**Postavenie Úradu PVII v oblasti kritickej infraštruktúry:**

Základným pilierom pre ochranu kritickej infraštruktúry je Zákon č. 45/2011 Z. z. Zákon o kritickej infraštruktúre.

§ 1

Predmet zákona

(1) Tento zákon ustanovuje

a) organizáciu a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry,

b) postup pri určovaní prvku kritickej infraštruktúry,

c) povinnosti prevádzkovateľa pri ochrane prvku kritickej infraštruktúry a zodpovednosť za porušenie týchto povinností.

(2) Súčasťou kritickej infraštruktúry je obranná infraštruktúra podľa osobitného predpisu.

(§ 26 a 27 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 330/2003 Z. z.)

Organizácia a pôsobnosť orgánov štátnej správy na úseku kritickej infraštruktúry

§ 3

Štátnu správu na úseku kritickej infraštruktúry vykonávajú

a) vláda Slovenskej republiky (ďalej len „vláda“),

b) Ministerstvo vnútra Slovenskej republiky (ďalej len „ministerstvo“),

c) Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky a Ministerstvo zdravotníctva Slovenskej republiky (ďalej len „ústredný orgán“).

Príloha č. 3 k zákonu č. 45/2011 Z. z.

SEKTORY V PÔSOBNOSTI ÚSTREDNÝCH ORGÁNOV

|  |  |  |
| --- | --- | --- |
| **Sektor** | **Podsektor** | **Ústredný orgán** |
| 1. Doprava | Cestná doprava  Letecká doprava  Vodná doprava  Železničná doprava | Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky |
| 2. Elektronické komunikácie | Satelitná komunikácia  Siete a služby pevných a mobilných elektronických komunikácií | Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky |
| 3. Energetika | Baníctvo  Elektroenergetika  Plynárenstvo  Ropa a ropné produkty | Ministerstvo hospodárstva Slovenskej republiky |
| 4. Informačné a komunikačné technológie | Informačné systémy a siete  Internet | Ministerstvo financií Slovenskej republiky |
| 5. Pošta | Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť | Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky |
| 6. Priemysel | Farmaceutický priemysel  Hutnícky priemysel  Chemický priemysel | Ministerstvo hospodárstva Slovenskej republiky |
| 7. Voda a atmosféra | Meteorologická služba  Vodné stavby  Zabezpečovanie pitnej vody | Ministerstvo životného prostredia Slovenskej republiky |
| 8. Zdravotníctvo |  | Ministerstvo zdravotníctva Slovenskej republiky |

**ÚPVII v oblasti kritickej infraštruktúry môže vykonávať štátnu správu pre oblasť informačných a komunikačných technológií.**

**Je potrebné zistiť, či z MF SR prešli na ÚPVII všetky kompetencie v oblasti informačných systémov, ak áno tak vykonáva štátnu správu. V prípade, že sa to ešte nerozhodlo je v tom potrebné urobiť jasný záver.**

V kompetenčnom zákone Zákon č. 575/2001 Z. z. Zákon o organizácii činnosti vlády a organizácii ústrednej štátnej správy to nie je jednoznačne stanovené.

§ 34a

Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu

(1) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu je ústredným orgánom štátnej správy pre

1. riadenie, koordináciu a dohľad nad využívaním finančných prostriedkov z fondov Európskej únie,
2. oblasť informatizácie spoločnosti,
3. oblasť investícií.

(2) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu v oblasti informatizácie spoločnosti zabezpečuje centrálne riadenie informatizácie spoločnosti a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní finančných zdrojov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti. – **toto môže byť priamym napojením na kritickú infraštruktúru (v zmysle zákona o KI), ak nie je možné úplne vylúčiť, že integrovaný informačný systém verejnej správy nie je prvkom KI, čo asi v každom prípade bude.**

(3) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu v oblasti investícií zabezpečuje strategické plánovanie a strategické projektové riadenie vrátane vypracovania národného strategického investičného rámca, ako aj koordináciu investičných projektov určených vládou Slovenskej republiky.

(4) Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu plní aj úlohy spojené s odborným, organizačným a technickým zabezpečovaním činnosti podpredsedu vlády Slovenskej republiky pre investície a informatizáciu.

Z pohľadu operačného programu OPII však sú definované nasledovné ciele relevantné ku KI

*ŠPECIFICKÝ CIEĽ 7.9:* ***Zvýšenie kybernetickej bezpečnosti v spoločnosti***

***Opis východiskovej situácie***

Základný rámec informačnej bezpečnosti Slovenskej republiky tvorí dokument „Národná stratégia pre informačnú bezpečnosť v SR“40. V podmienkach digitálneho a kybernetického priestoru SR sú zavádzané opatrenia najmä proti úniku informácií a ich neoprávnenému použitiu, narušeniu integrity údajov, porušeniu práv občanov na ochranu osobných údajov, a na ochranu pred poškodzovaním a zneužívaním informačných a komunikačných systémov, ako aj opatrenia na presadzovanie príslušných právnych noriem Slovenska a EÚ.

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.

**Investičná priorita 2c) bude napĺňaná prostredníctvom aktivít:**

ŠC 7.9

P. Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti:

─ Vytvorenie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných incidentov

**─ Zabezpečenie kritickej infraštruktúry**

─ Zavádzanie európskej stratégie pre kybernetickú bezpečnosť

**Z tohto pohľadu, nakoľko podľa kompetenčného zákona je ÚPVII je ústredným orgánom štátnej správy pre riadenie, koordináciu a dohľad nad využívaním finančných prostriedkov z fondov Európskej únie, oblasť informatizácie spoločnosti, oblasť investícií tak úrad má definované určité postavenie aj pri ochrane kritickej infraštruktúry.**

**Úlohy týkajúce sa kritickej infraštruktúry z Akčného plánu realizácie Koncepcie**

**kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2.4. | Vydávať štandardy, metodiky a metodické usmernenia v oblasti kybernetickej bezpečnosti. | V pôsobnosti Komisie pre kybernetickú bezpečnosť NBÚ zriadiť pracovné skupiny pre:  -   kybernetický zločin a počítačovú kriminalitu  -   metodiku a štandardy  -   terminológiu v oblasti KB. | NBÚ |  | 04/2016 |
|  |  | Vydávať štandardy, metodiky a metodické usmernenia. | NBÚ | ÚNMS SRVPA  SIS | priebežne |
| Zriadiť centrálny prístupový bod k normám a štandardom pre ochranu prvkov kritickej infraštruktúry a zabezpečovať pravidelnú aktualizáciu jeho obsahu. | NBÚ | ÚNMS  DC  SNAS  NASES | 06/2017 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3.1. | Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore. | Vypracovať metodiku hodnotenia rizík pre oblasť kybernetickej bezpečnosti na národnej úrovni. | NBÚ | AKOB  ZaA |
|  |  | Vytvoriť postupy pre analýzu stavu, vyhodnocovať ho a navrhovať bezpečnostné opatrenia na odstránenie/minimalizáciu rizík a možných krízových stavov v priestore štátu. | NBÚ |  |
| 3.2. | V rámci mechanizmu prevencie zaviesť jednotné opatrenia z úrovne vecne príslušných autorít. | Zaviesť opatrenia na minimalizáciu potenciálnych rizík a krízových stavov vo svojej pôsobnosti. | VPA |  |
| 3.3. | Vytvoriť procesy a mechanizmy pri koordinácii zabezpečovania ochrany významných informačných aktív štátu na národnej úrovni. | Vytvoriť metodiku pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry. | MF SR | NBÚ  MV SR  DC/CSIRT.SK |
| 3.4. | Vytvoriť a implementovať systém včasného varovania a reakcie na incidenty. | Implementovať jednotný systém včasného varovania, reakcie na incidenty a výmeny informácií podľa časového harmonogramu za účelom zníženia rizík vyplývajúcich z hrozieb informačných a komunikačných systémov a zabezpečovať jeho nepretržitú prevádzku v súlade s plnením úlohy „OAS02 Medzirezortného programu na ochranu kritickej infraštruktúry v SR.“ | NBÚ | DC/CSIRT.SK  VPA/JRI |
|  |  | Zriadiť Národný portál pre kybernetickú bezpečnosť ako súčasť ÚPVS. | ÚV SR | NASES |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.7. | Pravidelne vykonávať ohodnotenie úrovne bezpečnosti vo vládnych sieťach a kritických infraštruktúrach. | Vykonávať interné a externé penetračné testy informačných systémov vybraných organizácií verejnej správy, vrátane prvkov kritickej informačnej infraštruktúry a ďalších významných informačných systémov. | MF SR | ÚOŠS  DC/CSIRT.SK  Prevádzko-vatelia prvkov KII  SIS | priebežne |

Aktivity zamerané na vytváranie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných incidentov, zabezpečenie kritickej infraštruktúry a implementáciou opatrení európskej stratégie pre kybernetickú bezpečnosť, si však vyžadujú úpravu legislatívy a jej zosúladenie, čo návrh úloh primerane zohľadňuje.

Predpokladanými zdrojmi financovania aktivít sú predovšetkým:

       Operačný program pre Integrovanú infraštruktúru - OPII v gescii MDVaRR SR,

       Operačný program Výskum a inovácie v gescii MŠVVaŠ SR,

       Operačný program Ľudské zdroje, prioritná os 1: vzdelávanie, v gescii MŠVVaŠ SR / MPSVaR SR,

       Medzirezortný program pre ochranu kritickej infraštruktúry v gescii MV SR,

       Rozpočtová kapitola NBÚ a rozpočtové kapitoly dotknutých subjektov.

Ďalším uvažovaným zdrojom financovania je nadrezortný/medzirezortný program pre Ochranu kybernetického priestoru Slovenskej republiky pod gesciou Národného bezpečnostného úradu. Vypracovanie návrhu programu je zahrnuté do tohto materiálu v úlohe 1.6. Časový rámec čerpania z programu sa predpokladá až v rokoch 2017-2020.

**Ak z MF SR prešli na ÚPVII všetky kompetencie v oblasti informačných systémov. V prípade, že áno bude plniť pre povinnosti ÚOŠS pre konkrétne prvky KI.**

**V prípade, že sa to ešte nerozhodlo je v tom potrebné urobiť jasný záver.**