KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SR NA ROKY 2015-2020

ITAPA 2015, Bratislava, 4. novembra 2015

Mgr. Mário Italy

riaditeľ sekcie informačnej bezpečnosti a elektronického podpisu NBÚ

OBSAH

1. Východiská
2. Legislatívny proces
3. Opatrenia vyplývajúce z koncepcie
4. Aktuálne úlohy vyplývajúce z koncepcie

Východiská – čo predchádzalo prijatiu koncepcie

- záväzky SR ako členskej krajiny EÚ a NATO
- úloha uložená vedúcemu ÚV SR uznesením vlády SR č. 276 zo dňa 4. júna 2014 vypracovať Koncepciu kybernetickej bezpečnosti SR

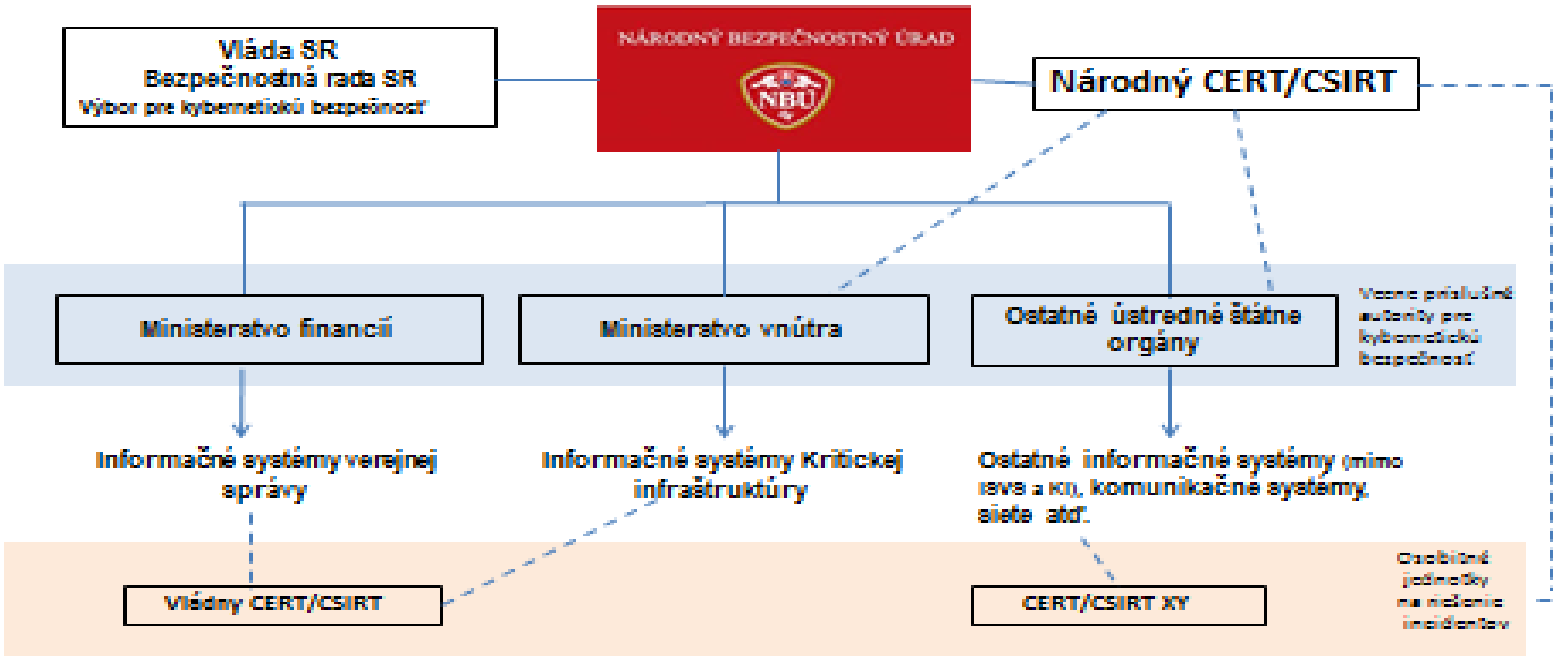
Legislatívny proces koncepcie

08/2014-02/2015	• **MPS na prípravu koncepcie** (ÚV SR, MF SR, NBÚ, MDPaRR SR, MŠVVaŠ SR, MO SR, SIS)
19.2.-25.2.2015	• **Medzirezortné pripomienkové konanie** (skrátené)
15.6.2015	• **MPK ukončené** (celkovo 95 pripomienok/52 zásadných => všetky pripomienky vysporiadané)
17.6.2015	• Schválená **uznesením vlády SR č. 328** zo 17. júna 2015

Opatrenia vyplývajúce z koncepcie

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

Opatrenie č.1:
Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.



CERT – Community Emergency Response Team
CSIRT – Computer Security Incident Response Team

Obrázok č. 1 Návrh rámcovej štruktúry riadenia kybernetickej bezpečnosti

Opatrenie č.2:
Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.

- prijať novelu kompetenčného zákona
- prijať osobitný zákon o kybernetickej bezpečnosti
- stanoviť záväznú terminológiu a štandardy
- vydať metodické usmernenia pre praktickú aplikáciu zákona a štandardov

Opatrenie č.3:
Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.

Na národnej úrovni rozpracovať základné mechanizmy zabezpečenia správy kybernetického priestoru a zabezpečiť ich aplikáciu:

1. **mechanizmus rozhodovania a riadenia**
   - opatrenie na minimalizáciu kybernetických bezpečnostných hrozieb a rizík a na zabránenie ich prerastania do krízových situácií,
   - vypracovávanie krízových plánov riešenia krízových situácií, atď.
2. **mechanizmus prevencie**
   - odborná príprava personálu v oblasti IKT, posilňovanie bezpečnostného povedomia obyvateľstva v oblasti IKT, technická/technologická podpora
3. **mechanizmus reakcie**
   - ako kvalifikovane a efektívne reagovať v prípade incidentu, alebo vzniku krízovej situácie,
4. **mechanizmus obnovy**

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

1. Spracovať návrh komplexného zabezpečenia vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov:

- všeobecného vzdelávania v SR na úrovni:
  - základného stupňa vzdelania,
  - stredného stupňa vzdelania,
- odborného vzdelávania na úrovni:
  - stredného stupňa vzdelania,
  - vysokoškolského stupňa vzdelania,
  - špecialistov.

Zodpovedný: MŠVVaŠ SR

2. Systematické šírenie osvety v oblasti kybernetickej bezpečnosti

Zodpovedný: MK SR

Opatrenie č.5:
Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami

1. Navrhnúť a vytvoriť riadiace a výkonné štruktúry s jasne vymedzenými pôsobnosťami, kompetenciami a stanovenými pravidlami vzájomnej komunikácie a súčinnosti na národnej úrovni.

2. Vypracovať a implementovať projekt systému on-line riadenia rizík a komunikácie medzi aktérmi zabezpečujúcimi funkčnosť systémov a služieb fungujúcich v národnom kybernetickom priestore, ako aj jeho ochranu a bezpečnosť (bezpečné systémy: výmeny informácií, včasného varovania a koordinovanej reakcie).

3. Vypracovať a implementovať projekt systému on-line nahlasovania a riešenia incidentov zahrňujúci používateľov systémov a služieb v rámci národného kybernetického priestoru.

4. Vypracovať a implementovať projekt správy a poskytovaných služieb registrov: identifikujúcich aktérov, ich pôsobnosť, kompetencie, poskytujúce služby a iné relevantné údaje.

Zodpovedný: NBÚ

Opatrenie č.6:
Medzinárodná spolupráca

- globálny charakter problematiky => vyžaduje si medzinárodnú spoluprácu
- členstvo v EÚ a NATO = povinnosť implementovať a transponovať legislatívne a koncepčné dokumenty
- národným kontaktným bodom pre EÚ a NATO v oblasti kybernetickej bezpečnosti bude ústredný orgán štátnej správy pre KB (NBÚ)
  - zabezpečuje a koordinuje plnenie úloh, vyplývajúcich z medzinárodnej spolupráce,
  - reprezentuje SR na medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
  - vypracúva konsolidované stanoviská a podklady pre politické a diplomatické rokovania
- organizácia a účasť na kybernetických cvičeniach (CyberCoalition, Locked Shield, Cyber Europe)
- dôraz na spoluprácu v rámci stredoeurópskeho regiónu:
  - Central European Cyber Security Platform (CECSP) – neformálna platforma krajín V4+Rakúska

Opatrenie č.7:
Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti

- **výskumné aktivity v oblasti KB bude koordinovať ústredný orgán štátnej správy pre KB (NBÚ)**
- **účasť na národných a európskych výskumných projektoch a aktivitách v oblasti KB**
- **dôraz na čerpanie finančných prostriedkov z Operačného programu Výskum a inovácie pre programové obdobie 2014-2020**

Aktuálne úlohy vyplývajúce z Koncepcie

1. **Novela kompetenčného zákona (zák.č. 575/2001 Z.z.)**

   zverenie kompetencie ÚOŠS v oblasti KB do pôsobnosti NBÚ

   T: ihneď Z: ÚV SR, NBÚ

   Riešenie úlohy: 2.čítanie v NR SR (ČPT 1730)

2. **Akčný plán realizácie Koncepcie kybernetickej bezpečnosti na roky 2015-2020**

   vecný, časový a finančný plán realizácie opatrení vyplývajúcich z koncepcie

   T: 12/2015 Z: NBÚ

   Riešenie úlohy: M+ÚOŠS do 10/2015 povinné zaslať podklady do Akčného plánu, NBÚ na základe podkladov v 12/2015 predloží do MPK návrh Akčného plánu

3. **Návrh zákona o kybernetickej bezpečnosti**

   T: 02/2016 Z: NBÚ

   Riešenie úlohy: príprava legislatívneho zámeru zákona o KB, 12/2015 PPK, 01/2016 MPK

Aktuálne úlohy vyplývajúce z Koncepcie

1. **Štatút Formálnej platformy pre spoluprácu verejnej správy, akademickej obce a súkromnej sféry**

   T: 09/2015 Z: ÚV SR

   Riešenie úlohy: Návrh Štatútu Komisie pre KB vzala vláda SR na vedomie 07.10.2015

   Komisia pre KB bude stálym poradným orgánom R NBÚ

   Komisia pre KB bude slúžiť na stály priamy dialóg medzi štátnymi a neštátnymi aktérmi kyberpriestoru SR

2. **Konsolidácia terminológie a jej zverejnenie v Terminologickom slovníku krízového riadenia**

   T: september 2015 Z: ÚV SR

   Riešenie úlohy: 24.09.2015 návrh terminológie predložený na rokovaní Terminologickej komisie BR SR

3. **Zriadenie Výboru BR SR pre kybernetickú bezpečnosť**

   Riešenie úlohy: Návrh novely zákona č. 110/2004 Z. z. o fungovaní BR SR v čase mieru v 2. čítaní v NR SR (ČPT 1646)

ĎAKUJEME

ZA POZORNOSŤ !