre cieľovú architektúru 2020 sú kriticky závislé od dôveryhodného a bezpečného prostredia, v ktorom budú prevádzkované, a ktorým budú zároveň chránené. Súčasné paradigmy v oblasti informatizácie, zachytené aj v NKIVS, ako je otvorenosť riešení, vysoké požiadavky na transparentnosť, zdieľanie údajov naprieč inštitúciami, agilný vývoj, outsourcing, prevádzka v cloude - v kombinácii s rastúcou závislosťou verejnej správy na spoľahlivo fungujúcich informačných systémoch v národnom kybernetickom priestore, kladie nové výzvy na riešenia v oblasti kybernetickej bezpečnosti.

Stratégia riešenia v oblasti ochrany systémov v kybernetickom priestore sa zameriava najmä na šírenie najlepších praktík a aplikovanie medzinárodne platných a uznávaných štandardov a metodík v oblasti bezpečnosti z centrálnej úrovne. Vytvorí sa tak základ pre prácu expertných skupín zameraných na reálny výkon činností potrebných pre zaistenie bezpečnosti, či už v rámci informačných a komunikačných systémov verejnej správy, v rámci ochrany kritickej infraštruktúry štátu alebo v bezpečnosti inteligentných zariadení.

Nové riešenia pre kybernetickú bezpečnosť vo verejnej správe budú budované na nasledovných zásadách:

- silná štandardizácia riešení, najmä v zmysle určených bezpečnostných opatrení pre typizované situácie,

- stanovia sa minimálne nevyhnutné požiadavky na bezpečnosť, tak z dôvodu efektívnosti investícií, ako aj pre minimalizáciu obmedzení vyplývajúcich z nasadených bezpečnostných opatrení,

- dôsledné sa odmieta princíp „security by obscurity“, utajené a neprístupné budú iba nevyhnutné záležitosti,

- realizuje sa systematická podpora používateľov pri bezpečnom používaní elektronických služieb,

- dôsledne pristúpime k riešeniu rizík prameniacich zo zdieľanej zodpovednosti za prevádzku integrovaného informačného systému verejnej správy.

Pre zaistenie zodpovedajúcej právnej sily a vhodných podmienok pre vymáhanie požiadaviek stanovených pre oblasti bezpečnosti je potrebné prijať aj právne predpisy v oblasti kybernetickej bezpečnosti a novelizovať existujúce legislatívne predpisy v oblasti riadenia a správy informačnej bezpečnosti zohľadňujúc aj novú smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

## Kybernetická bezpečnosť v Operačnom programe integrovaná infraštruktúra

Kybernetická bezpečnosť je taktiež súčasťou Operačného programu integrovaný infraštruktúry (ďalej len „OPII“), konkrétne prioritnej osi č.7 Informačná spoločnosť ako špecifický cieľ č.7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti. Uvedený špecifický cieľ je definovaný týmto spôsobom:

Informačná a kybernetická bezpečnosť je dynamicky sa vyvíjajúcim odvetvím, ktoré musí neustále reagovať na nové výzvy. V súvislosti s narastajúcou občianskou aj podnikateľskou aktivitou v digitálnom priestore bude nutné postupovať s ohľadom na opatrenia obsiahnuté v Stratégii kybernetickej bezpečnosti EÚ prezentovanej vo februári 2013. Informačné systémy a siete vyvíjané alebo aktualizované v nasledujúcom období budú posudzované z pohľadu naplnenia zadefinovaných bezpečnostných cieľov a súladu s existujúcou aj budúcou legislatívou.

Budú sa implementovať a vylepšovať opatrenia na riadenie bezpečnostných rizík, predovšetkým pre systémy verejnej správy patriace do kritickej infraštruktúry. Zvýši sa transparentnosť informovania o bezpečnostných incidentoch jednotlivcov, ktorých osobné údaje boli stratené, ukradnuté alebo pozmenené. Celkovo sa zvýši dôvera v digitálny priestor a povedomie o spôsobe riešenia kybernetických útokov. Prispeje k tomu tiež nasadenie platformy pre zber údajov a opatrení a pre posielanie výstrah súvisiacich s kybernetickou bezpečnosťou. Táto platforma bude interoperabilná s európskym riešením a napojená na Európske centrum pre kybernetický zločin.

Pričom táto priorita má byť naplnená prostredníctvom nasledovných aktivít:

- Vytvorenie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných

incidentov

- Zabezpečenie kritickej infraštruktúry

- Zavádzanie európskej stratégie pre kybernetickú bezpečnosť

## Ciele (návrh PS)

– riešenie problémov / priorít v strednodobom horizonte + stručná SWOT tohto riešenia (high level uroveň)

# Riešenia

Stav informačnej/kybernetickej bezpečnosti v Slovenskej republike 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 informačnej a kybernetickej bezpečnosti 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 IB/KB v SR a zvlášť bezpečnosti ISVS nasledujúci postup

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

V nasledujúcich častiach stručne rozoberieme uplatňovanie navrhovaného postupu

## Koncepcia, legislatíva, kompetencie

V súčasnosti je v legislatívnom procese návrh zákona o kybernetickej bezpečnosti a pripravuje sa zákon o výkone správy v oblasti informačných technológií. Návrh zákona o kybernetickej bezpečnosti implementuje Smernicu NIS, ale nerieši problémy informačnej bezpečnosti štátu, ktoré sú definované v legislatívnom zámere zákona o informačnej bezpečnosti. Pripravovaný zákon o výkone správy v oblasti informačných technológií je zameraný len na IKT v pôsobnosti orgánov verejnej správy. Keďže oba tieto návrhy sú už v pokročilom štádiu, bude potrebné ich analyzovať a

1. zosúladiť kompetencie ohľadne ISVS (PS a j tento dokument predpokladá, že VPA pre oblasť ISVS bude ÚPVII)
2. zaviesť bezpečnostnú kategorizáciu ISVS a definovať základné požiadavky na ochranu ISVS,
3. vytvoriť právny rámec pre organizačné zaistenie bezpečnosti ISVS (ÚPVIIvytvorí a bude udržiavať súbory opatrení pre jednotlivé kategórie ISVS, vydávať bezpečnostné štandardy, robiť bezpečnostnú certifikáciu a pod)

V dlhšom časovom horizonte bude potrebné analyzovať

1. Povinnosti v IB/KB, ktoré pre Slovensko vyplývajú z právnych aktov EÚ,
2. Zákony a podzákonné normy SR, týkajúce sa IB/KB (ISVS a celého virtuálneho priestoru SR) a identifikovať nezrovnalosti, duplicity a iné nedostatky a navrhnúť ich zosúladenie;
3. problémy, ktoré je na zaistenie IB/KB v SR potrebné riešiť, ale chýba na to právny základ.

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

Opäť rovnaký problém – kto to bude robiť, organizovať a kto presadí navrhované riešenia?

## Predpokladané riadenie/koordinácia zabezpečenia slovenského virtuálneho priestoru

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. Ale aj na výkon operatívy bude potrebný dostatočne „silný“ politický orgán (Národná autorita) podporovaný potrebnými odbornými kapacitami. (Bude potrebovať koordinovať spoluprácu s MV SR, MS SR, MZV SR, MF SR, UPVII, MŠ, NBÚ, MO SR, SIS a i.) buď na úrovni NBU, príp. MO / MV SR.

Národná autorita zodpovedná za informačnú/kybernetickú bezpečnosť SR potrebuje odborný koordinačno-koncepčno-výkonný orgán[[19]](#footnote-19) (pracovný názov – Komisia pre IB/KB) so zastúpením relevantných strán (štátne orgány, akademický sektor, súkromná sféra), ktorý by

1. mal prehľad o stave kybernetickej/informačnej bezpečnosti na Slovensku (spracovávanie dostupných informácií, časom vypracovanie metodiky na získavanie relevantných informácií a formu reportingu komu? Vláde, Bezpečnostnej rade?)
2. poskytoval odborné stanoviská pre Vládu SR (analógia vzťahu ENISA a Európskej komisie)
3. sledoval projekty a iné aktivity EU (v minulosti napr. FIDIS, epSOS, STORK; príprava direktív a nariadení, činnosť odborných komisií pri orgánoch EÚ a pod.), zastúpenie SR v odborných orgánoch EU,
4. rozvíjal/inicioval/podporoval odbornú činnosť v oblasti informačnej bezpečnosti zameranú na riešenie aktuálnych a perspektívnych problémov,
5. zosúladil[[20]](#footnote-20) existujúcu legislatívu, sledoval konzistentnosť pripravovaných zákonov a pod-zákonných noriem, budoval konzistentnú terminológiu,
6. posudzoval projekty a aktivity celoslovenského rozsahu zamerané na informačnú/kybernetickú bezpečnosť
7. a neskôr plnil aj iné úlohy v kybernetickej/informačnej bezpečnosti.

Komisia pre informačnú/kybernetickú bezpečnosť by mala mať okrem koordinačnej zložky mala mať aj stále odborné kapacity (pracovné skupiny) schopné riešiť dlhodobé úlohy. Momentálne existujú pracovné skupiny

1. Výbor pre kybernetickú bezpečnosť pri Bezpečnostnej rade
2. Komisia pre kybernetickú bezpečnosť Riaditeľa NBÚ
3. pracovná skupina pre kybernetickú bezpečnosť pri ÚPVII
4. pracovné skupiny pre kybernetický zločin, kritickú infraštruktúru (MV SR?)
5. vieme o iných?

ktoré majú príbuznú problematiku, v niektorých pôsobia tí istí ľudia. Tieto by sa mohli aspoň skoordinovať, niektoré možno perspektívne zlúčiť.

## Zabezpečenie základnej úrovne ochrany virtuálneho priestoru SR

Z centrálnej úrovne (autorita zodpovedná za informačnú/kybernetickú bezpečnosť SR) je na zabezpečenie aspoň základnej úrovne ochrany slovenského virtuálneho priestoru vo všeobecnosti a zvlášť pre bezpečnosť ISVS možné v krátkom čase spraviť nasledujúce kroky:

1. dohodnúť pokrytie (ISVS, celého priestoru?) existujúcimi CSIRT-ami (existujú aj iné akcieschopné útvary podobného zamerania, ktoré by sa na týchto úlohách mohli podieľať?)
2. definovať minimálne požiadavky na systémy a siete (v podobe štandardov ISVS) a súbor opatrení (baseline), ktorého implementácia stačí na splnenie minimálnych požiadaviek,
3. kontrolovať dodržiavanie minimálnych požiadaviek (audit),
4. sledovať nové hrozby a zraniteľnosti a aktualizovať minimálne požiadavky a súbor základných opatrení (baseline).

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 a tiež dostatočná odborná kapacita.[[21]](#footnote-21) Audit bezpečnosti informačných systémov je bežne používaným nástrojom kontroly dodržiavania štandardov, pri ktorom sa dajú dobre využiť externí auditori. Bude však potrebné špecifikovať požiadavky na audit, ako aj požiadavky na kvalifikáciu audítorov. Pozri príloha Audit. 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. Príloha Klasifikácia systémov a informácií.

Jedným z funkčných útvarov CSIRT je vojenský CSIRT. Okrem jeho zapojenia do operatívnej činnosti pri ochrane slovenského virtuálneho priestoru/ISVS je potrebné vyriešiť aj vzťah medzi ochranou a obranou kybernetického/virtuálneho priestoru (kompetencie, koordinácia civilných a vojenských zložiek, vyhlásenie a odvolanie stavu kybernetického ohrozenia a pod.)

1. akú predstavu o kybernetickej obrane má MO SR?

## Budovanie odborných kapacít

Je prvoradá úloha, lebo bez kvalifikovaných odborníkov sa informačná/kybernetická bezpečnosť nedá zaistiť. 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. Národná autorita pre budovanie odborných kapacít zabezpečí

1. identifikovanie potrieb (koľko a akých odborníkov SR/štátna sféra potrebuje)
2. špecifikáciu potrebných znalostí, zručností a schopností pre jednotlivé špecializácie (neskôr aj formálnu definíciu špecializácií)
3. identifikácia nositeľov potrebného know-how použiteľných na školiacu činnosť, možné školiace kapacity v zahraničí (pre oblasti, kde nemáme dostatočne kvalifikovaných vlastných ľudí)
4. stanovenie priorít – akých ľudí potrebujeme vyškoliť najskôr
5. spustenie projektu vzdelávania zameraného na vybudovanie výučbových kapacít a spustenie vzdelávania v informačnej/kybernetickej oblasti (revízia študijných materiálov MF SR a vydanie opraveného a doplneného vydania, terminologický slovník v informačnej bezpečnosti, )

Súčasne s týmito aktivitami je možné

1. vybudovať centrum excelencie pre IB/KB (výskum, expertná činnosť, vzdelávanie) – základ – Spoločné pracovisko Eset, UK, STU,
2. riešiť stabilizáciu odborníkov na IB/KB v štátnych inštitúciách
3. podporovať vzdelávanie v IB/KB v rámci existujúcich programov na vysokých školách (informatici, manažéri, právnici), nové špecializácie, postgraduálne vzdelávanie, celoživotné vzdelávanie.

Neskôr je možné vypracovať[[22]](#footnote-22), ale **najmä zaviesť do praxe** komplexný systém vzdelávania v IB/KB. Pre štátne organizácie z hľadiska informačnej/kybernetickej bezpečnosti rozlišujeme štyri skupiny zamestnancov v štátnych inštitúciách, a to vedúci pracovníci, manažéri informačnej/kybernetickej bezpečnosti, 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 roka je možné spustiť vzdelávanie pre vedúcich pracovníkov a manažérov informačnej/kybernetickej bezpečnosti. Stanovíme povinnosť školenia v IB/KB aspoň pre zamestnancov štátnych inštitúcií? Podrobnejší návrh systému vzdelávania a krokov potrebných na jeho zavedenie je uvedený v prílohe xxx

## Zavedenie systému pre riadenie kybernetickej a informačnej bezpečnosti (Security Governance) vo verejnej správe

Základným dôvodom nedostatočnej úrovne kybernetickej a informačnej bezpečnosti je absencia centrálnej autority v tejto oblasti, ktorá by mala dostatočné právomoci pre presadzovanie strategických zámerov v tejto oblasti.

V súlade s všeobecným zámerom informatizácie a to postupnou centralizáciou informačných systémov a ich prevádzka v cloudovom prostredí je potrebné adekvátne tomu vytvoriť aj proces pre postupné centralizovanie riadenia kybernetickej a informačnej bezpečnosti vo verejnej správe a tomu korešpondujúci inštitucionálny rámec.

Za týmto cieľom je potrebné vytvoriť organizáciu, ktorá by metodicky zastrešovala riadenie kybernetickej a informačnej bezpečnosti naprieč celou verejnou správou **Centrum pre kybernetickú a informačnú bezpečnosť**.

Centrum pre kybernetickú a informačnú bezpečnosť (ďalej len „Centrum“) bude plniť nasledovné úlohy:

* Vypracovanie metodického rámca pre riadenie kybernetickej a informačnej bezpečnosti vo verejnej správe (rola, zodpovednosti, metodické riadenie)
* Komunikácia so zúčastnenými stranami v oblasti kybernetickej bezpečnosti
* Vytvorenie platformy pre publicitu a osvetu kybernetickej bezpečnosti a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy a verejnosti
* Vytvorenie jednotného (unifikovaného) rámca bezpečnostných opatrení pre informačné systémy verejnej správy na princípoch efektivity a primeranosti.
* Dopracovanie a pravidelná aktualizácia detailných metodických postupov pre implementáciu bezpečnostných opatrení
* Vytvorenie rámca požiadaviek a postupov pre implementáciu a koordináciu požiadaviek GDPR regulácie vo verejnej správe
* Periodické vyhodnocovanie úrovne implementovaných bezpečnostných opatrení na úrovni celej verejnej správy.
* Presadzovanie určených bezpečnostných opatrení v organizáciách verejnej správy
* Vytvorenie sady kľúčových ukazovateľov efektivity opatrení kybernetickej bezpečnosti
* Návrh systému (forma, periodicita, spôsob) pre sústreďovanie a vyhodnocovanie kľúčových ukazovateľov efektivity opatrení kybernetickej bezpečnosti v rámci verejnej správy.
* Vytvorenie automatizovaného nástroja (portál) na hodnotenie, alebo tzv. self-assessment, úrovne implementovaných bezpečnostných opatrení v jednotlivých organizáciách verejnej správy, ako aj na zber kľúčových ukazovateľov efektivity bezpečnostných opatrení.
* Zabezpečenie kontinuálneho zlepšovanie bezpečnostných opatrení pre informačné systémy verejnej správy prostredníctvom získavania spätnej väzby a vyhodnocovania.
* Vytvorenie a koordinácia inštitucionálneho rámca (podmienky, riadenie, monitorovanie, kontrola) pre financovanie celkového zvýšenie kybernetickej bezpečnosti a odolnosti jednotlivých informačných systémov verejnej správy.

Veľmi dôležitým poslaním tejto organizácie by bolo aj postupná identifikácia tých aktivít a činností v procesoch riadenia KIB, ktoré je možné prevádzkovať pre viacero organizácií a inštitúcie 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 kybernetickej a informačnej bezpečnosti 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 sa 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.

V ďalších kapitolách budú podrobne rozpracované vymenované úlohy a navrhovaný spôsob ich realizácie.

## Vypracovanie metodického rámca pre riadenie kybernetickej a informačnej bezpečnosti vo verejnej správe

### Metodický rámec riadenia kybernetickej a informačnej bezpečnosti vo verejnej správe

Hlavnou úlohou Centra pre kybernetickú a informačnú bezpečnosť je revízia, aktualizácia, dopracovanie metodiky riadenia informačnej bezpečnosti na všetkých úrovniach verejnej správy ako jej exekúcia. Systém riadenia KIB by mal byť centralizovaný s metodickým riadením bezpečnostných pracovníkov na jednotlivých ústredných orgánoch štátnej správy.

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

#### Organizačná štruktúra Centra pre kybernetickú a informačnú bezpečnosť

V navrhovanej organizačnej štruktúre by mala byť v prvom rade zadefinovaná rola Chief Information Security Officera (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.

#### Organizačná štruktúra riadenia kybernetickej a informačnej bezpečnosti 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 informačnej bezpečnosti 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 (Ďalej aj „MIB“), ktorý je vlastníkom procesu riadenia a zaisťovania KIB na ÚOŠS.
* Stanovenú zodpovednosť realizuje MIB prostredníctvom:
  + organizačného útvaru „kybernetická a informačná bezpečnosť“
  + 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 MIB 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 MIB k Centru pre kybernetickú a informačnú bezpečnosť:

* MIB bude metodicky riadený CISO pre verejnú správu (tzv. dotted line reporting).
* Centrum bude poskytovať MIB metodickú podporu, odbornú podporu, podporu pri riešení bezpečnostných incidentov.
* Centrum bude slúžiť ako eskalačný subjekt
* MIB 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 ÚOŠS 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 MIB a  organizáciám podriadeným ÚOŠS.

Pre nadrezortné informačné systémy t.j. informačné systémy verejnej správy, ktoré hierarchicky integrujú spoločné časti jednotlivých informačných systémov verejnej správy, ktoré sú v pôsobnosti iných správcov, do hierarchicky vyššieho informačného systému verejnej správy bude potrebné jednoznačnej správcu, ktorý bude vykonávať v oblasti riadenia KIB obdobné úlohy ako ÚOŠS (definovaná pozícia MIB, 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 informačnej/kybernetickej bezpečnosti, 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 informačnej/kybernetickej bezpečnosti 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 IB/KB do výučby na stredných a základných školách (príprava e-learningových materiálov), prípadne vydávať metodické materiály IB/KB pre dospelých. Konkrétne školenia zamestnancov v IB/KB, musia robiť lokálni manažéri IB/KB (alebo lektori), aby vo vzdelávaní dokázali aplikovať všeobecné princípy na konkrétne podmienky organizácie.

## 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 GDPR“), 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 bude 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 zohľadnené aj pri definovaní bezpečnostných opatrení pre informačné systémy verejnej správy.

## Periodické vyhodnocovanie úrovne implementovaných bezpečnostných opatrení

Periodické vyhodnocovanie úrovne implementovaných bezpečnostných 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.

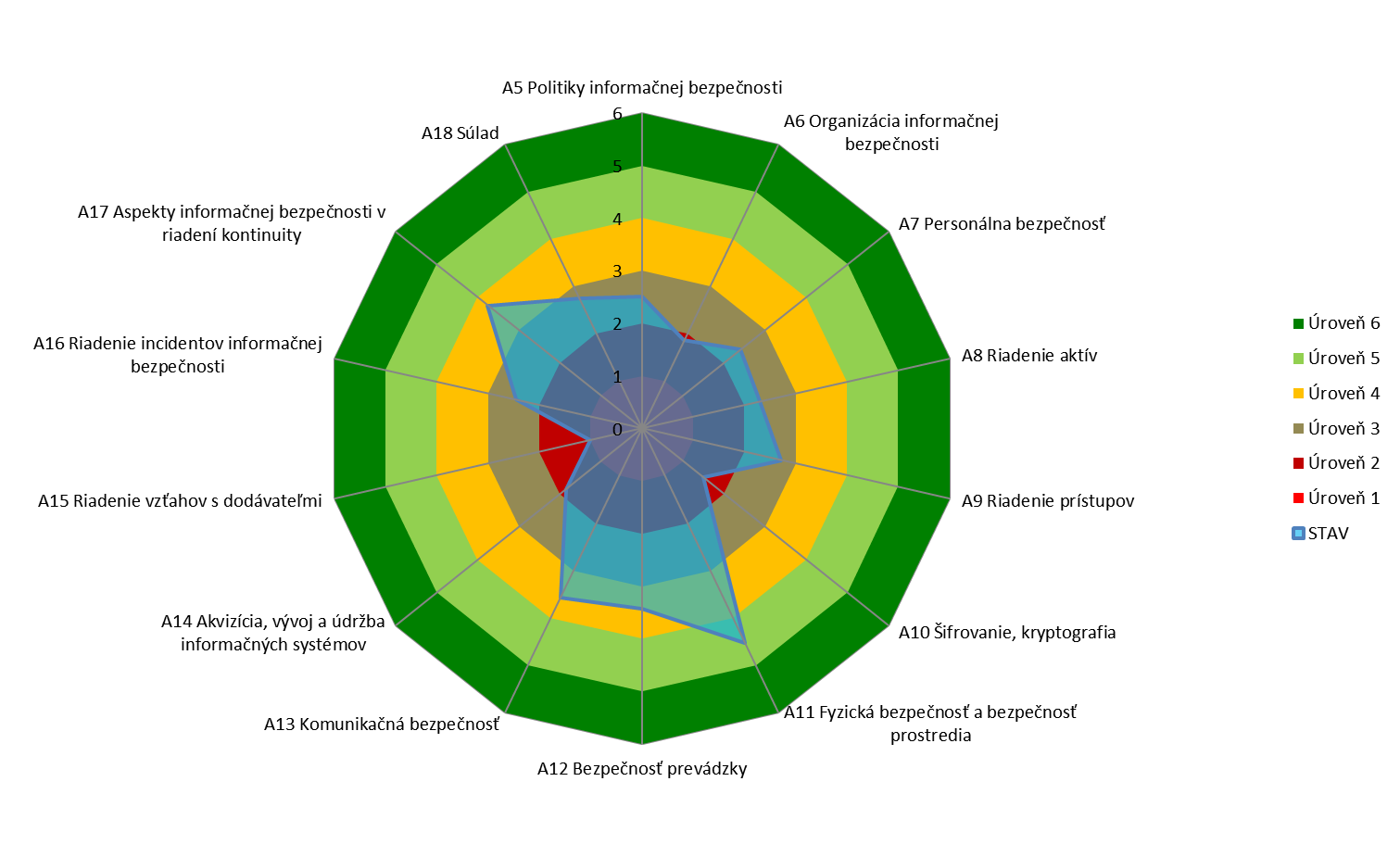
Cieľom nie je sankcionovanie, ale dosiahnutie reálneho stavu implementovaných opatrení a tým adekvátnu úroveň KIB vo verejnej správe (prípadne kritickej infraštruktúre). Významným prínosom bude taktiež ich neustále vylepšovanie paralelne s vývojom situácie v kybernetickej bezpečnosti ako aj v súlade 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.

Kritériami pre stanovenie aktuálnej úrovne opatrení môžu byť:

* Čiastočné alebo plnohodnotné uplatnenie metód opatrenia
* Stupeň formalizácie procesu k danému opatreniu
* Detailný popis rolí a zodpovedností
* Celkové začlenenie procesu, výstupov do procesu riadenia rizík
* Technologická podpora opatrenia
* Personálna podpora výkonu opatrenia
* Periodické preskúmavanie efektivity opatrenia

Príklad vyhodnocovania implementovaných opatrení je na nasledovnom obrázku. Vyhodnocované môžu byť jednotlivé organizácie, alebo celkovo celá verejná správa (prípadne kritická infraštruktúra).



Vyhodnocovanie opatrení musí korešpondovať so štruktúrou ich metodologického rozpracovania. Zároveň však musí byť dostatočne flexibilné vzhľadom na individuálne potreby organizácií so zachovaním adekvátneho stupňa unifikácie.

Hodnotenie úrovne implementovaných opatrení bude prebiehať prostredníctvom centrálneho adekvátne zabezpečeného nástroja (portálu), ktorý bude v správe Centra. Portál bude slúžiť aj na publikáciu opatrení a metodík ako aj na výmenu informácií medzi Centrom a jednotlivými organizáciami. Obdobne môžu byť prostredníctvom tohto nástroja vyhodnocované aj opatrenia určené pre prvky kritickej infraštruktúry.

Vyhodnocovanie bude vykonávané pravidelne v určitých časových obdobiach. V úvode, po zavedení unifikovaného rámca bezpečnostných opatrení, je potrebné pre zachytenie trendu vyhodnocovať progres častejšie napr. na štvrťročnej báze od určitého stanoveného dátumu.

Pri úvodnej harmonizácii oparení KIB bude potrebné počítať so zvýšenou podporou pre organizácie ako aj s vytvorením centralizovaného plánu implementácie opatrení vo verejnej správe. To poskytne možnosť aj pre výber najvhodnejšej technológie, transfer skúseností medzi rezortmi ako aj možnosť dosiahnutia špeciálnych dohôd, prípadne aj zliav u výrobcov a ďalších úspor.

Centrum bude vykonávať koordináciu, poskytovať analytickú a inú podporu (negociácie s dodávateľmi, eskalačný proces a pod.) ako aj prostredníctvom portálu sústreďovať relevantné informácie o situácii v KIB. Portál bude slúžiť aj na evidenciu bezpečnostných incidentov každej organizácie (v koordinácii s CISRT.SK).

Centrum bude taktiež oprávnené vykonávať audity stanovených bezpečnostných opatrení v organizáciách, prípadné iné kontrolné aktivity. CISO bude v pravidelných intervaloch napr. každých šesť mesiacov vyhodnocovať situáciu a výsledky reportovať na vyššiu úroveň.

## Vytvorenie a vyhodnocovanie kľúčových ukazovateľov efektivity implementovaných bezpečnostných opatrení.

Okrem vyhodnocovania samotnej úrovne implementovaných opatrení je pre zaistenie kontinuálneho rozvoja, najvyššej možnej efektivity ako aj pre dosiahnutie úspory zdrojov potrebné vyhodnocovať pravidelne aj účinnosť implementovaných opatrení.

Pre vyhodnocovanie účinnosti bezpečnostných opatrení bude vypracovaný súbor kľúčových merateľných ukazovateľov efektivity (KPI), ktoré budú merané v pravidelných časových intervaloch.

Základný súbor musí obsahovať minimálne KPI pre nasledovné oblasti:

* Proces posúdenia rizík
* Proces zvyšovania bezpečnostného povedomia
* Riadenie bezpečnostných incidentov
* Proces manažmentu zraniteľností
* Proces bezpečnostného testovania a kontrolných aktivít
* Proces bezpečnostného monitorovania
* Proces riadenia kontinuity

Príklady kľúčových ukazovateľov sú nasledovné:

* Percentuálny podiel prvkov informačno-komunikačnej infraštruktúry systémov, ktoré boli zahrnuté do procesu posúdenia rizík
* Percentuálny podiel rizík s vysokou závažnosťou
* Percentuálny pomer zamestnancov, ktorý absolvujú pravidelne tréning zameraný na zvyšovanie bezpečnostného povedomia
* Počet bezpečnostných incidentov podľa vybranej kategórie za stanovené časové obdobie
* Priemerná doba detekcie incidentu
* Priemerný čas obnovy po incidente
* Percentuálny počet systémov pokrytých manažmentom zraniteľností
* Vykonávanie penetračného testovania
* Priemerný počet nedostatkov z kontrolných aktivít za určené obdobie
* Percentuálny podiel nelegitímnych sieťových prenosov
* Percento informačných systémov pokrytých plánmi kontinuity

Predpokladá sa, že KPI pre meranie efektivity bezpečnostných opatrení sa budú postupne vyvíjať meniť a dopĺňať. Ukazovatele budú sústreďované pomocou portálu Centra, kde sa tento proces môže postupne automatizovať.

## 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 informačnej/kybernetickej bezpečnosti, rozsah a stúpajúca frekvencia kybernetických útokov. Slovensko, 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 Slovensko len v minimálnej miere zapája odborných projektov, resp. podieľa na práci pracovných skupín EÚ, čím sa o.i. ochudobňujeme o možnosť poznať v predstihu pripravované opatrenia EÚ, ktorým sa budeme musieť prispôsobiť. Národná autorita (v spolupráci s MZV SR) bude musieť

1. identifikovať (pracovné) orgány EÚ, NATO, prípadne iných medzinárodných organizácií ktoré riešia informačnú/kybernetickú bezpečnosť 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,
2. prezrieť medzinárodné zmluvy s informaticky vyspelými partnermi a zistiť, či na ich základe nie je možné nadviazať spoluprácu v oblasti IB/KB,
3. určiť, čo by sme od zahraničných partnerov potrebovali a čo im môžeme ponúknuť,
4. zaistiť účasť odborníkov v delegáciách, resp. na rokovaniach s potenciálnymi partnermi.
5. vyhodnocovať prínos zmlúv, Memoránd a dohôd pre IB/KB[[23]](#footnote-23).

## Kritické faktory úspechu

#### Riešenie personálneho obsadenia odborných pozícií

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

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

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

Pre stimulovanie motivácie je nevyhnutné aby vyššie platové ohodnotenie zamestnancov nebolo dostupné automaticky. Bezpečnostným špecialistom by bolo umožnené iba po splnení transparentne stanovených kvalifikačných, výkonnostných prípadne iných parametrov. Medzi vyhodnocované parametre by mali patriť najmä odborná úroveň, proaktívny prístup, inovatívnosť, tímová spolupráca a pod. Uvedený princíp je možné uplatniť pri diferenciácii junior a senior pozícií. ÚPVII môže prostredníctvom svojej koordinačnej roly v príprave IT rozpočtov jednotlivých ÚOŠS kontrolovať, či pre dané kompetencie / procesy sú alokované potrebné zdroje.

Dôležitým faktorom pre nájdenie optimálneho modelu bude aj činnosť 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 MIB 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.

Financovanie školení a vzdelávania špecialistov KIB môže byť financované z iných operačných programov (napr. OP EVS), 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 tými 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.

#### Komunikácia so zúčastnenými stranami v oblasti kybernetickej bezpečnosti

Centrum by malo slúžiť ako centrálna komunikačná platforma pre všetky zúčastnené strany v oblasti KIB, ktorými sú najmä:

* Profesijné združenia
* Organizácie verejnej správy
* Podnikateľské subjekty (banky, telekomunikačný operátori, priemyselné podniky a pod.)
* Výrobcovia, dodávatelia technológií
* Občania

V rámci komunikácie budú v Centre podľa potreby zriaďované rôzne platformy, v rámci ktorých budú diskutované oblasti KIB (napr. FIN fórum, TELCO fórum, ICS/SCADA fórum a pod.) .

Základným cieľom je výmena informácií a skúseností medzi zúčastnenými stranami, identifikácia možností vzájomnej spolupráce a podpory medzi privátnym a verejným sektorom, prípadne riešenie aktuálnych problémov.

Dôležitou môže byť komunikácia s výrobcami technológií, kde môžu byť prezentované nové technológie, detailne rozobrané bezpečnostné funkcionality a nastavenia, vykonávané testovanie (napr. CSIRT.SK) a pod.

Centrum bude zodpovedné aj za komunikáciu s partnerskými organizáciami v EÚ (napr. ENISA) a taktiež bude reprezentovať verejnú správu na rôznych konferenciách a iných podujatiach týkajúcich sa KIB.

# Ďalší postup / úlohy

## Vytvorenie platformy pre publicitu a osvetu kybernetickej bezpečnosti a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy

Medzi kľúčové predpoklady kontinuálneho zlepšovania úrovne KIB je potrebné dosiahnuť u zamestnancov verejnej správy dostatočnú úroveň bezpečnostného povedomia. Rovnako je nevyhnutné efektívnym spôsobom zvýšiť bezpečnostné povedomie občanov.

### Zvyšovanie bezpečnostného povedomia u zamestnancov verejnej správy

Centrum by malo vytvoriť platformu pre periodickébezpečnostné vzdelávania pre všetkých zamestnancov štátnej správy (prípadne aj samosprávy) formou e-learningu. Zvyšovanie bezpečnostného povedomia by malo byť zamerané najmä na:

* Celkový prehľad o stave a aktuálnych trendoch v kybernetickej bezpečnosti
* Sociálne inžinierstvo a jeho formy
* Používanie bezpečného hesla
* Druhy škodlivých kódov
* Bezpečné zaobchádzanie s emailom
* Bezpečnosť v sociálnych sieťach
* Ochrana informácií a osobných údajov
* Bezpečnosť na internete
* Bezpečnosť mobilných zariadení
* Ďalšie bezpečnostné zásady

Všetci zamestnanci by mali absolvovať školenie spojené s testovaním aspoň jeden krát ročne a o jeho absolvovaní by mali dostať osvedčenie. V ďalšom kroku je možné podmieniť vytvorenie prístupu nových zamestnancov do informačných systémov verejnej správy absolvovaním školenia a pod.

Ďalej bude možné uvedenú platformu rozvinúť o kurzy pre špecialistov KIB (napr. kurzy aplikačnej bezpečnosti, bezpečnosti databáz a pod.).

Zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy výrazne pomôže znížiť ich negatívny postoj k implementovaným bezpečnostným opatreniam a v konečnom dôsledku bezpečné zaobchádzanie s informačnými technológiami prenesú aj do svojho súkromného života.

### 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. 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.

## Šírenie osvety, marketingová a mediálna podpora

### Webstránka, online marketing, sociálne médiá

Súčasťou zvyšovania bezpečnostného povedomia je aj šírenie osvety. Okrem webstránky Centra bude pre oblasť KIB vytvorená aj komplexná stratégia online marketingu, práca so sociálnymi sieťami a pod. Vyššie spomínaný multimediálny obsah pre zvyšovanie bezpečnostného povedomia môže byť publikovaný aj prostredníctvom sociálnych médií, kde bude mať Centrum vytvorenú vlastnú stránku (Youtube kanál, Facebook stránka apod.).

Sociálne médiá budú slúžiť aj na komunikáciu s verejnosťou (napr. v prípade masového šírenia sa škodlivého kódu a pod.), kde bude možná veľmi efektívna a rýchla komunikácia s verejnosťou.

### Security Roadshow

Druhou možnosť pre propagáciu KIB ako aj vytvoreného vzdelávacieho portálu je možnosť uskutočnenia Security Roadshow. Táto aktivita by mohla byť uskutočnená aj v spolupráci (prípadne spolufinancovaním) s inými subjektami napr. bankmi, telekomunikačnými operátormi, ktorý majú rovnako záujem šíriť osvetu a zvyšovať bezpečnostné povedomie svojich zákazníkov t.j. väčšiny populácie. Uvedený formát by mohol poslúžiť aj ako príklad spolupráce verejného a privátneho sektoru v oblasti KIB.

## Vytvorenie inštitucionálneho rámca (podmienky, riadenie, monitorovanie, kontrola) pre spolufinancovanie

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 napr. OPII a OP EVS.

Uvedené podmienky musia odrážať špecifiká implementácie bezpečnostných opatrení, ktoré sú v niektorých prípadoch odlišné od špecifík informačných systémov kde je potrebné naplnenie špecificky iných kritérií.

|  |  |
| --- | --- |
| Ú.Leg.3. Štandardy IB/KB | |
| Názov | Vypracovať návrh štandardov IB/KB pre ISVS |
| Špecifikácia | Vypracovať prehľad ISO a iných IB/KB štandardov a oblastí, ktoré pokrývajú, prehľad existujúcich štandardov IB/KB relevantných pre ISVS, posúdenie ich aktuálnosti, úplnosti a konzistentosti a návrh špecifikácie (ešte nie textov) štandardov |
| Zdôvodnenie | Bezpečnostné riešenia pre ISVS by mali byť kompatibilné s medzinárodnými štandardami. Z analýzy štandardov vyplynie, ktoré štandardy treba zmeniť, ktoré možno prebrať a ktoré bude potrebné napísať, aby boli všetky oblasti bezpečnosti ISVS dostatočne pokryté. |
| Výstupy | Analýza slovenských aj medzinárodných štandardov IB/KB a návrh na doplnenie, úpravy, zmeny slovenských štandardov |
| Riešiteľ |  |
| Termín | 1 rok |
| Zdroje |  |
| Kooperujúce orgány |  |

|  |  |
| --- | --- |
| **Ú.Edu.1. Vzdelávanie v IB/KB** | |
| Názov | Vypracovanie systému vzdelávania a pilotný projekt vzdelávania v IB/KB |
| 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 IB/KB pre vyššie uvedené kategórie používateľov IKT. |
| Zdôvodnenie | Na zaistenie požadovanej úrovne informačnej/kybernetickej bezpečnosti 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 | UK a STU Bratislava |
| Doba trvania | 2 roky |
| Zdroje |  |
| Kooperujúce orgány | Ministerstvo školstva |
| 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.Gen.1. Prehľad stavu informačnej/kybernetickej bezpečnosti vo verejnej správe SR** | |
| Názov | Vypracovať prehľad stavu IB/KB ISVS alebo v SR raz za 2 roky |
| Špecifikácia | Prehľad bude založený na viacerých informačných zdrojoch:   1. dotazníkom rozposielaným orgánom/organizáciám VS sa bude zisťovať stav zabezpečenia ISVS, organizácia a riadenie informačnej/kybernetickej bezpečnosti v organizácii/rezorte, vlastné hodnotenie úrovne IB/KB v organizácii 2. CSIRT-y (zraniteľnosti, bezpečnostné incidenty, trendy, činnosť) 3. ministerstvá, ústredné orgány (NBÚ SR, MV SR, MS SR SIS,...) |
| Zdôvodnenie | Získanie a udržanie prehľadu o stave, problémoch a trendoch v informačnej/ky-bernetickej bezpečnosti ISVS/alebo SR. Bude sa využívať pre riadenie aktivít na zaistenie IB/KB 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 | 1. dotazníky 2. podklady zo štátnych orgánov 3. podklady z CSIRT-ov 4. financie – spracovanie dotazníka 10.000 eur, ostatné závisí od rozsahu a zložitosti analýzy |
| Kooperujúce orgány | NBÚ SR, CSIRT-y, SIS (?) |
| Poznámka | 1. Budeme zverejňovať celú správu, alebo bude mať utajenú časť? 2. nebudeme niektoré časti správy robiť každý rok? |
| **Ú.Leg.1. Prehľad legislatívy EÚ** | |
| Názov | Vypracovať prehľad legislatívy EÚ relevantnej z hľadiska informačnej/kybernetickej bezpečnosti. |
| Špecifikácia | Prehľad by mal identifikovať úlohy, ktoré Slovensku 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 eu právnymi aktami a závislosti medzi úlohami. |
| Zdôvodnenie | Získanie a udržanie prehľadu o povinnostiach, ktoré SR má v IB/KB vo vzťahu k EÚ, podklad pre slovenskú legislatívu, aj koordináciu aktivít štátnych orgánov SR |
| Výstup | Základný prehľad, a potom  raz ročne buď samostatná správa (podpredsedovi alebo Komisii?) alebo kapitola v správe o stave IB/KB v SR |
| Riešiteľ | buď právnici z ÚPVII, alebo úloha pre PraF UK (odhadovaná zložitosť 1000 hodín práce), príp. externá právna kancelária |
| Termín | 1 rok |
| Zdroje | 1. existujúce prehľady 2. financie 25.000 eur |
| Kooperujúce orgány | Ministerstvo zahraničných vecí SR |

# Prílohy

## Malý výkladový slovník

Terminológia informačnej resp. kybernetickej bezpečnosti sa dynamicky vyvíja a mnohé, dokonca aj základné pojmy, nie sú v medzinárodnej terminológii jednoznačne definované. Slovenská terminológia sa vyvíja živelne a zväčša preberá anglické termíny, v najlepšom prípade ich prekladatelia poslovenčujú alebo prekladajú. Tento dokument vychádza z výkladového slovníka pojmov informačnej bezpečnosti MF SR.

## Prehľad najdôležitejších dokumentov Informačnej a kybernetickej bezpečnosti SR (pracovný názov)

* Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválená uznesením vlády SR č. 570/2008,
* Návrh systému vzdelávania v oblasti informačnej bezpečnosti/kybernetickej bezpečnosti v Slovenskej republike, schválený uznesením vlády SR č. 391/2009,
* Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – 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 Slovenskej republike, 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 Slovenskej republike a Akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády SR,
* Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (ďalej len „Koncepcia“), schválená uznesením vlády SR č. 328/2015,
* [Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky](http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24695), schválená uznesením vlády SR č. 334/2015.
* Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020

## Aktuálny zoznam zákonov a vykonávacích predpisov relevantných pre informačnú a kybernetickú bezpečnosť ISVS

**Základný legislatívny rámec informačnej bezpečnosti** súčasnej právnej úpravy SR:

1. 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,
2. zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
3. zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov,
4. zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom
5. trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov,
6. zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov,
7. zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
8. zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
9. zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov,
10. 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,
11. zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
12. zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,
13. ústavný zákon č. 254/2006 Z. z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu,
14. zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
15. 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,
16. zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších právnych predpisov
17. nariadenie vlády Slovenskej republiky č. 216/2004 Z. z., ktorým sa ustanovujú oblasti utajovaných skutočností,
18. výnos č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky zo 4. marca 2014 o štandardoch pre informačné systémy verejnej správy
19. 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
20. Zbierka zákonov č. 525/2011 Výnos Ministerstva vnútra Slovenskej republiky z 12. decembra 2011 o štandardoch pre elektronické informačné systémy na správu registratúry
21. Zbierka zákonov č. 164/2013, Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení
22. Zbierka zákonov č. 117/2014, Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky 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
23. Zbierka zákonov č. 165/2013, Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky z 13. júna 2013 ktorou sa ustanovujú podrobnosti o skúške fyzickej osoby na výkon funkcie zodpovednej osoby
24. 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:

1. vyhláška Národného bezpečnostného úradu č. 301/2013 Z. z. o priemyselnej bezpečnosti a o bezpečnostnom projekte podnikateľa,
2. vyhláška Národného bezpečnostného úradu č. 134/2016 Z. z. o personálnej bezpečnosti,
3. vyhláška Národného bezpečnostného úradu č. 135/2016 Z. z. o skúške bezpečnostného zamestnanca,
4. 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.,
5. 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.,
6. vyhláška Národného bezpečnostného úradu č. 339/2004 Z. z. o bezpečnosti technických prostriedkov,
7. vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií,
8. 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,
9. 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,
10. vyhláška Národného bezpečnostného úradu č. 453/2007 Z. z. o administratívnej bezpečnosti.

## Úlohy Akčného plánu na realizáciu Koncepcie kybernetickej bezpečnosti

**1. OBLASŤ: VYTVORENIE INŠTITUCIONÁLNEHO RÁMCA RIADENIA KYBERNETICKEJ BEZPEČNOSTI**

| **Číslo úlohy** | **Úloha** | **Spôsob realizácie** | **Zodpovedný subjekt** | **Súčinnostný subjekt** | **Časový rámec realizácie** |
| --- | --- | --- | --- | --- | --- |
| 1.1. | Pripraviť návrh na vytvorenie formálnej platformy pre spoluprácu. | Zabezpečovať podmienky pre činnosť komisie pre kybernetickú bezpečnosť a jej pracovných skupín zriadených na platforme spolupráce verejnej správy, akademickej obce, vedeckých kruhov a súkromnej sféry. | NBÚ | AKOB  ZaA | priebežne |
| Zriadiť pracovný výbor pre kybernetickú bezpečnosť pri BR SR a zabezpečovať organizačné podmienky pre jeho činnosť. | ÚV SR | NBÚ | 2016 a priebežne |
| 1.2. | Vytvoriť podmienky pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť vo svojej pôsobnosti. | Vypracovať návrh na personálne a materiálno-technické predpoklady pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť. | VPA |  | 04/2016 |
| Vytvárať podmienky pre materiálno-technické zabezpečenie a konsolidáciu organizačného a personálneho zabezpečenia a plnenia základných úloh vecne príslušných autorít. | VPA |  | priebežne |
| Zabezpečiť spoluprácu vecne príslušných autorít pre kybernetickú bezpečnosť. | ÚOŠS SR |  | 2016-2020 |
| 1.3. | Zabezpečiť inštitucionálny rámec riadenia kybernetickej bezpečnosti. | Vytvoriť národné centrum pre kybernetickú bezpečnosť v pôsobnosti úradu. | NBÚ |  | 2017 |
| Vytvoriť medzirezortnú pracovnú skupinu (zoskupenie) na riešenie rozsiahlych počítačových/kybernetických útokov a tímu rýchleho nasadenia a v prípade potenciálneho ohrozenia kybernetického priestoru SR operatívne zasahovať. | NBÚ | MF SR  MV SR  MO SR  SIS | 2016 a priebežne |
| 1.4. | Budovať spôsobilosti kybernetickej bezpečnosti. | Dobudovať spôsobilosti CSIRT.MIL.SK, ako jednotky na riešenie incidentov, pre účely obrany SR, spôsobilosti aktívnej kybernetickej obrany, spôsobilosti v mobilných sieťach OS SR a implementáciu prvkov kybernetickej bezpečnosti do rezortných dátových sietí. | MO SR |  | 2016-2020 |
| Dobudovať vybrané spôsobilosti CSIRT.SK (vládnej jednotky) v DataCentre v pôsobnosti Ministerstva financií SR. | MF SR | DC/CSIRT.SK | 2016-2020 |
|  |  | Navrhnúť organizačné, personálne, materiálno-technické a finančné zabezpečenie jednotky na riešenie incidentov vo svojej pôsobnosti. | ÚV SR | NASES | 04/2016 |
| Zriadiť jednotku vo svojej pôsobnosti a dobudovať jej spôsobilosti. | ÚV SR | NASES | 2017 |
| Zabezpečiť zriadenie a výkon činností útvarov na riešenie incidentov typu CERT/CSIRT alebo zabezpečiť tento výkon činnosti prostredníctvom existujúcich útvarov/jednotiek pôsobiacich v pôsobnosti inej vecne príslušnej autority v súlade s ustanoveniami zákona o kybernetickej bezpečnosti. | VPA |  | 2017-2020 |
| 1.5. | Vytvoriť rámec riadenia kybernetickej bezpečnosti v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny. | Navrhnúť inštitucionálne riadenie kybernetickej bezpečnosti v núdzovom stave, výnimočnom stave, vojnovom stave a stave vojny. | NBÚ | MO SR  MV SR  BR SR | 2017/18 |
|  |  | Navrhnúť kontingenčný plán prechodu zodpovednosti za riadenie kybernetickej bezpečnosti v čase mieru, núdzového a výnimočného stavu do vojnového stavu a stavu vojny podľa ústavného zákona č. 227/2002 Z. z. | NBÚ | MO SR  MV SR  BR SR | 2017/18 |
| 1.6. | Vytvoriť medzirezortný/nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky“. | Predložiť na schválenie vláde SR nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky.“ | NBÚ | MF SR  MV SR  MDVaRR SR  MŠVVaŠ SR  MO SR  ÚV SR  SIS | 06/2016 |
|  |  | Predložiť na rokovanie vlády SR implementačný program „Ochrana kybernetického priestoru Slovenskej republiky“ v horizonte do roku 2025 obsahujúci súhrn projektov, aktivít, prác, činností a dodávok vykonávaných na splnenie zámerov a cieľov podľa rozpočtových pravidiel nadrezortného rozpočtového programu. | NBÚ | MF SR  MV SR  MDVaRR SR  MO SR  ÚV SR  NASES | 12/2016 |

**2. OBLASŤ: VYTVORENIE A PRIJATIE LEGISLATÍVNEHO RÁMCA KYBERNETICKEJ BEZPEČNOSTI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie |
| 2.1. | Vytvoriť legislatívne podmienky pre oblasť kybernetickej bezpečnosti. | Pripraviť návrh zákona o kybernetickej bezpečnosti a predložiť ho do formálneho legislatívneho procesu. | NBÚ | MF SR  VPA  NASES  CSIRT.SK | 06/2016 |
| Predložiť návrh zákona o kybernetickej bezpečnosti na rokovanie vlády SR. | NBÚ | MF SR | 09/2016 |
| Vytvárať podmienky pre implementáciu príslušných ustanovení zákona o kybernetickej bezpečnosti vo svojej pôsobnosti. | Povinné osoby |  | od 2017 |
| 2.2. | Zosúladiť súvisiace právne prepisy so zákonom o kybernetickej bezpečnosti. | Vykonať analýzu prostredia a pripraviť zoznam právnych predpisov s návrhom ich novelizácie a časovým harmonogramom. | NBÚ | ÚOŠS SR | 06/2017 |
| 2.3. | Pripraviť, vykonávacie predpisy k zákonu o kybernetickej bezpečnosti a zabezpečiť ich legislatívny proces (schválenie). | Pripraviť vykonávacie predpisy upravujúce podrobnosti k oblastiam na základe blanketnej normy v zákone o kybernetickej bezpečnosti. | NBÚ | ÚOŠS SR | 06/2017 |
| 2.4. | Vydávať štandardy, metodiky a metodické usmernenia v oblasti kybernetickej bezpečnosti. | V pôsobnosti Komisie pre kybernetickú bezpečnosť NBÚ zriadiť pracovné skupiny pre:  -   kybernetický zločin a počítačovú kriminalitu  -   metodiku a štandardy  -   terminológiu v oblasti KB. | NBÚ |  | 04/2016 |
|  |  | Vydávať štandardy, metodiky a metodické usmernenia. | NBÚ | ÚNMS SR VPA  SIS | priebežne |
| Zriadiť centrálny prístupový bod k normám a štandardom pre ochranu prvkov kritickej infraštruktúry a zabezpečovať pravidelnú aktualizáciu jeho obsahu. | NBÚ | ÚNMS  DC  SNAS  NASES | 06/2017 |
| 2.5. | Terminológia v oblasti kybernetickej bezpečnosti. | Aktualizovať slovník krízového riadenia v súlade s výstupmi Komisie pre kybernetickú bezpečnosť pri NBÚ v oblasti terminológie a doplniť ho o nové pojmy. | ÚV SR | VPA  NBÚ  BR SR | 06/2016 |
|  |  | Vytvoriť terminologický výkladový slovník za účelom zjednotenia pojmov pre účely tvorby koncepčných, strategických a legislatívnych materiálov v oblasti kybernetickej bezpečnosti a zabezpečovať jeho aktualizáciu. | NBÚ | AKOB | 06/2017  a potom priebežne |

**3. OBLASŤ: ROZPRACOVANIE A APLIKÁCIA ZÁKLADNÝCH MECHANIZMOV ZABEZPEČENIA SPRÁVY KYBERNETICKÉHO PRIESTORU**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie |
| 3.1. | Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore. | Vypracovať metodiku hodnotenia rizík pre oblasť kybernetickej bezpečnosti na národnej úrovni. | NBÚ | AKOB  ZaA | 12/2016 |
|  |  | Vytvoriť postupy pre analýzu stavu, vyhodnocovať ho a navrhovať bezpečnostné opatrenia na odstránenie/minimalizáciu rizík a možných krízových stavov v priestore štátu. | NBÚ |  | 2016  (každoročne) |
| 3.2. | V rámci mechanizmu prevencie zaviesť jednotné opatrenia z úrovne vecne príslušných autorít. | Zaviesť opatrenia na minimalizáciu potenciálnych rizík a krízových stavov vo svojej pôsobnosti. | VPA |  | 2018 |
| 3.3. | Vytvoriť procesy a mechanizmy pri koordinácii zabezpečovania ochrany významných informačných aktív štátu na národnej úrovni. | Vytvoriť metodiku pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry. | MF SR | NBÚ  MV SR  DC/CSIRT.SK | 2016 |
| 3.4. | Vytvoriť a implementovať systém včasného varovania a reakcie na incidenty. | Implementovať jednotný systém včasného varovania, reakcie na incidenty a výmeny informácií podľa časového harmonogramu za účelom zníženia rizík vyplývajúcich z hrozieb informačných a komunikačných systémov a zabezpečovať jeho nepretržitú prevádzku v súlade s plnením úlohy „OAS02 Medzirezortného programu na ochranu kritickej infraštruktúry v SR.“ | NBÚ | DC/CSIRT.SK  VPA/JRI | 2016-2020 |
|  |  | Zriadiť Národný portál pre kybernetickú bezpečnosť ako súčasť ÚPVS. | ÚV SR | NASES | 2017 |
| 3.5. | V rámci mechanizmu reakcie na bezpečnostné incidenty navrhnúť minimálne bezpečnostné opatrenia pre jednotlivé kategórie informačných aktív a zabezpečiť ich implementáciu. | Zaviesť jednotné opatrenia na národnej úrovni, ktorých cieľom bude kvalifikovane a efektívne reagovať na bezpečnostné incidenty. | NBÚ | VPA | 2018 |
| Navrhnúť a zaviesť pravidlá pre blokovanie útokov za účelom zvýšenia obranyschopnosti SR voči kybernetickým útokom na významné informačné systémy z externého prostredia/internetu, najmä voči šíreniu škodlivého kódu zo sietí infikovaných počítačov a šíreniu škodlivej aktivity z IP adresného rozsahu SR. | NBÚ | DC/CSIRT.SK  NASES  SIS | 2016 |
|  |  | Vytvoriť mechanizmus na eskaláciu na zodpovedajúce útvary krízového riadenia a na vládu SR, kompatibilné s mechanizmami európskej úrovne a NATO a koordináciu riešenia rozsiahlych bezpečnostných incidentov/útokov, krízových stavov na úrovni štátu podľa štandardných operačných procedúr za účelom zefektívnenia koordinácie postupov riešenia rozsiahlych bezpečnostných incidentov. | NBÚ | MV SR  MO SR  MDVaRR SR  MZVaEZ SR  SIS  DC/CSIRT.SK NASES | 2017 |
| 3.6. | Aktualizovať plány riešenia krízových situácií pre oblasť kybernetickej bezpečnosti. | Aktualizovať katalógové listy a doplniť ich tak, aby reflektovali na bezpečnostné incidenty v rámci kybernetického priestoru. | NBÚ |  | 2017 |
| 3.7. | Pravidelne vykonávať ohodnotenie úrovne bezpečnosti vo vládnych sieťach a kritických infraštruktúrach. | Vykonávať interné a externé penetračné testy informačných systémov vybraných organizácií verejnej správy, vrátane prvkov kritickej informačnej infraštruktúry a ďalších významných informačných systémov. | MF SR | ÚOŠS  DC/CSIRT.SK  Prevádzko-vatelia prvkov KII  SIS | priebežne |

**4. OBLASŤ: PODPORA, VYPRACOVANIE A ZAVEDENIE SYSTÉMU VZDELÁVANIA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie | |
| 4.1. | Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti. | Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov:  a) všeobecného vzdelávania (základný a stredný stupeň vzdelania) a  b) odborného vzdelávania (stredný a vysokoškolský stupeň vzdelania, špecialisti). | MŠVVaŠ SR |  | 06/2016 | |
| 4.2. | Zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti. | Na základe výsledkov mapovania stavu vzdelávania spracovať návrh na inováciu a zabezpečenie vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov všeobecného vzdelávania (základný a stredný stupeň vzdelania) a podporu odborného vzdelávania (stredný a vysokoškolský stupeň vzdelania, špecialisti). | MŠVVaŠ SR | NBÚ  MO SR  SIS  MV SR  NASES | 03/2017 | |
| 4.3. | Zaviesť inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti. | Zaviesť inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti v rámci všeobecného vzdelávania (základný a stredný stupeň vzdelania) a podporiť odborné vzdelávanie (stredný a vysokoškolský stupeň vzdelania, špecialisti) v tejto oblasti. | MŠVVaŠ SR | MO SR  SIS  MV SR  NASES | | 09/2018 |
| 4.4. | Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti. | Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti, ktoré zabezpečí vzdelávanie a dosiahnutie aspoň základnej úrovne kompetencií v oblasti kybernetickej bezpečnosti všetkých pedagogických zamestnancov v regionálnom školstve, inovovať praktickú prípravu budúcich učiteľov jednotlivých stupňov škôl. | MŠVVaŠ SR | MPSVaR SR | | 06/2017 |
| 4.5. | Systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti. | Zabezpečiť šírenie osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy | NBÚ | MF SR  MK SR  MPSVaR SR  NASES | | priebežne |
| 4.6. | Zabezpečiť školenie o kybernetickej bezpečnosti. | V rámci rozvoja siete Govnet a služieb ÚPVS rozšíriť obsah existujúcich školení aj o oblasť kybernetickej bezpečnosti. | ÚV SR | NASES | | 2016-2020 |
|  |  | Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o ďalšie špecifické oblasti a zabezpečiť pokračovanie vzdelávania. | NBÚ | AKOB | | 2017 |
| Realizovať školenia pracovníkov verejnej správy v oblasti ochrany informačných aktív voči kybernetickým útokom z externého prostredia. | MF SR | DC/CSIRT.SK | |  |
| 4.7. | Vytvoriť študijné programy v rámci celoživotného vzdelávania profesionálnych vojakov. | V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov – špecialistov IKT so zameraním na kybernetickú bezpečnosť. | MO SR |  | | 2016-2017 |
|  |  | V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov so zameraním na kybernetickú bezpečnosť. | MO SR |  | | 2017-2019 |
| 4.8. | Zabezpečiť vzdelávanie v oblasti informačnej a kybernetickej bezpečnosti v rámci justičných orgánov. | Zaviesť minimálnu úroveň systematického vzdelávania pre všetkých sudcov, prokurátorov na všetkých úrovniach. | MS SR | GP SR  JA SR Súdna rada | | 2016-2020 |
|  |  | Zaviesť rozšírené vzdelávanie pre vybraných sudcov, prokurátorov na všetkých úrovniach. | MS SR | GP SR  JA SR Súdna rada | | 2016-2020 |
| 4.9. | Zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti v rámci vyšetrovacích orgánov. | Zaviesť minimálnu úroveň systematického vzdelávania v oblasti kybernetickej bezpečnosti pre vyšetrovateľov na všetkých úrovniach. | MV SR | APZ | | 2016-2020 |
| Zaviesť rozšírené vzdelávanie v oblasti kybernetickej bezpečnosti pre vybraných vyšetrovateľov na všetkých úrovniach. | MV SR | APZ | | 2016-2020 |
| 4.10. | Zabezpečiť vytvorenie popisu kvalifikácie pre oblasť informačnej a kybernetickej bezpečnosti v rámci národnej sústavy kvalifikácií v SR. | Vykonať analýzu existujúceho stavu pre oblasť bezpečnosti IKT a v spolupráci s relevantnými ústrednými orgánmi štátnej správy pripraviť návrh doplnenia zoznamu kvalifikácií a predložiť materiál na rokovanie vlády SR. | NBÚ | MPSVaR SR | | 2017 |

**5. OBLASŤ: STANOVENIE A APLIKÁCIA KULTÚRY RIADENIA RIZÍK A SYSTÉMU KOMUNIKÁCIE MEDZI ZAINTERESOVANÝMI STRANAMI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie |
| 5.1. | Vytvoriť efektívny model spolupráce na národnej úrovni medzi jednotlivými subjektmi kybernetickej bezpečnosti. | Vypracovať návrh spolupráce na národnej úrovni medzi pracoviskami na riešenie incidentov (CERT/CSIRT a pod.) za účelom výmeny a zdieľania informácií najmä o bezpečnostných incidentoch. | NBÚ | VPA | 2016 |
|  |  | Vytvoriť bezpečný komunikačný kanál prostredníctvom ktorého budú jednotky pre riešenie incidentov automatizovane prijímať a spracovávať hlásenia o závažných kybernetických bezpečnostných incidentoch. | NBÚ | DC  NASES | 2017 |
| 5.2. | Implementovať systém nahlasovania a riešenia bezpečnostných incidentov. | Implementovať on-line systém nahlasovania a riešenia bezpečnostných incidentov. | NBÚ | DC/CSIRT.SK  NASES | 2017 |

**6. OBLASŤ: AKTÍVNA MEDZINÁRODNÁ SPOLUPRÁCA**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie |
| 6.1. | V rámci členstva v EÚ sa aktívne zúčastňovať na príprave a realizácii legislatívnych a nelegislatívnych iniciatív týkajúcich sa kybernetickej bezpečnosti. | Zabezpečiť aktívnu účasť expertov v dotknutých pracovných skupinách a výboroch inštitúcií EÚ predovšetkým ku negociácii a implementácii smernice o sieťovej a informačnej bezpečnosti. | NBÚ | MZVaEZ SR MF SR | priebežne |
|  |  | Zabezpečovať aktívnu účasť expertov na programoch, projektoch a ďalších iniciatívach týkajúcich sa informačnej/kybernetickej bezpečnosti v kontexte viacročného finančného rámca EÚ 2014-2020 a v kontexte implementácie Stratégie kybernetickej bezpečnosti EÚ a jednotného digitálneho trhu. | NBÚ | MZVaEZ SR  MF SR | priebežne |
|  |  | Spolupracovať a aktívne sa podieľať na činnostiach a aktivitách medzinárodných platforiem v rámci medzinárodných organizácií. | MZVaEZ SR | NBÚ  MF SR | 2016-2020 |
| 6.2. | V rámci členstva v NATO podporovať spoluprácu s NATO v oblasti kybernetickej obrany. | Podpísať Memorandum o spolupráci v oblasti kybernetickej obrany. | NBÚ | MO SR | 02/2016 |
|  |  | Podporovať spoluprácu s NATO v oblasti kybernetickej obrany, najmä s ohľadom na reakcie na počítačové bezpečnostné incidenty a výmenu technických informácií o hrozbách a zraniteľnostiach. | NBÚ | MO SR  MZVaEZ SR | 2016-2020 |
| Podpísať „Statement of Interest“ o pristúpení SR k NATO projektu MISP (Malware Information Sharing Platform). | NBÚ | MO SR  MZVaEZ SR | 06/2016 |
| 6.3. | V rámci stredoeurópskeho priestoru rozvíjať vzťahy a nadväzovať bilaterálne spoluprácu s vybranými krajinami v oblasti kybernetickej bezpečnosti. | Aktívne sa podieľať, rozvíjať a podporovať spoluprácu v rámci krajín V4, predovšetkým prostredníctvom Stredoeurópskej platformy kybernetickej bezpečnosti (Central European Cyber Security Platform, CECSP). | NBÚ | DC  MO SR | priebežne |
| Nadväzovať a prehlbovať bilaterálne spolupráce s krajinami, ktoré vykonávajú podobné aktivity ako SR. | NBÚ | MZVaEZ SR | priebežne |
| 6.4. | Zapájať sa a zúčastňovať sa na medzinárodných kybernetických cvičeniach. | Zabezpečiť pravidelnú aktívnu účasť na medzinárodných kybernetických cvičeniach (Cyber Coalition, Locked Shields, Cyber Europe a iné). | NBÚ  MF SR/DC  MO SR |  | priebežne |
| 6.5. | Zintenzívniť spoluprácu s Centrom výnimočnosti pre kybernetickú obranu (NATO Cooperative Cyber Defence Centre of Excellence – CCD CoE). | Navýšiť personálne kapacity zástupcov SR vyslaných na plnenie služobných povinností do CCD CoE. | MO SR |  | 2018 |
| Na základe ponuky školení a vzdelávacích aktivít CCD CoE pravidelne informovať subjekty a umožniť účasť na predmetných aktivitách. | MO SR |  | priebežne |

**7. OBLASŤ: PODPORA VEDY A VÝSKUMU V OBLASTI KYBERNETICKEJ BEZPEČNOSTI**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Číslo úlohy | Úloha | Spôsob realizácie | Zodpovedný subjekt | Súčinnostný subjekt | Časový rámec realizácie |
| 7.1. | Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti. | Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti prostredníctvom domácich grantových schém. | MŠVVaŠ SR | AKOB  MF SR  NASES | 2016-2020 |
|  |  | Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti prostredníctvom prostriedkov vyčlenených pre Európsky výskumný priestor. | MŠVVaŠ SR | AKOB  MF SR  NASES | 2016-2020 |
| 7.2. | Podporovať budovanie forenzných pracovísk. | Podporovať budovanie nových špecializovaných pracovísk za účelom posilnenia ochrany významných informačných aktív štátu, s následným využitím ich poznatkov pre podporu rozvoja vedy a výskumu v oblasti kybernetickej bezpečnosti. | NBÚ |  | 2016-2020 |
|  |  | Vytvárať forenzné pracoviská vo svojej pôsobnosti zamerané na vykonávanie analytických činností pri riešení bezpečnostných incidentov/útokov a vykonávaním úkonov súvisiacich so zberom a vyhodnocovaním digitálnych stôp v organizácii pre poskytovanie služieb organizáciám štátnej správy a zabezpečovať ich prevádzku. | ÚOŠS |  | 2016-2020 |

## Kapacity SR v IB/KB

### Na riešenie incidentov informačnej bezpečnosti

Fungujúce CSIRT-y

* CSIRT.SK (Datacentrum, 7 rokov, xx ľudí, medzinárodne uznaný a akreditovaný)
* CSIRT.MIL (Ministerstvo obrany, xx rokov, xx ľudí, medzinárodne uznaný, zatiaľ neakreditovaný)
* NBÚ,
* NASES ?

súkromné CSIRTy

1. Slovak Telekom?

### Organizácie

1. Slovenská asociácia pre informačnú bezpečnosť
2. ISACA Slovensko

### Súkromné spoločnosti

1. Eset

### Vzdelávacie inštitúcie

1. UK (FMFI UK – kryptológia, manažment IB, bezpečnosť počítačových systémov a sietí, učiteľstvo informatiky, Práv. Fakulta – počítačové právo, právo duševného vlastníctva, Fakulta manažmentu Manažment IB)
2. STU (FEI STU – Kryptológia a informačná bezpečnosť, FIIT - manažment IB, bezpečnosť počítačových systémov a sietí)
3. Vojenská akadémia Liptovský Mikuláš ?

## 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[[24]](#footnote-24) 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. |

Príloha:



## Poznatky CSIRT.SK o stave informačnej/kybernetickej bezpečnosti vo verejnej správe

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[[25]](#footnote-25), informácií získaných z threat intelligence platformy implementovanej CSIRT.SK[[26]](#footnote-26), 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 zriadovateľskej 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 1 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[[27]](#footnote-27) incidentov typu prienik, alebo pokus o prienik do informačných systémov.

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

Tabuľka 1Kybernetické útoky v SR



Stav informačnej bezpečnosti vo verejnej správe – bezpečnostné povedomie

Pre účely praktického overenia úrovne bezpečnostného povedomia zamestnancov štátnej správy CSIRT.SK v roku 2013 počas národného cvičenia na ochranu kritickej infraštruktúry SISE 2013 simuloval phishingový útok prostredníctvom emailu adresovaného jednotlivým rezortom. Text phishingového emailu bol pripravený na základe zaznamenaných útokov na Slovensku 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 pláce. 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. V prípade komplexných neobmedzených penetračných testov (cca 15 percent celkového počtu), v ktorých bola dosiahnutá 100% úspešnosť kompromitácie v intervale 3-48 hodín[[28]](#footnote-28), CSIRT.SK dospel k záveru, že pokročilý útočník by mohol bez väčších problémov kompromitovať väčšinu organizácií.

Identifikované nedostatky v organizáciách verejnej správy možno rozdeliť najmä do nasledujúcich oblastí[[29]](#footnote-29):

* **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[[30]](#footnote-30) 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[[31]](#footnote-31) bolo pri viac ako 90 percent penetračných testoch identifikovaná aspoň jedná závažná[[32]](#footnote-32) a/alebo kritick[[33]](#footnote-33)á 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)

#### Analýza rizík, inventarizácia, klasifikácia informačných aktív

Základným pilierom procesu riadenia KIB je počiatočná celková a kontinuálna analýza rizík na úrovni ÚOŠS a jednotlivých inštitúcií verejnej správy (povinných osôb). Na úvod je potrebné vypracovanie celkovej, počiatočnej analýzy rizík, ktorej výstupom bude základný dokument tzv. register rizík kybernetickej a informačnej bezpečnosti, kde budú popísané identifikované bezpečnostné riziká, určená ich závažnosť a popísané protiopatrenia. Celková analýza rizík bude musieť byť vypracovaná na základe jednotnej metodiky pre celú verejnú správu, ktorú pripraví Centrum. Hodnoty z celkovej analýzy rizík budú jedným z kľúčových ukazovateľov efektivity systému riadenia KIB.

Celkovej analýze rizík musí predchádzať inventarizácia informačných aktív. Bude potrebné vykonanie inventarizácie informačných aktív vo všetkých ÚOŠS a jednotlivých inštitúcií verejnej správy (povinných osôb).

Bez poznania aké druhy informácií (informačné aktíva) sú spracovávané v informačno-komunikačnej infraštruktúre organizácie a aká je ich hodnota t.j. „čo je potrebné chrániť“ nie je možné dosiahnuť požadovanú efektivitu bezpečnostných opatrení v niektorých prípadoch ani ich správnu implementáciu, nehovoriac o efektívnom vynakladaní zdrojov.

K inventarizácii informačných aktív bude potrebné vytvoriť klasifikačnú schému vo forme interného predpisu a v procese inventarizácie informačných aktív, zistiť od vlastníkov ich požiadavky na dôvernosť, dostupnosť a integritu. Následne podľa schémy zaradiť každé informačné aktívum do jednej z klasifikačných tried. Centrum stanoví jednotnú klasifikačnú schému pre informačné systémy verejnej správy.

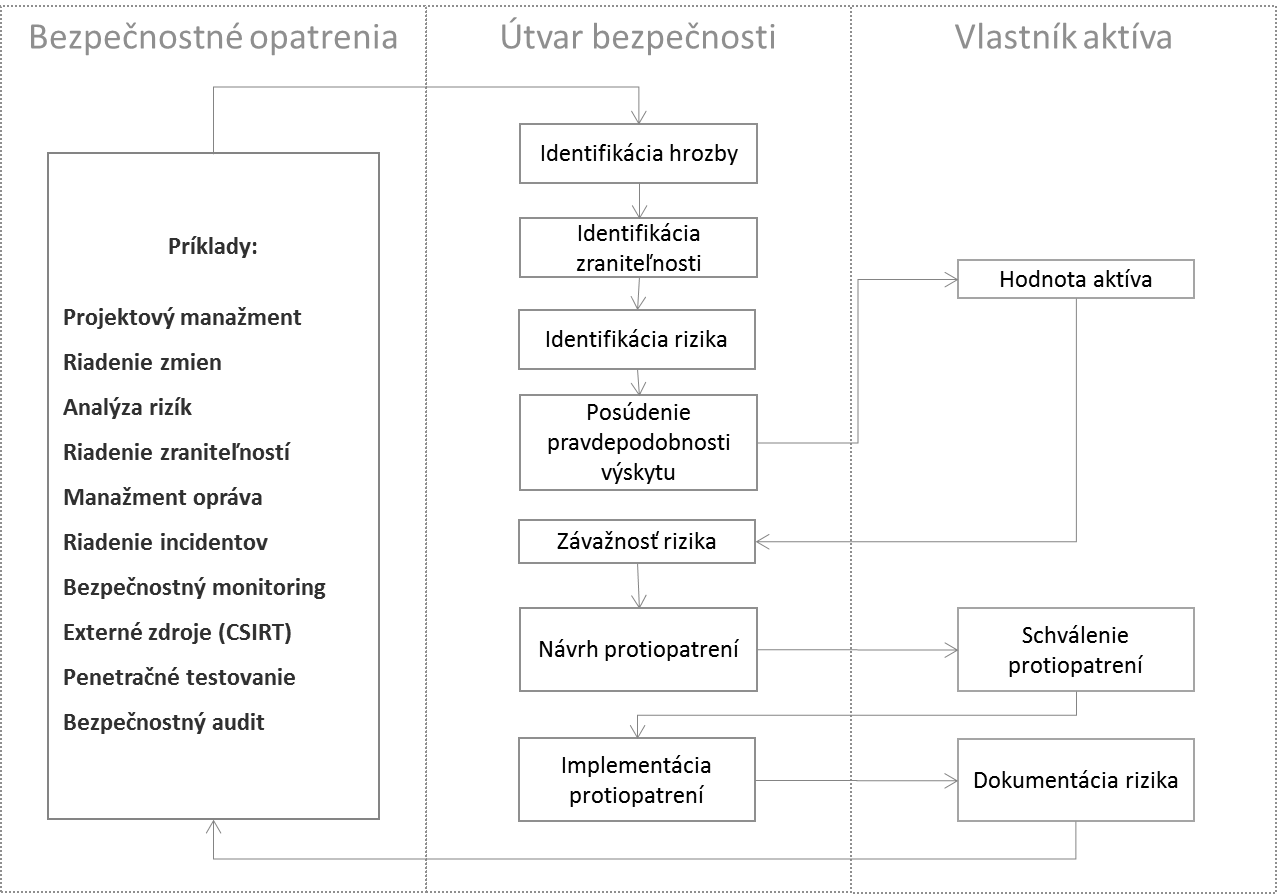
Inventarizáciu a klasifikáciu informačných aktív ako aj celkovú prvotnú analýzy rizík je možné vykonať ako samostatný projekt v rámci iných operačných programov (napr. OP EVS).

Definovanie a metodické rozpracovanie opatrení KIB a ich následná implementácia pomôže k výraznému zníženiu úrovne závažnosti identifikovaných bezpečnostných rizík.

#### Kontinuálna analýza bezpečnostných rizík

Po vykonaní prvotnej analýzy rizík bude hlavnou činnosťou MIB a organizačného útvaru KIB vykonávať kontinuálnu analýzu rizík. Výkon bude realizovať prostredníctvom bezpečnostných nástrojov, procesov, kontrolou efektívnosti, presadzovaním bezpečnostných opatrení a pod.

Kontinuálna analýza bezpečnostných rizík je znázornená na nasledovnom obrázku



Personálne obsadenia organizačného útvaru KIB by malo byť tvorené okrem samotného MIB aj nasledovnými špecialistami:

* Špecialista pre riadenie rizík a metodickú činnosť
* Technologický špecialisti (virtualizácia, operačné systémy, aplikácie, databázy, sieťové technológie)
* Podľa potreby špecialista pre ochranu osobných údajov

Predpokladaný počet na každom ÚOŠS je MIB a oddelenie KIB s 3-8 špecialistami.

## Vytvorenie jednotného (unifikovaného) rámca bezpečnostných opatrení

Základným poslaním komplexného rámca bezpečnostných opatrení je výrazné zužovanie priestoru pre kybernetický útok (cyber-attacks surface).

### Bezpečnostné opatrenia pre informačné systémy verejnej správy

Unifikovaný rámec bezpečnostných opatrení (niekde uvádzané aj ako bezpečnostné kontroly) pre informačné systémy verejnej správy bude vypracovaný na základe medzinárodných štandardov, ktoré sú prijaté aj ako Slovenské Technické Normy (STN) STN ISO/IEC 27001:2014 a STN ISO/IEC 27002:2014. Súbor odporúčaných kontrol a opatrení je uvedený ako príloha A štandardu STN ISO/IEC 27001:2014. Opatrenia sú následne podrobne rozvinuté v norme STN ISO/IEC 27002:2014.

Dôvodom pre zvolenie uvedených štandardov je ich aplikovateľnosť na akúkoľvek organizáciu no najmä skutočnosť, že tento rámec je dlhoročne používaný vo verejnej správe pre implementáciu bezpečnostných opatrení a rovnako aj ako základný rámec pre vykonávanie auditov informačnej bezpečnosti.

Opatrenia sa týkajú rôznych aspektov a oblastí informačnej bezpečnosti a definujú tak určitý celkový rámec, ktorý je zavedený v organizácii. V praxi to znamená, že efektívny systém riadenia informačnej bezpečnosti musí zahŕňať implementáciu opatrení vo všetkých uvedených oblastiach. Samozrejme s ohľadom na aktuálne existujúce riziká.

Komplexný rámec riadenia informačnej bezpečnosti v zmysle prílohy A štandardu STN ISO/IEC 27001:2014 je nasledovný:

* A.5 Politiky informačnej bezpečnosti
  + A.5.1 Usmernenie pre informačnú bezpečnosť
* A.6 Organizácia informačnej bezpečnosti
  + A.6.1 Vnútorná organizácia
  + A.6.2 Mobilné zariadenia a práca na diaľku
* A.7 Personálna bezpečnosť
  + A.7.1 Pred nástupom do zamestnania
  + A.7.2 Počas zamestnania
  + A.7.3 Ukončenie a zmena zamestnania
* A.8 Riadenie aktív
  + A.8.1 Zodpovednosť za aktíva
  + A.8.2 Klasifikácia informácií
  + A.8.3 Zaobchádzanie s médiami
* A.9 Riadenie prístupov
  + A.9.1 Požiadavky na riadenie prístupov
  + A.9.2 Riadenie používateľských prístupov
  + A.9.3 Zodpovednosť používateľov
  + A.9.4 Riadenie systémových a aplikačných prístupov
* A.10 Šifrovanie, kryptografia
  + A.10.1 Riadenie šifrovania
* A.11 Fyzická bezpečnosť a bezpečnosť prostredia
  + A.11.1 Zabezpečené oblasti
  + A.11.2 Bezpečnosť zariadení
* A.12 Bezpečnosť prevádzky
  + A.12.1 Prevádzkové postupy a zodpovednosť
  + A.12.2 Ochrana pred škodlivým kódom
  + A.12.3 Zálohovanie
  + A.12.4 Zaznamenávanie dát a monitorovanie
  + A.12.5 Riadenie operačného softvéru
  + A.12.6 Riadenie technickej zraniteľnosti
  + A.12.7 Audit informačných systémov
* A.13 Komunikačná bezpečnosť
  + A.13.1 Riadenie bezpečnosti v sieťach
  + A.13.2 Prenos informácií
* A.14 Akvizícia, vývoj a údržba informačných systémov
  + A.14.1 Bezpečnostné požiadavky na informačné systémy
  + A.14.2 Bezpečnosť pri vývoji a pri podporných procesoch
  + A.14.3 testovacie údaje
* A.15 Riadenie vzťahov s dodávateľmi
  + A.15.1 Informačná bezpečnosť vo vzťahoch s dodávateľmi
  + A.15.2 Riadenie dodávateľských služieb
* A.16 Riadenie incidentov informačnej bezpečnosti
  + A.16.1 Riadenie incidentov informačnej bezpečnosti a zlepšovanie
* A.17 Aspekty informačnej bezpečnosti v riadení kontinuity
  + A.17.1 Kontinuita informačnej bezpečnosti
  + A.17.2 Redundancia
* A.18 Súlad
  + A.18.1 Súlad s právnymi a zmluvnými požiadavkami
  + A.18.2 Preskúmanie informačnej bezpečnosti

Pre jednotlivé oblasti bezpečnostných opatrení resp. jednotlivé opatrenia musia byť definované základné zásady. Každá oblasť musí byť ďalej detailne rozpracovaná do metodických pokynov pre potreby verejnej správy tak, aby obsahovala minimálne:

* Ciele opatrenia (eliminácia hrozieb, zraniteľností a rizík)
* Základné zásady opatrenia
* Rozšírené zásady opatrenia
* Proces prevádzky opatrenia (vstupy, výstupy, eskalácie)
* Zaradenie opatrenia, procesu, výstupu do celkového systému riadenia rizík organizácie
* Nároky na personálne a iné zdroje
* Možné technológie na podporu opatrenia a minimálne nároky

Implementácia jednotlivých kontrol a opatrení môže mať rôznu úroveň vyspelosti a to najmä vzhľadom na kritickosť spracovávaných informácií. Implementácia opatrení bude smerovať k organizácii ako celku (t.j. celú informačno-komunikačnú infraštruktúru). Na základe kritickosti údajov budú vyžadovaná konkrétna úroveň opatrení. Za účelom unifikácie bude potrebné vytvoriť jednotnú štruktúru označenia a zaradenia informačno-komunikačnej infraštruktúry organizácie do určitej triedy podľa kritickosti. Napríklad ak je v informačnej a komunikačnej infraštruktúre prevádzkovaný informačný systém s vysoko kritickými aktívami, bude celá infraštruktúra zaradená do triedy ako vysoko kritická a budú v nej musieť byť implementované opatrenia najvyššej úrovne vyspelosti.

Pre implementáciu potrebných bezpečnostných opatrení bude stanovený primeraný časový rámec (napr. 2-3 roky).

Niektoré oblasti môžu byť vylúčené v prípade, že nie sú pre organizáciu relevantné napr. v organizácii nie je vykonávaný vývoj aplikácií. Pre daný príklad však platí, že v prípade ak je vývoj v organizácii vykonávaný treťou stranou je potrebné kontroly a opatrenia definovať do oblasti riadenia bezpečnosti vo vzťahu s dodávateľmi t.j. do zmluvy s tretími stranami.

Komplexný súbor bezpečnostných opatrení základnej úrovne by mal byť vydaný formou výnosu, alebo ako súčasť Výnosu č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy.

Vo svojej podstate sa bude jednať o dokument typu politiky kybernetickej a informačnej bezpečnosti pre verejnú správu. Z tohto dôvodu je vhodnejšie aby bol vydaný formou samostatného výnosu. (napr. „Výnos o Politike kybernetickej a informačnej bezpečnosti pre verejnú správu“)

Následne budú jednotlivé oblasti (opatrenia) uvedené vo výnose detailne rozpracované do metodických pokynov a to na niekoľko úrovní podľa vyspelosti. Metodické materiály nebudú verejne prístupné a budú používané výhradne pre interné potreby.

Príklad možnej štruktúry riadiacich dokumentov pre oblasť KIB:

Výnos - Politika informačnej bezpečnosti Metodické pokyny (detailné procedúry, manuály)

Povinné výstupy a bezpečnostné štandardy

**Výnos - Politika informačnej bezpečnosti**

* Rámcový dokument obsahujúci základné zodpovednosti a oprávnenia jednotlivých zainteresovaných strán (organizácia bezpečnosti) a základné zásady pre jednotlivé oblasti s definovaním zodpovedných organizačných zložiek.
* Jednotlivé oblasti upravené podľa STN ISO/IEC 27001:2014 a STN ISO/IEC 27002:2014
* Relatívne nemenný dokument vyžadujúci minimálnu aktualizáciu (pri ďalšej revízii ISO/IEC 2700X)

**Metodické pokyny pre vypracovanie detailných procedúry, politík a manuálov**

* Dielčie politiky, postupy, detailné rozpracovanie jednotlivých oblastí z centrálnej politiky informačnej bezpečnosti.
* Manuály pre jednotlivé skupiny zainteresovaných strán najmä pre používateľov, administrátorov a tretie strany. Zhrnutie všetkých špecifických záväzných zodpovedností, povinností a oprávnení pre jednotlivé skupiny za účelom zjednodušenia oboznamovania sa a lepšieho pochopenia.
* Príklad: Pre bežného používateľa nie je potrebné aby poznal kryptografické opatrenia, alebo požiadavky pre bezpečný vývoj aplikácií.
* Možnosť detailnejšej špecifikácie oproti centrálnej politike informačnej bezpečnosti.
* Pre dokumenty v tejto kategórii je predpokladaná častejšia zmena, odporúčame tomu prispôsobiť aj proces ich aktualizácie zo zachovaním ich záväznosti.
* Manuál pre tretie strany je možné prikladať k zmluvám s tretími stranami, čím sa štandardizujú požiadavky v oblasti informačnej bezpečnosti pri spolupráci s tretími stranami.

**Povinné výstupy a štandardy**

* Záväzné výstupy z rozpracovanie jednotlivých opatrení napr. zoznam povolených služieb pre operačné systémy, plány obnovy pre jednotlivé systémy zoznam informačných aktív a pod.

### Role a zodpovednosti za jednotlivé oblasti

Pre jednotlivé oblasti KIB je možné vypracovanie schémy rolí podľa uvedenej charakteristiky tzv. RASCI matice podľa uvedeného príkladu.

R (Responsible) - subjekt primárne zodpovedný za vykonanie aktivity

A (Accountable) - subjekt zodpovedný za aktivitu ako celok

S (Supportive) - subjekt aktívne asistujúci pri návrhu, implementácii, alebo riadeniu aktivít

C (Consulted) - subjekt poskytujúci poradné služby, pomoc a usmernenie

I (Informed) - subjekt, ktorý je informovaný o aktivitách

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Jednotlivé oblasti informačnej bezpečnosti podľa  STN ISO/IEC 27002:2014** | | **Vlastník inform. aktíva** | **Zamestnanci** | **Kancelária ministra** | **Vedúci sekcií** | **Sekcia informatiky** | **Bezpečn. výbor** | **Manažér informačnej bezpečnosti** | **Oddelenie bezpečnosti** | **Personálny odbor** | **Odbor centrálneho obstarávania a nákupu** | **Odbor právnych služieb** | **Odbor financovania** | **Odbor správy majetku** |
| **5 Politiky informačnej bezpečnosti** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5.1.1 | Politiky informačnej bezpečnosti | **C** | **I** | **C** | **A** | **S** | **S** | **R** | **S** | **C** | **S** | **C** | **C** | **C** |
| 5.1.2 | Preskúmanie politík informačnej bezpečnosti | **C** |  | **S** | **A** | **S** | **S** | **R** | **C** | **S** | **S** | **S** | **S** | **C** |
| **6 Organizácia informačnej bezpečnosti** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6.1.1 | Role a zodpovednosti v informačnej bezpečnosti | **A** | **I** |  | **R** | **C** | **S** | **C** |  | **C** |  | **C** |  |  |
| 6.1.2 | Oddelenie právomocí | **A** | **I** |  | **C** | **C** | **S** | **R** |  |  |  |  |  |  |
| 6.1.3 | Kontakt s autoritami | **S** |  |  | **S** |  | **S** | **A** | **R** |  |  | **S** |  |  |
| 6.1.4 | Kontakt so špeciálnymi záujmovými skupinami | **S** |  |  | **C** | **S** | **C** | **A** | **R** |  |  | **S** |  |  |
| 6.1.5 | Informačná bezpečnosť v projektovom riadení | **S** |  |  | **C** | **A** | **S** | **R** |  |  |  |  |  |  |
| 6.2.1 | Politiky pre mobilné zariadenia | **S** | **I** |  | **C** | **C** | **S** | **A** | **R** |  |  |  |  |  |
| 6.2.2 | Práca na diaľku | **S** | **I** |  | **S** | **C** | **S** | **A** | **R** |  |  |  |  |  |
| **7 Personálna bezpečnosť** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7.1.1 | Preverovanie uchádzačov | **A** |  |  |  |  | **S** |  |  | **R** |  |  |  |  |
| 7.1.2 | Pracovná náplň a podmienky zamestnania | **A** | **I** |  | **S** |  | **S** |  |  | **R** |  | **R** |  |  |
| 7.2.1 | Manažérska zodpovednosť | **S** | **I** |  | **A** |  | **S** |  | **R** | **S** |  | **S** |  |  |
| 7.2.2 | Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť | **S** | **S** |  | **S** |  | **S** | **R** | **S** | **A** |  | **C** |  |  |
| 7.2.3 | Disciplinárny proces | **S** | **I** |  | **S** |  | **S** | **S** |  | **R** |  | **R** |  |  |
| 7.3.1 | Zodpovednosti pri ukončení alebo zmene zamestnania | **A** | **I** |  | **A** | **S** | **S** |  |  | **R** |  | **R** |  |  |
| **8 Riadenie aktív** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8.1.1 | Inventárny zoznam aktív | **A** |  |  |  | **C** | **S** | **C** | **R** |  | **S** |  |  |  |
| 8.1.2 | Vlastníctvo aktív | **A** |  |  | **R** | **C** | **S** | **S** | **S** |  |  |  | **S** | **S** |
| 8.1.3 | Prijateľné používanie aktív | **A** | **I** |  |  |  | **S** | **R** | **C** | **S** | **S** |  |  | **S** |
| 8.1.4 | Vrátenie aktív | **A** | **I** |  | **R** | **S** | **S** |  | **S** | **S** | **S** |  | **C** | **S** |
| 8.2.1 | Klasifikácia informácií | **A** | **I** |  | **S** |  | **S** | **R** | **S** |  |  | **C** |  |  |
| 8.2.2 | Označovanie informácií | **A** | **I** |  |  | **S** | **S** | **R** |  | **C** | **C** | **C** | **C** | **S** |
| 8.2.3 | Zaobchádzanie s aktívami | **A** | **I** |  |  | **R** | **S** | **C** | **C** |  |  |  | **C** | **S** |
| 8.3.1 | Riadenie prenosných médií | **A** | **I** |  |  | **R** | **S** | **C** | **C** |  |  |  |  | **S** |
| 8.3.2 | Likvidácia médií | **A** | **I** |  |  | **R** | **S** | **C** | **C** |  |  |  | **C** |  |
| 8.3.3 | Fyzický prenos médií | **A** | **I** |  |  | **R** | **S** | **C** | **C** |  |  |  |  |  |
| **9 Riadenie prístupov** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9.1.1 | Politika riadenia prístupov | **A** |  |  | **S** | **S** | **S** | **C** | **R** | **C** | **C** |  |  |  |
| 9.1.2 | Prístup do sietí a sieťových služieb | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 9.2.1 | Registrácia a de-registrácia používateľov | **A** |  |  |  | **R** | **S** | **C** | **C** | **C** |  |  |  |  |
| 9.2.2 | Poskytovanie používateľských prístupov | **A** |  |  |  | **R** | **S** | **C** | **C** |  |  |  |  |  |
| 9.2.3 | Riadenie privilegovaných prístupov | **A** |  |  | **C** | **R** | **S** | **C** | **C** | **C** |  |  |  |  |
| 9.2.4 | Riadenie utajených autentizačných údajov | **A** |  |  |  | **R** | **S** | **C** | **C** |  |  |  |  |  |
| 9.2.5 | Preskúmanie prístupových práv | **A** |  |  |  | **S** | **S** | **S** | **R** |  |  |  |  |  |
| 9.2.6 | Odstránenie alebo prispôsobenie prístupových práv | **A** |  |  |  | **R** | **S** | **S** | **C** |  |  |  |  |  |
| 9.3.1 | Používanie utajených autentizačných údajov | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 9.4.1 | Obmedzenie prístupu k informáciám | **A** | **I** |  |  | **R** | **S** | **C** | **C** |  |  | **C** |  |  |
| 9.4.2 | Bezpečné postupy prihlasovania | **A** |  |  |  | **R** | **S** | **C** | **C** |  |  |  |  |  |
| 9.4.3 | Systém riadenia hesiel | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 9.4.4 | Používanie privilegovaných pomocných programov | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 9.4.5 | Riadenie prístupu k zdrojovým kódom programov | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| **10 Šifrovanie, kryptografia** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10.1.1 | Politika pri používaní opatrení na šifrovanie | **A** | **I** |  |  | **S** | **S** | **R** | **C** |  |  |  |  |  |
| 10.1.2 | Riadenie šifrovacích kľúčov | **A** |  |  |  | **S** | **S** | **R** | **C** |  |  |  |  |  |
| **11 Fyzická bezpečnosť a bezpečnosť prostredia** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11.1.1 | Perimeter fyzickej bezpečnosti | **A** | **I** |  |  | **C** | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.1.2 | Riadenie fyzických prístupov | **A** | **I** |  |  | **C** | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.1.3 | Zabezpečenie kancelárií, miestností a prostriedkov | **A** | **I** |  |  | **C** | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.1.4 | Ochrana pred externými hrozbami a hrozbami prostredia | **A** | **I** |  |  | **C** | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.1.5 | Práca v chránených priestoroch | **A** | **I** |  |  |  | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.1.6 | Priestory na nakladanie a vykladanie | **A** | **I** |  |  |  | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.2.1 | Umiestnenie zariadení a ich ochrana | **A** | **I** |  |  |  | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.2.2 | Podporné služby | **A** |  |  |  | **C** | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.2.3 | Bezpečnosť kabeláže | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  | **S** |
| 11.2.4 | Údržba zariadení | **A** |  |  |  |  | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.2.5 | Odstraňovanie zariadení | **A** | **I** |  |  |  | **S** | **C** | **S** |  |  |  |  | **R** |
| 11.2.6 | Vynášanie zariadení mimo priestory | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  | **C** |
| 11.2.7 | Bezpečné znehodnotenie a opätovné používanie | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  | **S** |
| 11.2.8 | Zariadenia bez dozoru | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  | **S** |
| 11.2.9 | Politika čistého stola a čistej obrazovky | **A** | **I** |  | **R** | **S** | **S** | **C** | **S** |  |  |  |  | **S** |
| **12 Bezpečnosť prevádzky** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12.1.1 | Dokumentované prevádzkové postupy | **A** |  |  |  | **R** |  | **C** | **S** |  |  |  |  |  |
| 12.1.2 | Riadenie zmien | **A** | **I** |  | **S** | **R** | **S** | **C** | **C** |  |  |  |  |  |
| 12.1.3 | Riadenie kapacít | **A** |  |  | **S** | **R** | **S** | **S** | **S** |  | **S** |  |  | **C** |
| 12.1.4 | Oddelenie vývojového, testovacieho a prevádzkového prostredia | **A** |  |  | **S** | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 12.2.1 | Opatrenia proti škodlivému softvéru | **A** |  |  | **S** | **R** |  | **C** | **S** |  |  |  |  |  |
| 12.3.1 | Zálohovanie informácií | **A** |  |  | **S** | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 12.4.1 | Zaznamenávanie udalostí | **A** |  |  | **S** | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 12.4.2 | Ochrana súborov so záznamom udalostí | **A** |  |  | **S** | **S** | **S** | **R** | **C** |  |  |  |  |  |
| 12.4.3 | Záznamy činnosti správcov a operátorov systémov | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 12.4.4 | Synchronizácia času |  |  |  |  | **R** |  | **C** | **S** |  |  |  |  |  |
| 12.5.1 | Inštalácia software do operačných systémov | **A** | **I** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 12.6.1 | Riadenie technickej zraniteľnosti | **A** |  |  |  | **R** | **S** | **S** | **S** |  |  |  |  |  |
| 12.6.2 | Obmedzenia pri inštalácii software | **A** | **I** |  |  | **R** | **S** | **S** | **S** |  |  |  |  |  |
| 12.7.1 | Audit informačných systémov | **A** |  |  | **S** | **S** | **S** | **R** | **S** |  |  |  |  |  |
| **13 Komunikačná bezpečnosť** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13.1.1 | Sieťové opatrenia | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 13.1.2 | Bezpečnosť sieťových služieb | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 13.1.3 | Oddeľovanie sietí | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 13.2.1 | Politiky a postupy pri prenose informácií | **A** | **I** |  |  | **S** | **S** | **R** |  |  |  | **S** |  |  |
| 13.2.2 | Dohody o výmene informácií | **A** |  |  | **S** | **S** | **S** | **R** |  |  |  | **S** |  |  |
| 13.2.3 | Výmena elektronických správ | **A** | **I** |  | **S** | **R** | **S** | **C** |  |  |  | **S** |  |  |
| 13.2.4 | Zmluvy o mlčanlivosti alebo utajení | **A** |  |  | **S** | **S** | **S** | **S** | **S** | **S** |  | **R** | **S** |  |
| **14 Akvizícia, vývoj a údržba informačných systémov** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14.1.1 | Analýza a špecifikácia požiadaviek na bezpečnosť informačných systémov | **A** |  |  | **C** | **C** | **S** | **R** | **S** |  | **I** |  |  |  |
| 14.1.2 | Zabezpečenie prenosov vo verejných sieťach | **A** |  |  | **C** | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.1.3 | Bezpečnosť aplikačných transakcií | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.2.1 | Politika bezpečného vývoja | **A** |  |  | **C** | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.2.2 | Riadenie zmien počas vývoja | **A** |  |  | **C** | **R** | **S** | **C** | **S** |  | **C** |  |  |  |
| 14.2.3 | Technické preskúmanie aplikácií pri zmene platformy | **A** |  |  |  | **S** | **S** | **C** | **R** |  |  |  |  |  |
| 14.2.4 | Obmedzenia zmien v softvérových balíkoch | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.2.5 | Princípy bezpečného systémového inžinierstva | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.2.6 | Prostredie pre bezpečný vývoj | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.2.7 | Vývoj prostredníctvom externých zdrojov | **A** |  |  |  | **R** | **S** | **C** | **S** |  | **S** |  |  |  |
| 14.2.8 | Testovanie bezpečnosti systémov | **A** |  |  |  | **S** | **S** | **R** | **S** |  |  |  |  |  |
| 14.2.9 | Akceptačné testy systémov | **A** | **C** |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| 14.3.1 | Ochrana testovacích dát | **A** |  |  |  | **R** | **S** | **C** | **S** |  |  |  |  |  |
| **15 Riadenie vzťahov s dodávateľmi** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 15.1.1 | Politika informačnej bezpečnosti pre vzťahy s dodávateľmi | **A** |  |  | **C** | **C** | **S** | **R** | **S** |  | **C** |  |  |  |
| 15.1.2 | Ošetrenie bezpečnosti v zmluvách s dodávateľmi | **A** |  |  |  | **C** | **S** | **R** | **S** |  |  | **S** |  |  |
| 15.1.3 | Dodávateľské reťazce informačných a komunikačných technológií | **A** |  |  |  | **S** | **S** | **R** | **S** |  |  | **S** |  |  |
| 15.2.1 | Monitorovanie a preskúmavanie dodávateľských služieb | **A** |  |  |  | **R** | **S** | **S** | **C** |  |  | **S** |  |  |
| 15.2.2 | Riadenie zmien v službách dodávateľa | **A** |  |  |  | **R** | **S** | **S** | **C** |  |  |  |  |  |
| **16 Riadenie incidentov v informačnej bezpečnosti** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16.1.1 | Zodpovednosti a postupy | **A** |  |  | **C** | **S** | **S** | **R** | **S** | **S** |  | **C** |  | **S** |
| 16.1.2 | Informovanie o udalostiach informačnej bezpečnosti | **A** | **R** |  |  | **S** | **S** | **R** | **S** |  |  |  |  | **S** |
| 16.1.3 | Informovanie o slabinách informačnej bezpečnosti | **A** | **R** |  |  | **S** | **S** | **R** | **S** |  |  |  |  | **S** |
| 16.1.4 | Posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich | **A** |  |  | **C** | **S** | **S** | **R** | **S** | **S** |  | **C** |  | **S** |
| 16.1.5 | Riešenie incidentov informačnej bezpečnosti | **A** |  |  | **S** | **S** | **S** | **R** | **S** | **S** |  | **C** | **C** | **S** |
| 16.1.6 | Poučenie sa z incidentov informačnej bezpečnosti | **A** |  |  | **S** | **C** | **S** | **R** | **S** | **C** |  |  | **C** | **C** |
| 16.1.7 | Zber dôkazov | **A** |  |  | **S** | **S** | **S** | **R** | **S** | **S** |  | **C** |  | **S** |
| **17 Informačná bezpečnosť a kontinuita činností** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 17.1.1 | Plánovanie kontinuity informačnej bezpečnosti | **A** |  |  |  | **S** | **S** | **R** | **S** |  |  |  |  | **S** |
| 17.1.2 | Implementovanie kontinuity informačnej bezpečnosti | **A** |  |  | **S** | **S** | **S** | **R** | **S** |  |  |  |  | **S** |
| 17.1.3 | Overenie, preskúmanie a vyhodnotenie kontinuity informačnej bezpečnosti | **A** |  |  |  | **S** |  | **R** | **S** |  |  |  |  | **S** |
| 17.2.1 | Dostupnosť zariadení na spracúvanie informácií | **A** |  |  | **S** | **R** | **S** | **C** | **S** |  |  |  |  | **S** |
| **18 Súlad** | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 18.1.1 | Identifikácia platnej legislatívy a zmluvných požiadaviek | **A** | **I** |  | **C** | **S** | **S** | **S** |  |  |  | **R** |  | **S** |
| 18.1.2 | Práva duševného vlastníctva, autorské a licenčné práva | **A** | **I** |  | **C** | **S** | **S** | **S** |  |  |  | **R** |  |  |
| 18.1.3 | Ochrana záznamov | **A** | **I** |  | **S** | **R** | **S** | **S** | **S** |  |  |  |  |  |
| 18.1.4 | Ochrana osobných údajov | **A** | **I** |  | **S** | **S** | **S** | **C** | **S** |  |  | **R** |  | **S** |
| 18.1.5 | Riadenie šifrovania | **A** |  |  |  | **S** | **S** | **R** | **S** |  |  | **C** |  |  |
| 18.2.1 | Preskúmavanie úrovne informačnej bezpečnosti | **I** |  |  | **S** | **C** | **S** | **A** | **R** |  |  |  |  | **S** |
| 18.2.2 | Súlad s bezpečnostnými politikami a normami | **I** | **I** |  | **S** | **S** | **S** | **A** | **R** |  |  | **C** |  | **S** |
| 18.2.3 | Preskúmavanie technického súladu | **I** |  |  | **S** | **S** | **S** | **A** | **R** |  |  | **C** |  |  |

Jednotlivé bezpečnostné opatrenia, metodické pokyny ako aj role a zodpovednosti budú na úrovni Centra vždy prekonzultované s jednotlivými zúčastnenými stranami (MIB – ÚOŠS) s cieľom overenia ich uplatnenia v praxi, identifikácie možných problémov (napr. formou workshopov zameraných na konkrétnu oblasť). Je potrebné vylúčiť situácie, pri ktorých nebude možné navrhnuté opatrenia implementovať v praxi.

## Klasifikácia informácie a systémov

* filozofia FIPS 199 a FIPS 200,
* chýba zoznam typov informácie, ktoré je potrebné rozlišovať
* možno by bolo dobré spraviť zoznam typov systémov, aby sme si vedeli predstaviť, na čo sa budú všeobecné požiadavky aplikovať a či to je relevantné

### Význam a podstata klasifikácie informácií a kategorizácie  systémov

1. v prvom rade potrebujeme zaistiť dôvernosť, integritu, dostupnosť, autentickosť informácie (CIAA), lebo od toho závisí kvalita rozhodovania, dostupnosť, spoľahlivosť a kvalita služieb
2. rôzne informácie si vyžadujú rôznu úroveň ochrany, bezpečnostné požiadavky na systémy sa odvodzujú od bezpečnostných požiadaviek na informáciu, ktorá sa prostredníctvom nich spracováva
3. okrem základných bezpečnostných požiadaviek existujú aj ďalšie – zachovanie súkromnosti (privacy) informácie, nepopretie pôvodu, nepopretie doručenia a i.
4. úroveň bezpečnostných potrieb systému sa určuje pomocou analýzy rizík a
5. systémov pomocou ktorých sa spracováva, prenáša alebo uchováva informácia je príliš veľa na to, aby bolo možné pre každý z nich robiť analýzu rizík
6. bežné systémy však využívajú štandardné technológie (hardvér aj programové vybavenie) , spracovávajú sa v nich informácie s podobnými bezpečnostnými požiadavkami a bezpečnostné požiadavky na ochranu týchto systémov sa veľmi nelíšia
7. klasifikácia informácie a kategorizácia systémov umožňuje zjednodušiť ochranu systémov tým, že definuje typy informácie, stanoví úroveň bezpečnostných požiadaviek na jednotlivé typy, na základe toho, aké typy informácie sa v systéme spracovávajú určí (bezpečnostnú) kategóriu systému. Pre jednotlivé kategórie systémov sú definované súbory opatrení, ktoré postačujú na dosiahnutie požadovanej úrovne ochrany systému. Súbory opatrení sa ešte upravujú podľa požiadaviek na úroveň ochrany z hľadiska CIAA, resp. špecifických potrieb majiteľa systému.
8. klasifikácia informácie a kategorizácia systémov je podstatne jednoduchšia ako analýza rizík a štandardné súbory opatrení sa dajú udržiavať centrálne
9. ďalšími výhodami štandardizovaného riešenia je kompatibilita a zaručenie potrebnej úrovne ochrany

### Realizácia

1. potrebujeme právny základ
2. typy informácie a stanovenie úrovní ochrany pre jednotlivé typy
3. klasifikačnú schému (neformálne popísaná vyššie)
4. súbory opatrení pre jednotlivé kategórie systémov (štandardne 3)
5. niekoho, kto bude sledovať vývoj hrozieb, objavovanie sa zraniteľností a aktualizovať súbory opatrení
6. aj USA, aj Nemecko majú štandardizované súbory opatrení pre ich analógiu ISVS

## Zoznam bezpečnostných rolí a kvalifikačné požiadavky na jednotlivé roly

1. máme detailne rozpracované znalostné štandardy pre
2. laikov
3. vedúcich pracovníkov
4. informatikov
5. špecialistov v IB/KB (manažéri IB/KB)
6. znalostné štandardy pre informatikov sú použiteľné aj pre učiteľov IB/KB pre stredné a základné školy (ale chýba metodika vyučovania)
7. znalostné štandardy pokrývajú nasledujúce oblasti

## Systém vzdelávania v IB/KB

1. existuje Vládou schválený materiál, ktorý sa podarilo realizovať len čiastočne, nevyrábajme ďalší, ale skúsme rozbehnúť prípravu kvalifikovaných ľudí v čo najkratšom čase:
2. stanovme priority – akých ľudí štátny sektor akútne potrebuje
3. máme definované znalostné štandardy;
4. máme podrobné sylaby a učebné texty;
5. zrevidujme existujúce materiály a doplňme ich (analýza použiteľnosti materiálov zo vzdelávacieho  projektu MF SR je hotová)
6. spravme inventarizáciu vzdelávacích kapacít (v prvom rade ľudí, až potom inštitúcií)
7. pripravme a spustime pilotný projekt na vyškolenie týchto ľudí (úvodné školenia, praktické vzdelávanie, cyklické celoživotné vzdelávanie)
8. vyhodnoťme pilotný projekt (resp., ak to chceme skrátiť, vychádzajme z poznatkov zo vzdelávacieho projektu MF SR) – obsah, formy, témy, ktoré by bolo treba doplniť, výber ľudí, metodika vzdelávania, skúšky, certifikát
9. identifikujme inštitúcie, ktoré by sa dali použiť ako školiace pracoviská, ponúknime im metodickú (technickú a materiálnu?) pomoc, zorganizujeme školenia lektorov, prípadne stáže vo fungujúcich inštitúciách
10. vysoké školy (TU Žilina, UPJŠ a TU Košice)
11. špeciálne vysoké školy a vzdelávacie inštitúcie (Liptovský Mikuláš, Policajná akadémia Bratislava, Justičná akadémia (?) Bratislava)
12. formy
13. rozšírenie obsahu existujúcich študijných programov o IB/KB, resp. doplnenie výberovej výučby
14. plné vzdelávanie podľa študijných programov vypracovaných centrálne
15. spustíme vzdelávanie v školiacich pracoviskách

## Návrh postupu systematického riešenia informačnej/kybernetickej bezpečnosti v SR

### národná/štátna úroveň

1. čo treba upratať v legislatíve a kompetenciách, zdôraznenie nepokrytých oblastí
2. vybudovanie centrálnych odborných kapacít (na začiatku budú asi virtuálne, viazané na štátnu inštitúciu (NBU, ÚPVII?) poskytujúcou organizačné a finančné zabezpečenie a s nejakým koordinačným orgánom), ktoré budú plniť (bude treba začať postupne a potom sa uvidí, či je rozumné sústreďovať ich a ak áno, ktoré)
   1. metodické a koncepčné úlohy
   2. tvorba legislatívy, sledovanie európskej a slovenskej pripravovanej legislatívy (opravy, koordinácia – ale na to potrebujeme garanta s dostatočnou autoritou, aby to dokázal presadiť)
   3. štandardizácia v oblasti IB/KB – medzinárodná (výber medzinárodných štandardov, ktoré budú zaradené do STN a podpora ich prebratia/prekladu; tvorba domácich štandardov)
   4. bezpečnostné štandardy pre ISVS a odporúčané pre ostatných; najmä systémy patriace do bezpečnostného okolia ISVS
   5. certifikácia a akreditácia systémov, nezávislý audit a testovanie
   6. terminológia
   7. vlastný výskum v kľúčových oblastiach
   8. stimulácia a koordinácia výskumu v IB/KB (účasť na tvorbe programov, činnosti grantových agentúr a pod.)
   9. klasifikácia informácie a systémov (metodika klasifikácie a kritériá pre klasifikáciu, možno kategorizácia = stanovenie typov informácie)
   10. požiadavky na základnú úroveň ochrany (analógia Grundschutz BSI) a ich udržiavanie (sledovanie vývoja hrozieb, objavovania zraniteľností, posudzovanie nových systémov a technológií)
   11. sledovanie úrovne IB/KB na Slovensku (raz za dva roky prieskum stavu IB a predloženie do Vlády s návrhom opatrení)
   12. kontrola, testovanie a audit bezpečnosti ISVS (tieto funkcie budú primárne musieť plniť aj štátne orgány v okruhu svojej pôsobnosti, ale v prípade vážnych problémov by takéto funkcie mal kvôli nezávislej kontrole mať možnosť vykonávať aj centrálny orgán)
   13. znalostné štandardy (aké znalosti a zručnosti v IB/KB potrebujeme, koľko akých ľudí) požiadavky na vzdelávanie (akreditácia programov), možno vzdelávanie vybraných skupín ľudí (kvôli spätnej väzbe a overovaniu metodiky)
   14. podpora vzdelávania v IB/KB na vzdelávacích inštitúciách (technická IB/KB, manažérska, právnici, vyšetrovatelia)
   15. cvičenia v IB/KB (účasť na medzinárodných, organizácia národných cvičení)
   16. zastupovanie SR v odborných orgánoch (pracovných skupinách) EÚ, NATO a iných organizácií a využívanie (použiteľných) informácií (semináre);
3. centrálne operačné kapacity na riešenie globálnych bezpečnostných incidentov a rozsiahlych útokov na slovenský virtuálny priestor (monitoring slovenského virtuálneho priestoru a jeho častí; identifikácia príznakov útokov a organizácia obrany – armáda? a CSIRTy);
4. budovanie globálneho obranného systému slovenského virtuálneho priestoru
5. vytváranie/zvyšovanie bezpečnostného povedomia používateľov
6. budovanie odborných kapacít na zabezpečenie existujúcich systémov (rutinná prevádzka) (príloha 8.9)

### CSIRT

1. zmapovanie potrieb verejnej správy v oblasti podpory pri riešení bezpečnostných incidentov (Koľko a akých útvarov CSIRT bude treba v optimálnom prípade, čo je nutné minimum,. kde by mali byť zriadené a postup pri ich budovaní)
2. podpora existujúcich útvarov CSIRT
3. využívanie existujúcich útvarov CSIRT na prípravu odborníkov pre nové útvary CSIRT
4. dohoda o spolupráci
5. podpora pri medzinárodnom etablovaní nových útvarov
6. vytvorenie cvičného akademického útvaru CSIRT (SANET, vysoké školy, ale najmä príprava ľudí pre prax)

### Ministerstvá a im na roveň postavené štátne orgány

1. inštitúcie zodpovedné za rezort alebo oblasť
2. ustanovenie človeka zodpovedného za IB/KB – bezpečnostný manažér rezortu
3. týchto ľudí budeme asi musieť vyškoliť,  pripraviť im návrh postupu a poskytovať minimálne metodickú, ale asi aj odbornú pomoc (výnimiek nebude veľa)
4. bezpečnostný manažér (s prípadnou pomocou externých odborníkov) zabezpečí zmapovanie stavu IB/KB v rezorte (kritické informačné systémy)
5. stručná koncepcia (čo rezort v IB/KB potrebuje) a postup, ako to dosiahnuť
6. ale súčasne s koncepčnými a analytickými prácami presadzovanie štandardizovaných riešení

### Štátne inštitúcie (stredná a nižšia úroveň)

1. inštitúcie zodpovedajúce za ISVS alebo prevádzkujúce ISVS
2. na podnet/príkaz nadriadeného orgánu zriadenie funkcie bezpečnostného manažéra
3. vyškolenie bezpečnostného manažéra (uvidíme, koľko ich treba, môžeme poskytnúť metodické materiály, pri zvládnuteľnom počte ich aj školiť centrálne)
4. jednoduchý bezpečnostný projekt organizácie, bezpečnostná politika
5. školenia zamestnancov
6. podobne ako v prípade ministerstiev súčasne s koncepčnými a analytickými prácami presadzovanie štandardizovaných riešení

### Špeciálne systémy a aplikácie

1. pozrieť sa či neexistujú ISVS, pre ktoré nestačí uplatnenie štandardných postupov z častí Ministerstvá a im na roveň postavené štátne orgány a Štátne inštitúcie (stredná a nižšia úroveň)
2. kritická informačná infraštruktúra – štátna, súkromná, iná (Direktíva NIS)
3. systémy súvisiace s e-Gov (ÚPVS, referenčné registre, systémy pre manažment identity)
4. utajované skutočnosti
5. osobné údaje
6. majú inštitúcie prevádzkujúce takéto ISVS dostatočne kvalifikovaných ľudí?
7. ak nie,
8. vyškoliť ľudí
9. spraviť analýzu rizík
10. bezpečnostné projekty na špeciálne systémy
11. zavedenie ISMS
12. správa rizík, priebežné monitorovanie a nezávislý audit
13. ak áno, bezpečnostný projekt a ostatné si spravia sami (stačí skontrolovať)
14. povinná certifikácia a akreditácia (kto to bude robiť?)

### Systémy ktoré nie sú ISVS

1. pre tie, ktoré nie sú pripojené k ISVS majú bezpečnostné štandardy a baseline ochrana len charakter odporúčaní
2. systémy, ktoré komunikujú s ISVS musia spĺňať podmienky na pripojenie, aby neohrozili ISVS

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-1)
2. niekedy sa uvádzajú len tri confidentiality, integrity, availability, CIA, pričom integrita zahŕňa aj autentickosť [↑](#footnote-ref-2)
3. obrázok je prevzatý z normy ISO/IEC 27032:2012 [↑](#footnote-ref-3)
4. Internet Security Threat Report 2017, https://www.symantec.com/security-center/threat-report [↑](#footnote-ref-4)
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-5)
6. podrobnejší zoznam na <http://cordis.europa.eu/search/result_en?q=cybersecurity> obsahuje 165 položiek [↑](#footnote-ref-6)
7. s výnimkou systémov, ktoré sú izolované, alebo zapojené len do vyhradených sietí [↑](#footnote-ref-7)
8. Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008. [↑](#footnote-ref-8)
9. schválená uznesením vlády SR č. 328/2015 [↑](#footnote-ref-9)
10. § 4, ods. 2), písm. f) zákona č. 275/2006 Z .z. [↑](#footnote-ref-10)
11. § 10b zákona č. 110/2004 Z. z. [↑](#footnote-ref-11)
12. GSI 2017, International Telecommunication Union (ITU) 2017, s.20 Methodology [↑](#footnote-ref-12)
13. Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike, MF SR, 2013 [↑](#footnote-ref-13)
14. https://www.csirt.gov.sk [↑](#footnote-ref-14)
15. IP adresy pridelené subjektom v Slovenskej republike, webové portály a služby v rámci TLD domény .sk [↑](#footnote-ref-15)
16. 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-16)
17. Z výnimkou vysoko zabezpečených infraštruktúr [↑](#footnote-ref-17)
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-18)
19. blízko k tomu má ale len 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, ochota počúvať odborné argumenty a schopnosť presadzovať navrhované riešenia [↑](#footnote-ref-19)
20. analyzoval a pripravil návrh na zosúladenie [↑](#footnote-ref-20)
21. katalóg hrozieb, zraniteľností a opatrení Spolkového úradu pre informačnú bezpečnosť má niekoľko tisíc strán [↑](#footnote-ref-21)
22. Stále je aktuálny Systém vzdelávania v informačnej bezpečnosti, schválený Vládou SR v roku 2009 [↑](#footnote-ref-22)
23. majú sa na mysli zmluvy zahŕňajúce spoluprácu v IB/KB [↑](#footnote-ref-23)
24. GCI 2017, International Telecommunication Union (ITU) 2017, s. 17 CGI Pillars and Sub-pillars [↑](#footnote-ref-24)
25. IP adresy pridelené subjektom v Slovenskej republike, webové portály a služby v rámci TLD domény .sk [↑](#footnote-ref-25)
26. 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-26)
27. Pozn. rok 2016, je potrebné prepočítať za predchádzajúce obdobie [↑](#footnote-ref-27)
28. Z výnimkou vysoko zabezpečených infraštruktúr [↑](#footnote-ref-28)
29. [↑](#footnote-ref-29)
30. Analýza rizík je iba formálna alebo chýba úplne [↑](#footnote-ref-30)
31. S vylúčením útoku na celý perimeter organizácie pri testovaní iba konkrétnej služby, projektu alebo časti perimetra [↑](#footnote-ref-31)
32. 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-32)
33. 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-33)