**Národná koncepcia informatizácia verejnej správy**

**Strategická priorita 10 Kybernetická bezpečnosť**

verzia 1.5

Bratislava, 01.10.2017

**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 |

Obsah

[1 Úvod 6](#_Toc494647084)

[2 Ciele dokumentu 6](#_Toc494647085)

[3 Adresáti dokumentu 6](#_Toc494647086)

[4 Základné pojmy a označenia 7](#_Toc494647087)

[4.1 Základné pojmy 7](#_Toc494647088)

[4.2 Skratky 8](#_Toc494647089)

[5 Súčasná situácia v IB/KB 9](#_Toc494647090)

[5.1 Koncepcia a legislatíva EÚ v kybernetickej bezpečnosti 9](#_Toc494647091)

[5.2 Informačná a kybernetická bezpečnosť SR a ISVS 10](#_Toc494647092)

[5.2.1 Legislatívny rámec IB/KB v SR 11](#_Toc494647093)

[5.2.2 Kompetencie 12](#_Toc494647094)

[5.2.3 Koncepcie informačnej a kybernetickej bezpečnosti a ich realizácia 12](#_Toc494647095)

[5.2.4 Know-how a personálne kapacity 13](#_Toc494647096)

[5.2.5 Hodnotenie stavu informačnej/kybernetickej bezpečnosti Slovenska podľa GSI 14](#_Toc494647097)

[5.2.6 Stav ochrany ISVS 15](#_Toc494647098)

[5.3 Zhrnutie stavu informačnej a kybernetickej bezpečnosti v SR 16](#_Toc494647099)

[6 Riešenia 16](#_Toc494647100)

[6.1 koncepcia, legislatíva, kompetencie 17](#_Toc494647101)

[6.2 Riadenie/koordinácia zabezpečenia slovenského virtuálneho priestoru 17](#_Toc494647102)

[6.3 Zabezpečenie základnej úrovne ochrany virtuálneho priestoru SR 18](#_Toc494647103)

[6.4 Budovanie odborných kapacít 18](#_Toc494647104)

[6.5 Budovanie bezpečnostného povedomia 19](#_Toc494647105)

[6.6 Zahraničná spolupráca 19](#_Toc494647106)

[7 Priority 20](#_Toc494647107)

[7.1 Ciele (návrh PS) 20](#_Toc494647108)

[7.2 Kritické faktory úspechu 20](#_Toc494647109)

[8 Ďalší postup 20](#_Toc494647110)

[9 Prílohy 20](#_Toc494647111)

[9.1 Zoznam skratiek 20](#_Toc494647112)

[9.2 Malý výkladový slovník 21](#_Toc494647113)

[9.3 Prehľad najdôležitejších dokumentov Informačnej a kybernetickej bezpečnosti SR (pracovný názov) 21](#_Toc494647114)

[9.4 Úlohy Akčného plánu na realizáciu Koncepcie kybernetickej bezpečnosti 22](#_Toc494647115)

[9.5 Kapacity SR v IB/KB 32](#_Toc494647116)

[9.5.1 Na riešenie incidentov informačnej bezpečnosti 32](#_Toc494647117)

[9.5.2 Organizácie 32](#_Toc494647118)

[9.5.3 Súkromné spoločnosti 32](#_Toc494647119)

[9.5.4 Vzdelávacie inštitúcie 32](#_Toc494647120)

[9.6 Hodnotenie Slovenskej republiky na základe ITU indexu 33](#_Toc494647121)

[9.7 Klasifikácia informácie a systémov 37](#_Toc494647122)

[9.7.1 Význam a podstata klasifikácie informácií a kategorizácie  systémov 37](#_Toc494647123)

[9.7.2 Realizácia 37](#_Toc494647124)

[9.8 Zoznam bezpečnostných rolí a kvalifikačné požiadavky na jednotlivé roly 38](#_Toc494647125)

[9.9 Systém vzdelávania v IB/KB 38](#_Toc494647126)

[9.10 Návrh postupu systematického riešenia informačnej/kybernetickej bezpečnosti v SR 39](#_Toc494647127)

[9.10.1 národná/štátna úroveň 39](#_Toc494647128)

[9.10.2 CSIRT 40](#_Toc494647129)

[9.10.3 Ministerstvá a im na roveň postavené štátne orgány 40](#_Toc494647130)

[9.10.4 Štátne inštitúcie (stredná a nižšia úroveň) 40](#_Toc494647131)

[9.10.5 Špeciálne systémy a aplikácie 40](#_Toc494647132)

[9.10.6 Systémy ktoré nie sú ISVS 41](#_Toc494647133)

# 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 základnými cieľmi sú

* definovať úlohy, ktoré štát potrebuje vyriešiť na to, aby zaistil primeranú úroveň bezpečnosti ISVS a ich bezpečnostného okolia;
* vysvetliť jednotlivým kategóriám zainteresovaných, aké úlohy majú 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 vypracovaný členmi pracovnej skupiny a v prípade jeho osvojenia si 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

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

# Základné pojmy 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

*[toto napíšeme nakoniec, keď budeme vedieť, aké pojmy sme v texte použili, zatiaľ skúsme robiť zoznam]*

*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, napájanie, personál, 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.

* aktívum
* hrozba
* zraniteľnosť
* bezpečnostný incident
* útok
* informačná bezpečnosť
* kybernetický priestor
* kybernetická bezpečnosť
* opatrenie/protiopatrenie
* riziko

## Skratky

AKOB

AKOBZaA

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

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

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[[1]](#footnote-1), dramaticky stúpa rozsah a závažnosť cielených útokov na IKT a údaje, ktoré sa v nich spracovávajú. Podľa najnovšej Správy EÚ[[2]](#footnote-2) 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, ba dokonca 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[[3]](#footnote-3), 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 (p. Kašíková, p. Šimko)?

## 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[[4]](#footnote-4) 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&KBa 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).

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 nahradí 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 a NBÚ SR navyše nemá odborné kapacity na vykonávanie činností potrebných na zabezpečenie slovenského kybernetického priestoru.

### 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[[5]](#footnote-5) a Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020[[6]](#footnote-6). Obe koncepcie sa zhodli na rovnakých najdôležitejších prioritách.

MF SR, ktoré zodpovedalo za informačnú bezpečnosť vo verejnej správe do roku 2015 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

V roku 2015 prešli kompetencie v informačnej bezpečnosti (premenovanej na kybernetickú bezpečnosť) na NBÚ SR a 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, 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.

### Know-how a personálne kapacity

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, experná činnosť pre vládu, 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)

### 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[[7]](#footnote-7), prínosom údajov vychádzajúcich z GSI je jeho celosvetový záber, snaha o objektivizáciu porovnania a celkový trend vývoja v relatívnom porovnaní medzi krajinami, kde je zrejmé relatívne zaostávanie 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

Nedostatky popísané v predchádzajúcich častiach sa prejavujú aj v prístupe k ochrane ISVS a celkovej úrovni zabezpečenia ISVS. Posledný prieskum stavu informačnej bezpečnosti robilo MF SR v roku 2013[[8]](#footnote-8), súborné informácie o stave zabezpečenia ISVS chýbajú. Istý obraz o stave bezpečnosti ISVS dávajú výsledky CSIRT.SK[[9]](#footnote-9), ktorý rieši informačno-bezpečnostné incidenty v orgánoch verejnej správy a vykonáva aj penetračné testovanie (hľadanie zraniteľností, ktoré umožňujú útočníkovi preniknúť do systému). 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[[10]](#footnote-10), súborné informácie o stave zabezpečenia ISVS chýbajú.

Istý obraz o stave bezpečnosti ISVS dávajú výsledky CSIRT.SK[[11]](#footnote-11), ktorý rieši informačno-bezpečnostné incidenty v orgánoch verejnej správy a vykonáva aj penetračné testovanie (hľadanie zraniteľností, ktoré umožňujú útočníkovi preniknúť do systému).

Podľa zistení CSIRT.SK

Zistenia CSIRT.SK sú postavené na riešení bezpečnostných incidentov vo verejnej správe a IP adresnom priestore SR[[12]](#footnote-12), informácií získaných z threat intelligence platformy implementovanej CSIRT.SK[[13]](#footnote-13), 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 bolo v roku 2016 infikovaných 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[[14]](#footnote-14) percent 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[[15]](#footnote-15), 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[[16]](#footnote-16):

* **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[[17]](#footnote-17) 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[[18]](#footnote-18) bolo pri viac ako 90 percent penetračných testoch identifikovaná aspoň jedná závažná[[19]](#footnote-19) a/alebo kritick[[20]](#footnote-20)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)

## 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[[21]](#footnote-21) 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.**

# Riešenia

Stav informačnej/kybernetickej bezpečnosti v Slovenskej republike je neuspokojivý (FX) a za takýchto podmienok (legislatíva, odborné kapacity, zdroje, úroveň bezpečnostného povedomia) štát nedokáže zabezpečiť adekvátnu ochranu svojho virtuálneho priestoru. Takýto stav je vzhľadom na možné dôsledky vyradenia kritických IKT a/alebo systémov v masovom rozsahu neprijateľný. Vychádzajúc z poznania stavu, kritických problémov a disponibilných zdrojov a zohľadňujúc problémy s realizáciou predchádzajúcich koncepcií, navrhujeme na riešenie stavu IB/KB v SR nasledujúci postup

* rýchle riešenie kritických problémov (prostredníctvom legislatívy, vzdelávania, štandardizácie, koordinácie činnosti, medzinárodnej spolupráce, podporou existujúcich pracovísk)
* priebežne upresňovanie údajov o stave IB/KB v SR (monitorovanie a vyhodnocovanie bezpečnostných incidentov, inventarizácia odborných kapacít, možných zdrojov, analytická činnosť, cielený vedecký výskum)
* stanovenie priorít pre systematické riešenie (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, ktorého prijatie môže výrazne ovplyvniť stav IB/KB v SR.

## Riadenie/koordinácia zabezpečenia virtuálneho priestoru VS

## Zabezpečenie základnej úrovne ochrany virtuálneho priestoru SR

Z centrálnej úrovne (autorita zodpovedná za informačnú/kybernetickú bezpečnosť IS VS)

## 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

## 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.

## 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).

# 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)

## Kritické faktory úspechu

(vrátane všetkých relevantných predpokladov

# Ďalší postup

# Prílohy

## Zoznam skratiek

spravíme po napísaní dokumentu, podľa rozsahu buď pôjde na začiatok dokumentu alebo do príloh

## 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 (schválený Vládou SR v roku 2016)

## 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

* Slovak Telekom?

### Organizácie

* Slovenská asociácia pre informačnú bezpečnosť
* ISACA Slovensko

### Súkromné spoločnosti

* Eset

### Vzdelávacie inštitúcie

* UK (FMFI UK – kryptológia, manažment IB, bezpečnosť počítačových systémov a sietí, učiteľstvo informatiky, Práv. Fakulta – počítačové právo, právo duševného vlastníctva, Fakulta manažmentu Manažment IB)
* STU (FEI STU – Kryptológia a informačná bezpečnosť, FIIT - manažment IB, bezpečnosť počítačových systémov a sietí)
* 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:



## 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

* v prvom rade potrebujeme zaistiť dôvernosť, integritu, dostupnosť, autentickosť informácie (CIAA), lebo od toho závisí kvalita rozhodovania, dostupnosť, spoľahlivosť a kvalita služieb
* rôzne informácie si vyžadujú rôznu úroveň ochrany, bezpečnostné požiadavky na systémy sa odvodzujú od bezpečnostných požiadaviek na informáciu, ktorá sa prostredníctvom nich spracováva
* okrem základných bezpečnostných požiadaviek existujú aj ďalšie – zachovanie súkromnosti (privacy) informácie, nepopretie pôvodu, nepopretie doručenia a i.
* úroveň bezpečnostných potrieb systému sa určuje pomocou analýzy rizík a
* systémov pomocou ktorých sa spracováva, prenáša alebo uchováva informácia je príliš veľa na to, aby bolo možné pre každý z nich robiť analýzu rizík
* 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
* 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.
* klasifikácia informácie a kategorizácia systémov je podstatne jednoduchšia ako analýza rizík a štandardné súbory opatrení sa dajú udržiavať centrálne
* ďalšími výhodami štandardizovaného riešenia je kompatibilita a zaručenie potrebnej úrovne ochrany

### Realizácia

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

## Zoznam bezpečnostných rolí a kvalifikačné požiadavky na jednotlivé roly

* máme detailne rozpracované znalostné štandardy pre
* laikov
* vedúcich pracovníkov
* informatikov
* špecialistov v IB/KB (manažéri IB/KB)
* znalostné štandardy pre informatikov sú použiteľné aj pre učiteľov IB/KB pre stredné a základné školy (ale chýba metodika vyučovania)
* znalostné štandardy pokrývajú nasledujúce oblasti

## Systém vzdelávania v IB/KB

* existuje Vládou schválený materiál, ktorý sa podarilo realizovať len čiastočne, nevyrábajme ďalší, ale skúsme rozbehnúť prípravu kvalifikovaných ľudí v čo najkratšom čase:
* stanovme priority – akých ľudí štátny sektor akútne potrebuje
* máme definované znalostné štandardy;
* máme podrobné sylaby a učebné texty;
* zrevidujme existujúce materiály a doplňme ich (analýza použiteľnosti materiálov zo vzdelávacieho  projektu MF SR je hotová)
* spravme inventarizáciu vzdelávacích kapacít (v prvom rade ľudí, až potom inštitúcií)
* pripravme a spustime pilotný projekt na vyškolenie týchto ľudí (úvodné školenia, praktické vzdelávanie, cyklické celoživotné vzdelávanie)
* 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
* 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
* vysoké školy (TU Žilina, UPJŠ a TU Košice)
* špeciálne vysoké školy a vzdelávacie inštitúcie (Liptovský Mikuláš, Policajná akadémia Bratislava, Justičná akadémia (?) Bratislava)
* formy
* rozšírenie obsahu existujúcich študijných programov o IB/KB, resp. doplnenie výberovej výučby
* plné vzdelávanie podľa študijných programov vypracovaných centrálne
* spustíme vzdelávanie v školiacich pracoviskách

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

### národná/štátna úroveň

* čo treba upratať v legislatíve a kompetenciách, zdôraznenie nepokrytých oblastí
* 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);
* 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);
* budovanie globálneho obranného systému slovenského virtuálneho priestoru
* vytváranie/zvyšovanie bezpečnostného povedomia používateľov
* budovanie odborných kapacít na zabezpečenie existujúcich systémov (rutinná prevádzka) (príloha )

### CSIRT

* 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)
* podpora existujúcich útvarov CSIRT
* využívanie existujúcich útvarov CSIRT na prípravu odborníkov pre nové útvary CSIRT
* dohoda o spolupráci
* podpora pri medzinárodnom etablovaní nových útvarov
* vytvorenie cvičného akademického útvaru CSIRT (SANET, vysoké školy, ale najmä príprava ľudí pre prax)

### Ministerstvá a im na roveň postavené štátne orgány

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

### Štátne inštitúcie (stredná a nižšia úroveň)

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

### Špeciálne systémy a aplikácie

* pozrieť sa či neexistujú ISVS, pre ktoré nestačí uplatnenie štandardných postupov z častí a
* kritická informačná infraštruktúra – štátna, súkromná, iná (Direktíva NIS)
* systémy súvisiace s e-Gov (ÚPVS, referenčné registre, systémy pre manažment identity)
* utajované skutočnosti
* osobné údaje
* majú inštitúcie prevádzkujúce takéto ISVS dostatočne kvalifikovaných ľudí?
* ak nie,
* vyškoliť ľudí
* spraviť analýzu rizík
* bezpečnostné projekty na špeciálne systémy
* zavedenie ISMS
* správa rizík, priebežné monitorovanie a nezávislý audit
* ak áno, bezpečnostný projekt a ostatné si spravia sami (stačí skontrolovať)
* povinná certifikácia a akreditácia (kto to bude robiť?)

### Systémy ktoré nie sú ISVS

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

1. Internet Security Threat Report 2017, https://www.symantec.com/security-center/threat-report [↑](#footnote-ref-1)
2. 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-2)
3. podrobnejší zoznam na <http://cordis.europa.eu/search/result_en?q=cybersecurity> obsahuje 165 položiek [↑](#footnote-ref-3)
4. s výnimkou systémov, ktoré sú izolované, alebo zapojené len do vyhradených sietí [↑](#footnote-ref-4)
5. Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008. [↑](#footnote-ref-5)
6. schválená uznesením vlády SR č. 328/2015 [↑](#footnote-ref-6)
7. GSI 2017, International Telecommunication Union (ITU) 2017, s.20 Methodology [↑](#footnote-ref-7)
8. Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike, MF SR, 2013 [↑](#footnote-ref-8)
9. https://www.csirt.gov.sk [↑](#footnote-ref-9)
10. Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike, MF SR, 2013 [↑](#footnote-ref-10)
11. https://www.csirt.gov.sk [↑](#footnote-ref-11)
12. IP adresy pridelené subjektom v Slovenskej republike, webové portály a služby v rámci TLD domény .sk [↑](#footnote-ref-12)
13. 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-13)
14. Pozn. rok 2016, je potrebné prepočítať za predchádzajúce obdobie [↑](#footnote-ref-14)
15. Z výnimkou vysoko zabezpečených infraštruktúr [↑](#footnote-ref-15)
16. [↑](#footnote-ref-16)
17. Analýza rizík je iba formálna alebo chýba úplne [↑](#footnote-ref-17)
18. S vylúčením útoku na celý perimeter organizácie pri testovaní iba konkrétnej služby, projektu alebo časti perimetra [↑](#footnote-ref-18)
19. 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-19)
20. 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-20)
21. 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-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)