Akčný plán realizácie Koncepcie kybernetickej bezpečnosti SR na roky 2015 – 2020

Bratislava, máj 2016

Ján Hochmann
Národný bezpečnostný úrad

Obsah

1. Pôsobnosť a aktivity Národného bezpečnostného úradu v roku 2015
2. Digitálny priestor / kybernetický priestor
3. Stratégia, koncepcia a Akčný plán kybernetickej bezpečnosti v SR na roky 2015 - 2020

Aktivity NBÚ - 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 SR v čase mieru v znení zákona č. 319/2012 Z. z, ktorým bol zriadený **Výbor pre kybernetickú bezpečnosť** Bezpečnostnej rady SR.

Pôsobnosť orgánov štátnej správy

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)

Dokumenty

- **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,

Dokumenty

- **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)

Dokumenty

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

- **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

Dokumenty

Návrh zákona o kybernetickej bezpečnosti (NBÚ)

- **Uznesenie vlády SR č. 328/2015** ku Koncepcii 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**

Definičné vymedzenie pôsobnosti

1. **Digitálny priestor je súhrn**

   a) **informačných a komunikačných technológií**, vrátane ich programového vybavenia a informačných systémov a sietí,

   b) **informácií, vrátane údajov**, ktoré sa prenášajú, spracovávajú alebo uchovávajú prostredníctvom informačných a komunikačných technológií alebo opisujú štruktúru, konfiguráciu a činnosť informačných a komunikačných technológií,

   c) **procesov**, ktoré prebiehajú v rámci informačných a komunikačných technológií,

   d) **podpornej infraštruktúry** zabezpečujúcej činnosť informačných a komunikačných technológií, vrátane elektronických komunikačných sietí, a

   e) **vzťahov** medzi údajmi a informáciami podľa druhého bodu a pravidiel upravujúcich tieto vzťahy,

Definičné vymedzenie pôsobnosti

2. **Digitálnym priestorom**

   a) **štátu** alebo organizácie je časť digitálneho priestoru v ich pôsobnosti, pričom táto organizácia alebo štát majú právo určovať pravidlá a spôsob fungovania príslušnej časti digitálneho priestoru a majú prostriedky na presadzovanie týchto pravidiel,

   b) Slovenskej republiky je časť digitálneho priestoru v pôsobnosti Slovenskej republiky, na ktorý sa vzťahujú všeobecné právne predpisy Slovenskej republiky

3. **Kybernetickým priestorom**

   je časť digitálneho priestoru pozostávajúca zo všetkých informačných systémov prepojených na globálnej dátovej úrovni, pričom jej základom je Internet; informačný systém alebo prvok v izolovanom priestore nie je súčasťou kybernetického priestoru!

Stratégia, Koncepcia a Akčný plán kybernetickej bezpečnosti v SR

- **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,
- Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií 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. ..../2016)

Koncepcia kybernetickej bezpečnosti 2015 až 2020

Sedem vecných oblastí a ich rozpracovanie v akčnom pláne

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.
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 riadenia kybernetickej bezpečnosti.

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 a prijatie legislatívneho rámca kybernetickej bezpečnosti

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 + univerzity

3. Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru

1. Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore - NBU
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 navrhnúť 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. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti

1. Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov: MŠVVaŠ 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)*, MŠVVaŠ SR

4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti

3. 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

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 osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy učiteľov jednotlivých stupňov škôl, NBÚ + ...

4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti

6. V 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. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti

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. Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami

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

6. Aktívna 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 v oblasti kybernetickej bezpečnosti

1. Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti – MŠVVaŠ SR

2. Podporovať budovanie forenzných pracovísk – NBÚ + ÚOŠS SR

ĎAKUJEM ZA POZORNOSŤ