

Kybernetická bezpečnosť a jej väzba na novo pripravovaný zákon o Kybernetickej bezpečnosti v Slovenskej republike

Mgr. Mário Italy, Ing. Ján Hochmann,
Národný bezpečnostný úrad



Obsah

1. **Aktivity Národného bezpečnostného úradu v roku 2015**
2. **Akčný plán kybernetickej bezpečnosti v SR ku Konceptii kybernetickej bezpečnosti 2015 - 2020**
3. **Štruktúra návrhu zákona o kybernetickej bezpečnosti**

Pôsobnosť a aktivity v roku 2015

- Prijatie zákona č. 339/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, ktorým bol **NBÚ ustanovený ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť**;
- Zriadenie **Komisie pre kybernetickú bezpečnosť**, ktorej štatút prerokovala vláda Slovenskej republiky a vzala na vedomie (č. m. UV-33740/2015);
- Prijatie zákona č. 346/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z., ktorým bol zriadený **Výbor pre kybernetickú bezpečnosť** Bezpečnostnej rady Slovenskej republiky.

Pôsobnosť orgánov štátnej správy v oblasti IB/KB

Ústredný orgán pre kybernetickú bezpečnosť

- NBÚ (od 1. 1. 2016 - kompetenčný zákon)

Koordinácia a riadenie

- MV SR (zákon č. 45/2011 Z. z. o kritickej infraštruktúre)
- MF SR (zákon č. 275/2006 Z. z. o ISVS)

Výkon v oblasti kritickej infraštruktúry - sektory

- MF SR, MDVRR SR, MH SR, MZ SR, MŽP SR

Špecifická oblasť

- MO SR (zákon o obrane SR, vojenská oblasť - NATO)

Východiská

- **Národná stratégia** pre informačnú bezpečnosť v Slovenskej republike (ďalej len „NSIB“), schválená uznesením vlády Slovenskej republiky č. 570/2008,
- Návrh **Akčného plánu** na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválený uznes. vlády SR č. 46/2010,
- **Legislatívny zámer zákona o IB**, schválený uznes. vlády SR č. 136/2010,

Východiská

- **Smernica Európskeho parlamentu a Rady** o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii,
- **Koncepcia kybernetickej bezpečnosti** Slovenskej republiky na roky 2015-2020, (uznes. vlády SR č. 328/2015).
- **Akčný plán ku Koncepcii kybernetickej bezpečnosti** SR na roky 2015 až 2020, (uznes. vlády SR č. 93/2016)

Východiská

Stratégia pre informačnú bezpečnosť v SR (MF SR)

- Uznesenie vlády SR č. 270/2008 (úloha - pripraviť legislatívny zámer zákona o informačnej bezpečnosti)

Legislatívny zámer zákona o informačnej bezpečnosti (MF SR)

- **Uznesenie vlády SR č. 136/2010** - rok 2012

Návrh zákona o informačnej bezpečnosti (MF SR)

- Návrh zákona o informačnej bezpečnosti vypracovaný v októbri 2014 (legislatívny proces zastavený)
- Plánovaný termín predloženia návrhu do vlády - 30. 12. 2016

Východiská

Návrh zákona o kybernetickej bezpečnosti (NBÚ)

- Uznesenie vlády SR č. 328/2015 ku Konceptii kybernetickej bezpečnosti
- Termín predloženia návrhu do vlády – február 2016,

Nová úloha:

- Zrušenie uznesení vlády SR č. 136/2010 a č. 328/2015 uznesením vlády SR č. 93/2016 a stanovenie termínu predloženia návrhu zákona o kybernetickej bezpečnosti v septembri 2016

Akčný plán ku Konceptii - oblasti

Sedem vecných oblastí a ich rozpracovanie v akčnom pláne ku kyber. bezpečnosti na roky 2015 - 2020

1. Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
2. Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
3. Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.

Akčný plán ku Konceptii - oblasti

4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej **bezpečnosti**.
5. Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
6. Aktívna medzinárodná spolupráca.
7. Podpora vedy a výskumu v oblasti kybernetickej **bezpečnosti**.

1. Vytvorenie inštitucionálneho rámca

1. Pripraviť návrh na vytvorenie formálnej platformy pre spoluprácu - NBÚ
2. Vytvoriť podmienky pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť vo svojej pôsobnosti - VPA
3. Zabezpečiť inštitucionálny rámec riadenia kybernetickej bezpečnosti - NBÚ
4. Budovať spôsobilosti jednotiek na riešenie incidentov CSIRT.SK/CERT
5. Vytvoriť rámec riadenia kybernetickej bezpečnosti v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny - MO SR
6. Vytvoriť medzirezortný/nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky“ - MO SR

2. Vytvorenie legislatívneho rámca

1. Vytvárať legislatívne podmienky pre oblasť kybernetickej bezpečnosti
NBU/MF SR
2. Zosúladiť súvisiace právne prepisy so zákonom o kybernetickej bezpečnosti
- NBÚ
3. Pripraviť, vykonávacie predpisy k zákonu o kybernetickej bezpečnosti a zabezpečiť ich legislatívny proces (schválenie)
- NBÚ
4. Vydávať štandardy, metodiky a metodické usmernenia v oblasti kybernetickej bezpečnosti
- NBÚ
5. Terminológia v oblasti kybernetickej bezpečnosti
NBÚ + UK, STU

3. Základné mechanizmy správy

1. Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore - NBÚ
2. V rámci mechanizmu prevencie zaviesť jednotné opatrenia z úrovne vecne príslušných autorít - VPA
3. Vytvoriť procesy a mechanizmy pri koordinácii zabezpečovania ochrany významných informačných aktív štátu na národnej úrovni – MF SR
4. Vytvoriť a implementovať systém včasného varovania a reakcie na incidenty
5. V rámci mechanizmu reakcie na bezpečnostné incidenty navrhnuť minimálne bezpečnostné opatrenia pre jednotlivé kategórie informačných aktív a zabezpečiť ich implementáciu - NBÚ
6. Aktualizovať plány riešenia krízových situácií pre oblasť kybernetickej bezpečnosti - NBÚ
7. Pravidelne vykonávať ohodnotenie úrovne bezpečnosti vo vládnych sieťach a kritických infraštruktúrach – MF SR penetračné testy

4. Zavedenie systému vzdelávania

1. **Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov:** MŠV VaŠ SR
 - všeobecného vzdelávania (základný a stredný stupeň)
 - odborného vzdelávania (stredný a vysokoškolský stupeň, špecialisti)
2. 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*), MŠV VaŠ SR

4. Zavedenie systému vzdelávania

3. **Zaviest'** inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti v rámci všeobecného vzdelávania (základný a stredný stupeň vzdelania) a **podporit'** odborné vzdelávanie (stredný a vysokoškolský stupeň vzdelania, špecialisti) v tejto oblasti,
MŠVVaŠ SR
4. 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
5. Zabezpečiť šírenie osvedy o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy učiteľov jednotlivých stupňov škôl,
NBÚ + ...

4. Zavedenie systému vzdelávania

6. rámci rozvoja siete Govnet a služieb ÚPVS rozšíriť obsah existujúcich školení aj o oblasť kybernetickej bezpečnosti, ÚV SR

Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o ďalšie špecifické oblasti a zabezpečiť pokračovanie vzdelávania, NBÚ

Realizovať školenia pracovníkov verejnej správy v oblasti ochrany informačných aktív voči kybernetickým útokom z externého prostredia,

MF SR + CSIRT.SK

7. V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov so zameraním na kybernetickú bezpečnosť, MO SR + APZ

V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov – špecialistov IKT so zameraním na kybernetickú bezpečnosť, MO SR + APZ

4. Zavedenie systému vzdelávania

8. Zaviesť minimálnu úroveň systematického vzdelávania pre všetkých sudcov, prokurátorov na všetkých úrovniach, MS SR
Zaviesť rozšírené vzdelávanie pre vybraných sudcov, prokurátorov na všetkých úrovniach, MS SR
9. Zaviesť minimálnu úroveň systematického vzdelávania v oblasti kybernetickej bezpečnosti pre vyšetrovateľov na všetkých úrovniach, MV SR
Zaviesť rozšírené vzdelávanie v oblasti kybernetickej bezpečnosti pre vybraných vyšetrovateľov na všetkých úrovniach, MV SR
10. 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

5. Kultúra riadenia rizík - spolupráca

1. Vytvoriť efektívny model spolupráce na národnej úrovni medzi jednotlivými subjektmi kybernetickej bezpečnosti - NBÚ
2. Implementovať systém nahlasovania a riešenia bezpečnostných incidentov NBÚ + MF SR/CSIRT.SK

5. Medzinárodná spolupráca

1. V rámci členstva v EÚ sa aktívne zúčastňovať na príprave a realizácii legislatívnych a nelegislatívnych iniciatív týkajúcich sa kybernetickej bezpečnosti
– NBÚ + MZVaEZ SR
2. V rámci členstva v NATO podporovať spoluprácu s NATO v oblasti kybernetickej obrany
- NBÚ
3. V rámci stredoeurópskeho priestoru rozvíjať vzťahy a nadväzovať bilaterálne spoluprácu s vybranými krajinami v oblasti kybernetickej bezpečnosti
4. Zapájať sa a zintenzívniť spoluprácu s Centrom výnimočnosti pre kybernetickú obranu (NATO Cooperative Cyber Defence Centre of Excellence – CCD CoE)
– NBÚ, MF SR, MO SR
5. Zintenzívniť spoluprácu s Centrom výnimočnosti pre kybernetickú obranu (NATO Cooperative Cyber Defence Centre of Excellence – CCD CoE)
MO SR

7. Podpora vedy a výskumu

1. Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti
– MŠV VaŠ SR
2. Podporovať budovanie forezných pracovísk – NBÚ + ÚOŠS SR

Štruktúra návrhu zákona o KB

Predmet zákona

- a) pôsobnosť orgánov štátnej správy na úseku kybernetickej bezpečnosti,
- b) práva a povinnosti fyzických a právnických osôb v oblasti kybernetickej bezpečnosti,
- c) pôsobnosť a požiadavky na útvary pre riešenie bezpečnostných incidentov v kybernetickom priestore,
- d) rámec notifikácie a riešenia bezpečnostných incidentov v kybernetickom priestore,
- e) klasifikáciu informácií a kategorizáciu IS,
- f) minimálne požiadavky na bezpečnosť jednotlivých kategórií IS počas ich životného cyklu,
- g) proces riadenia informačnej bezpečnosti,
- h) kontrolu bezpečnosti a audit bezpečnosti,
- i) spôsobilosti a vzdelávanie v kybernetickej bezpečnosti,
- j) zodpovednosť za porušenie povinností.

Správu na úseku kybernetickej bezpečnosti vykonávajú

§ 3

- Vláda Slovenskej republiky (ďalej len „vláda“)
- Národný bezpečnostný úrad (ďalej len „úrad“)
- Ústredný orgán štátnej správy podľa osobitného predpisu, ktorý je vecne príslušnou autoritou (ďalej len „ústredný orgán“)
- Jednotky a útvary pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“)

Povinné osoby na úseku kybernetickej bezpečnosti

§ 8

- osoby, ktoré sú správcami informačného systému verejnej správy podľa osobitného predpisu,
- prevádzkovatelia informačných systémov verejnej správy, ktoré sú významnými informačnými systémami,
- prevádzkovatelia prvkov kritickej infraštruktúry, pričom súčasťou týchto prvkov je časť digitálneho priestoru Slovenskej republiky podľa osobitného predpisu,
- poskytovatelia elektronických komunikačných sietí a poskytovatelia elektronických komunikačných služieb podľa osobitného predpisu,
- osoby, na ktoré sa vzťahujú všeobecné právne predpisy Slovenskej republiky, najmä poskytovatelia služieb informačnej spoločnosti podľa osobitného predpisu, prevádzkovatelia hazardných hier podľa osobitného predpisu a poskytovatelia služieb podľa osobitného predpisu.
- *osoby podľa smernice EÚ o NIS, ktoré nie sú uvedené v písm. a) až e).*

Ďakujeme za pozornosť



eFOCUS