Koncepcia kybernetickej bezpečnosti Slovenskej republiky

na roky 2015 - 2020

ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

NASES
NÁRODNÁ AGENTÚRA PRE SIEŤOVÉ A ELEKTRONICKÉ SLUŽBY

NBÚ

Koncepcia kybernetickej bezpečnosti Slovenskej republiky

na roky 2015 - 2020

Obsah

Úvodné slovo

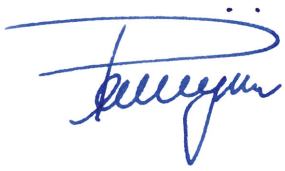
Súčasná spoločnosť je každým dňom viac závislá na informačných a komunikačných technológiách, pričom tieto v poslednom desaťročí zmenili a ovplyvnili takmer každý aspekt nášho života. Činnosti a aktivity ľudí sa pomaly, ale isto vo veľkej miere presúvajú z fyzického priestoru do kybernetického priestoru. Na jednej strane nám informačné a komunikačné technológie uľahčujú život, urýchľujú komunikáciu a prístup k informáciám a službám. Na druhej strane však narastajúca závislosť verejného a súkromného sektora na týchto technológiách v prípade nedostatočnej ochrany spôsobuje aj ich vyššiu zraniteľnosť, čím sa kybernetická bezpečnosť stáva jedným najvýznamnejších výziev dnešnej doby, na ktorú musí štát reagovať. Z globálnosti a významnosti dopadu možného kybernetického útoku vyplynula aj potreba koncepčného a koordinovaného riadenia ochrany a obrany kybernetického priestoru.

Prijatím tejto koncepcie boli stanovené vízie a priority Slovenskej republiky, ktoré zabezpečia kybernetickú bezpečnosť v krajine. Predloženú koncepciu treba chápať ako „základný kameň“, ako základný a východiskový dokument pre následnú tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru.

Vychádzajúc zo strategického a metodického rámca, formovaného v dokumentoch NATO, EÚ, OECD a OSN pre oblasť kybernetickej bezpečnosti koncepcia navrhuje prijať a prioritne riešiť sedem kľúčových opatrení, ktorých realizácia bude konkretizovaná do vecného, časového a finančného plánu v podobe Akčného plánu realizácie koncepcie. Cieľom kybernetickej bezpečnosti v Slovenskej republike má byť podľa koncepcie otvorený, bezpečný a chránený národný kybernetický priestor, t.j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku.

Kybernetickú bezpečnosť je potrebné vnímať ako jeden z kľúčových komponentov bezpečnosti štátu. Je komplexnou problematikou zahŕňajúcou právne i technické aspekty, ktorú je možné dosiahnuť dôverou a spoluprácou medzi verejným sektorom, súkromným sektorom a akademickou obcou. Práva, povinnosti ako aj úlohy jednotlivých aktérov v kybernetickom priestore budú v najbližšom období stanovené prijatím a vybudovaním inštitucionálneho a legislatívneho rámca kybernetickej bezpečnosti, pričom zákon o kybernetickej bezpečnosti bude bezpochyby zásadným medzníkom vo vnímaní kybernetickej bezpečnosti v Slovenskej republike.

Kybernetickú bezpečnosť dosiahneme iba vzájomnou dôverou a spoluprácou, pretože výlučne spoločným úsilím sa nám podarí vytvoriť na jednej strane otvorený, na druhej strane bezpečný kybernetický priestor, ktorý bude na prospech nás všetkých.



Peter Pellegrini
predseda Národnej rady
Slovenskej republiky
digitálny líder Slovenskej republiky

Robert Fico
predseda vlády
Slovenskej Republiky

1 Úvod

Exponenciálny nárast používania informačných a komunikačných technológií od druhej polovice 20. storočia významným spôsobom ovplyvnil vývojové trendy v spoločnosti. Moderné informačné a komunikačné technológie zásadne rozšírili možnosti a zefektívnili spôsoby interakcie geograficky vzdialených subjektov z rozdielnych oblastí spoločnosti, ekonomiky a hospodárstva. Narastajúci počet používateľov informačných a komunikačných technológii spôsobuje narastajúcu závislosť verejného aj súkromného sektora na týchto technológiách, čo spôsobuje ich vyššiu zraniteľnosť.

Popri vysokej závislosti spoločnosti na informačných a komunikačných technológiách, úvod 21. storočia predznačila výrazná zmena globálneho bezpečnostného prostredia a narastajúci počet asymetrických hrozieb s vyššou mierou sofistikovanosti a účinnosti ich dopadov. Široká paleta možných spôsobov zneužitia a poškodenia elektronických informačných, komunikačných a riadiacich systémov, ako aj negatívneho ovplyvnenia spoločenských a hospodárskych procesov v rámci medzinárodného kybernetického priestoru, tak zaradila kybernetické hrozby medzi potenciálne závažné globálne hrozby, ako sú medzinárodný terorizmus, šírenie zbraní hromadného ničenia a podobne.

Dôležité riadiace, technologické, komunikačné a bezpečnostné systémy, ako aj služby, ktorých nefunkčnosť, alebo chybná funkčnosť by mala závažný dopad na fungovanie štátu (najmä v jeho základných bezpečnostných oblastiach), sú ohrozené novými formami útokov. Dynamicky sa rozvíjajúce moderné technológie umožňujú vznik ďalších nových bezpečnostných hrozieb.

Slovenská republika musí byť pripravená reagovať na široké spektrum existujúcich aj potenciálnych hrozieb, pričom si uvedomuje fakt, že hrozby a útoky, objavujúce sa v kybernetickom priestore, môžu eskalovať do úrovne, ktorá bude vyžadovať spoluprácu spojencov Organizácie Severoatlantickej zmluvy (ďalej len „NATO“) podľa článku 5 Severoatlantickej zmluvy[1] a ktorá vyústi do kolektívnej obrany, resp. koordinovanej odozvy. Kybernetickú bezpečnosť je preto nutné vnímať aj ako podsystém národnej bezpečnosti a kybernetický priestor ako novú operačnú doménu. Slovenská republika hodlá spolupracovať so všetkými relevantnými štátnymi aj súkromnými aktérmi kybernetického priestoru, ktorí vyznávajú rovnaké hodnoty a neobmedzujú slobodu a bezpečnosť používania kybernetického priestoru.

Táto Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (ďalej len „Koncepcia“) definuje východiská a ciele Slovenskej republiky v oblasti kybernetickej bezpečnosti. Koncepcia je v súlade s Bezpečnostnou stratégiou Slovenskej republiky a je základným a východiskovým dokumentom pre následnú tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zabezpečeniu kybernetickej bezpečnosti.

1 *Severoatlantická zmluva (NorthAtlanticTreaty) zo dňa 4.apríla 1949, tzv. Washingtonská zmluva, ktorej podpisom vznikla Organizácia Severoatlantickej zmluvy (North Atlantic Treaty Organisation – NATO).*

2 Východiská a princípy kybernetickej bezpečnosti

Koncepcia vychádza z uvedenia a opisu základných pojmov, základných princípov, charakteristiky aktuálneho stavu strategického, legislatívneho a inštitucionálneho rámca v oblasti kybernetickej bezpečnosti v Slovenskej republike a zo strategického a metodického rámca formovaného dokumentmi NATO a Európskej únie (ďalej len „EÚ“) a z nich následne formuluje princípy, ciele a návrhy riešení.

2.1 Základné pojmy

Kybernetická bezpečnosť je jedným z určujúcich prvkov bezpečnostného prostredia Slovenskej republiky a podsystémom národnej bezpečnosti. Na úrovni štátu, ***predstavuje systém*** nepretržitého a plánovitého zvyšovania politického, právneho, hospodárskeho, bezpečnostného, obranného a vzdelanostného povedomia, ktorý zahŕňa aj zvyšovanie účinnosti prijatých a aplikovaných technicko-organizačných opatrení riadenia rizík v kybernetickom priestore za účelom jeho transformácie do dôveryhodného prostredia, ktoré umožnia bezpečné fungovanie spoločenských a hospodárskych procesov pri zaistení akceptovateľnej úrovne rizík v kybernetickom priestore.

Slovenská republika ešte nemá formálne ustálenú terminológiu v oblasti kybernetickej bezpečnosti. Slovo *kybernetický*, ako aj jeho ďalšie gramatické tvary sa nevyskytuje v žiadnom všeobecne záväznom právnom predpise, ani v terminologických slovníkoch[2].

Definície v praxi používaných pojmov z oblasti kybernetickej bezpečnosti, ako aj definície kľúčových pojmov: *kybernetická bezpečnosť, kybernetický priestor, národný kybernetický priestor* pre účely tejto Koncepcie sú uvedené v prílohe č. 1 Koncepcie[3]. Pre reálny výkon štátnej správy v oblasti kybernetickej bezpečnosti, ako aj pre pochopenie vzťahu kybernetickej bezpečnosti k základným bezpečnostným oblastiam fungovania štátu[4], má právne záväzné definovanie obsahu týchto pojmov zásadný význam[5]. Vzťah kybernetickej bezpečnosti k základným bezpečnostným oblastiam fungovania štátu a vzájomný vzťah medzi *kybernetickou bezpečnosťou* a *informačnou bezpečnosťou* sú predmetom nasledujúcej kapitoly Koncepcie.

2.2 Základné princípy kybernetickej bezpečnosti

Problematiku kybernetickej bezpečnosti nie je možné vnímať izolovane ako problém Slovenskej republiky ani ako izolovaný problém jednej alebo niektorých zložiek spoločnosti. Kybernetická bezpečnosť je vzhľadom na svoj globálny charakter celospoločenským fenoménom. Kybernetická bezpečnosť musí byť založená na komplexnom prístupe, čo vyžaduje intenzívne spoločné využívanie informácií a koordináciu aktivít na národnej, ako aj medzinárodnej úrovni. Pri budovaní kybernetickej bezpečnosti je potrebné presadzovať spoluprácu medzi civilnými a bezpečnostnými zložkami štátu, verejným a súkromným sektorom, ako aj medzi národnými a medzinárodnými inštitúciami. Zaistenie efektívnej a účinnej ochrany kybernetického priestoru musia zabezpečiť príslušné subjekty, ktoré sú na národnej úrovni zodpovedné za infraštruktúry jednotlivých odvetví, ako aj subjekty zodpovedné za fungovanie medzinárodných infraštruktúr[6].

---

2 *Na webovom sídle Ministerstva financií Slovenskej republiky.*

3 *Príloha nie je záväzným terminologickým slovníkom pre kybernetickú bezpečnosť.*

4 *Základné bezpečnostné oblasti fungovania štátu podľa štruktúry v Správe o bezpečnosti Slovenskej republiky.*

5 *Čl. 2 ods. 2 zákona č. 460/1992 Z .z. Ústava Slovenskej republiky: Štátne orgány môžu konať iba na základe ústavy, v jej medziach a v rozsahu a spôsobom, ktorý ustanoví zákon.*

6 *Napríklad: Internet Corporation for Assigned Names and Numbers, ICANN; Internet Assigned Numbers Authority, IANA; Governmental Advisory Committee, GAC.*

Slovenská republika sa stotožňuje s princípmi kybernetickej bezpečnosti uvedenými v strategickom dokumente „Stratégia kybernetickej bezpečnosti Európskej únie“[7], ako aj s princípmi uvedenými v „Posilnenej politike kybernetickej obrany NATO“[8].

Charakteristické osobitosti kybernetickej bezpečnosti

Významným špecifikom kybernetickej bezpečnosti je skutočnosť, že jednotlivé komponenty kybernetického priestoru majú rôznych vlastníkov, správcov, prevádzkovateľov, ale aj používateľov. Nedodržiavanie minimálnych bezpečnostných zásad, metód ochrany a minimálnych bezpečnostných opatrení v oblasti kybernetickej bezpečnosti, resp. ich chýbajúca unifikácia zvyšujú mieru zraniteľnosti prevádzkovaných elektronických informačných, komunikačných a riadiacich systémov a v prípade kybernetického útoku môže spôsobiť aj ohrozenie vybranej časti, alebo celého kybernetického priestoru.

Zvládnutie bezpečnostných incidentov a udalostí nezávisí len od schopností verejného sektora, ale významnou mierou závisí aj od konštruktívnej spolupráce aktérov pôsobiacich mimo verejného sektora.

Kybernetická bezpečnosť ako súčasť bezpečnostného systému štátu

Nedostatočná ochrana a obrana pred bezpečnostnými incidentmi vytvára predpoklady zraniteľnosti samotnej spoločnosti s dôsledkami v celej šírke spoločenských a hospodárskych procesov, t. j. závažným spôsobom môžu byť ohrozené základné bezpečnostné oblasti fungovania štátu (ďalej len „bezpečnostné oblasti“):

- Bezpečnostné záujmy Slovenskej republiky v zahraničnej a obrannej politike.
- Ochrana ústavného zriadenia, verejného poriadku, bezpečnosť občana a štátu.
- Sociálna stabilita štátu.
- Ekonomická stabilita štátu.
- Ochrana životného prostredia.

Kybernetická bezpečnosť je vnímaná ako kľúčový komponent bezpečnosti štátu. Za základné komponenty vytvárania a realizácie bezpečnostného systému Slovenskej republiky sú v zmysle zákona[9] považované: zahraničná politika, obranné plánovanie, civilné núdzové plánovanie a koordinácia spravodajských služieb. V legislatívnom procese je t. č. návrh zákona, ktorým je ochrana národného kybernetického priestoru považovaná za ďalší základný komponent bezpečnostného systému štátu.

Z globálnosti a významnosti dopadu možného kybernetického útoku vyplýva potreba koncepčného a koordinovaného riadenia ochrany a obrany kybernetického priestoru.

---

7 *Stratégia kybernetickej bezpečnosti Európskej únie. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013).*

8 *Posilnená politika kybernetickej obrany NATO. Enhanced NATO Policy on Cyber Defence. 2014.*

9 *Zákon č. 110/2004 Z. z. o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z..*

Kybernetická bezpečnosť a informačná bezpečnosť - súvislosti

Pre účely tejto Koncepcie sa pri vymedzení obsahu pojmov kybernetická bezpečnosť a informačná bezpečnosť vychádza najmä z dokumentov EÚ[10]. Z týchto dokumentov vyplýva, že sa jedná o dva kľúčové, vzájomne prepojené okruhy problémov, t.j. bezpečnosť kybernetického priestoru a bezpečnosť informačného prostredia, resp. kybernetickú bezpečnosť a informačnú bezpečnosť.

Informačné prostredie je jedno z významných reálnych prostredí[11] v rámci konkrétnej štruktúry spoločensko-ekonomického prostredia.

Kybernetický priestor je ohraničený používaním elektroniky a elektronického spektra na vytvorenie, uloženie, modifikovanie, výmenu a využívanie dát prostredníctvom vzájomne závislých a prepojených sietí.

Kybernetická bezpečnosť predstavuje systém, ktorého úlohou je poskytnúť informačným prostrediam spoločensko-ekonomickej štruktúry štátu bezpečný, chránený a v primeranom rozsahu otvorený kybernetický priestor, t.j. garanciu bezpečnosti v tomto priestore sa nachádzajúcich elektronických informačných, komunikačných a riadiacich systémov, v týchto systémoch uchovávaných, spracovávaných a prenášaných dát, ako aj týmito systémami poskytovaných služieb.

Spoločnou úlohou kybernetickej a informačnej bezpečnosti je vo vzájomnej súčinnosti zaistiť bezpečnosť informácií, funkčnosť systémov a služieb, ako aj bezpečnosť prostredníctvom týchto systémov prenášaných a/alebo v nich spracovávaných a/alebo uchovávaných dát v rámci konkrétneho spoločensko-ekonomického prostredia.

2.3 Aktuálny stav v Slovenskej republike

Problematika kybernetickej bezpečnosti v Slovenskej republike na národnej strategickej úrovni ešte nie je vyriešená uceleným a konzistentným spôsobom. Téme kybernetickej bezpečnosti je čiastočne venovaná pozornosť v dokumente „Národná stratégia pre informačnú bezpečnosť v Slovenskej republike“[12] (ďalej len „Stratégia“) a v nadväzujúcom „Akčnom pláne na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike“[13].

Prehľad dokumentov, ktoré vláda Slovenskej republiky schválila v súvislosti s realizáciou Stratégie, ako aj ďalších strategických, resp. koncepčných dokumentov, ktorých obsah sa čiastočne venuje problematike ochrany kybernetického priestoru resp. kybernetickej bezpečnosti je uvedený v prílohe č. 2 Koncepcie.

Slovenská republika prijala viacero právnych predpisov, upravujúcich bezpečnosť informačných a komunikačných systémov a informácií, ktoré sú prostredníctvom nich spracovávané, resp. prenášné[14].

---

10 Návrh smernice Európskeho parlamentu a Rady o opatreniach vysokej úrovne bezpečností sietí a informácií. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013).

11 Napr.: sociálne, pracovné, právne a pod.

12 Vláda Slovenskej republiky materiál (č. mat. ÚV-18175/2008) schválila 27. augusta 2008 uznesením č.570/2008.

13 Vláda Slovenskej republiky materiál (č. mat. ÚV-30315/2009) schválila 19. januára 2010 uznesením č.46/2010.

14 Napríklad zákon č. 45/2011 Z. z. o kritickej infraštruktúre, ktorý vymedzuje organizáciu a pôsobnosť orgánov štátnej správy v oblasti kritickej infraštruktúry, zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

Zo „Správ o plnení úloh Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a úloh akčného plánu za roky 2008 až 2013“[15] vyplýva, že pri plnení úloh nelegislatívneho charakteru sú v oblasti informačnej bezpečnosti dosahované pozitívne výsledky najmä v budovaní spôsobilostí, vo vzdelávaní, v prevencii a pripravenosti na zvládnutie bezpečnostných počítačových incidentov, v odstránení ich následkov a následnej obnove informačných systémov v rámci ústrednej štátnej správy. Odborná príprava špecialistov štátnej správy prebieha najmä v gescii Ministerstva financií Slovenskej republiky. Zvyšovanie povedomia a vzdelávania v oblasti kybernetickej, či informačnej bezpečnosti nie je všeobecne obsahovou súčasťou systému vzdelávania v Slovenskej republike (základné, stredné a vysoké školy), ani systému formovania spoločenského povedomia. Vzdelávanie nie je riešené na úrovni špecializovaných odborov, ale nanajvýš na úrovni špecializovaných predmetov v rámci vybraných vzdelávacích inštitúcií. Pretrváva rôzna úroveň spôsobilosti a pripravenosti na kybernetické hrozby. Chýba centrum výnimočnosti, ktoré by sa sústredilo na otázky týkajúce sa kybernetickej bezpečnosti.

Spolupráca verejného sektora so súkromným sektorom, akademickou sférou, ako aj občianskou spoločnosťou nie je rozvinutá v potrebnom rozsahu a absentuje aj rámec pre systematickú, koordinovanú a efektívnu spoluprácu najmä na strategickej úrovni.

Kybernetické hrozby ešte nie sú vo všeobecnosti považované za dostatočne naliehavý problém. Je nevyhnutné neustále upozorňovať na zraniteľnosti, ktorým je dnešná spoločnosť stále vo väčšej miere vystavená, zvyšovať povedomie aj v radoch širokej verejnosti a podnikať kroky, ktoré budú viesť k eliminácii hrozieb a rizík spojených s využívaním moderných informačných a komunikačných technológií.

Najvážnejším problémom v oblasti kybernetickej bezpečnosti v podmienkach Slovenskej republiky je skutočnosť, že ochrana kybernetického priestoru, resp. kybernetická bezpečnosť Slovenskej republiky ešte nie sú výslovne a komplexne upravené v platnej legislatíve[16].

Existujúce kapacity a mechanizmy v oblasti bezpečnosti sietí a informácií už nepostačujú na to, aby držali krok s dynamicky sa meniacim prostredím hrozieb a aby vo všetkých oblastiach riadenia štátu a spoločenského života zabezpečovali dostatočne vysokú a najmä právne účinnú úroveň ochrany.

Slovenská republika ako členská krajina NATO a EÚ sa podieľa aj na tvorbe medzinárodných strategických a koncepčných dokumentov, medzinárodných politík a štandardov a prijaté dokumenty[17] musí implementovať a prevziať do národnej legislatívy. Slovenská republika je aktívna v medzinárodnej spolupráci, má svojich zástupcov v mnohých medzinárodných organizáciách, ako aj v orgánoch EÚ a NATO. Aktívne v nich presadzuje svoje záujmy v tejto oblasti. Pravidelne sa zúčastňuje na kybernetických cvičeniach (Cyber Coalition, Locked Shields, Cyber Europe, a iné), ktoré každoročne preverujú schopnosti a reakcie Slovenskej republiky na kybernetické útoky. Na národnej úrovni bolo koordinované cvičenie s názvom „SISE 2010 až 2013“. Úzko spolupracuje najmä s Centrom výnimočnosti pre oblasť spoločnej kybernetickej obrany v estónskom Taline (NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD COE), Európskou agentúrou pre sieťovú a informačnú bezpečnosť (Network and InformationSecurity Agency, ENISA) a s nedávno vzniknutým Centrom pre boj proti počítačovej kriminalite (European Cybercrime Centre; EC3). V rokoch 2013 – 2014 Národný bezpečnostný úrad plnohodnotne prevzal úlohu budovania kybernetickej obrany a informačnej bezpečnosti NATO v podmienkach Slovenskej republiky v rámci obranného plánovania Ciele síl 2013.

15 *http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s.*

16 *Pozri závery správ o plnení úloh Stratégie a Akčného plánu v prílohe č. 3 Koncepcie.*

17 *Najmä Stratégia kybernetickej obrany NATO (NATO Policy on Cyber Defence), 2011; Akčný plán kybernetickej obrany NATO (NATO Cyber Defence Action Plan); Posilnená stratégia kybernetickej obrany NATO (Enhanced NATO Policy on Cyber Defence), 2014; Stratégia kybernetickej bezpečnosti Európskej únie Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013).*

2.4 Cieľ Koncepcie

Strategickým cieľom kybernetickej bezpečnosti v Slovenskej republike je otvorený, bezpečný a chránený národný kybernetický priestor, t.j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku.

Vychádzajúc z aktuálneho stavu kybernetickej bezpečnosti v Slovenskej republike ***cieľom Koncepcie*** je dosiahnutie stavu, kedy:

- Ochrana národného kybernetické priestoru je systémom fungujúcim koncepčne, koordinovane, efektívne, účinne a na právnom základe.
- Bezpečnostné povedomie všetkých zložiek spoločnosti sa systematicky zvyšuje.
- Súkromný a akademický sektor, ako aj občianska spoločnosť sa aktívne zúčastňujú na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti.
- Je zabezpečená efektívna spolupráca na národnej, ako aj medzinárodnej úrovni.
- Prijaté opatrenia sú primerané a rešpektujú ochranu súkromia a základné ľudské práva a slobody.

3 Návrh riešenia

Na základe východísk, princípov a cieľov definovaných v predchádzajúcej kapitole Koncepcie, návrh riešenia uvedený v tejto časti určuje prostriedky a opatrenia ako Slovenská republika dosiahne zamýšľaný stav. Definuje spôsob a nástroje, ktorými sa Slovenská republika bude snažiť znižovať riziká a hrozby vyplývajúce z kybernetického priestoru a to bez obmedzovania výhod jeho využívania. Z nich bude následne vychádzať Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 (ďalej len „Akčný plán"), ktorý bude definovať konkrétne úlohy vrátane vecného, časového a finančného plánu realizácie Koncepcie.

Za základné ***prostriedky realizácie*** vyššie uvedeného cieľa Koncepcia považuje:

- Na právnom základe fungujúci systém riadenia kybernetickej bezpečnosti (inštitucionálny, regulačný a metodický rámec), zahrňujúci aj špecializované inštitúcie a terminologickú oblasť.
- Vysokú kultúru riadenia rizík, výmeny informácií medzi súkromným a verejným sektorom a zvyšovanie spôsobilostí aktérov.
- Systematickú osvetu a komplexný systém vzdelávania v oblasti kybernetickej bezpečnosti.
- Spoluprácu a partnerstvo na národnej a medzinárodnej úrovni medzi všetkými relevantnými subjektmi z verejného, súkromného a akademického sektora, ako aj občianskej spoločnosti.
- Rozvoj vnútorného trhu s produktmi a službami kybernetickej bezpečnosti, najmä s využitím grantov, fondov EÚ a podporou novovznikajúcich projektov či začínajúcich firiem, ako aj podporu výskumu, vývoja a inovácií priemyselných a technologických zdrojov kybernetickej bezpečnosti.

Koncepcia navrhuje prijať a prioritne riešiť nasledujúcich sedem kľúčových opatrení:

Opatrenie 1: Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.

Opatrenie 2: Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.

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

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

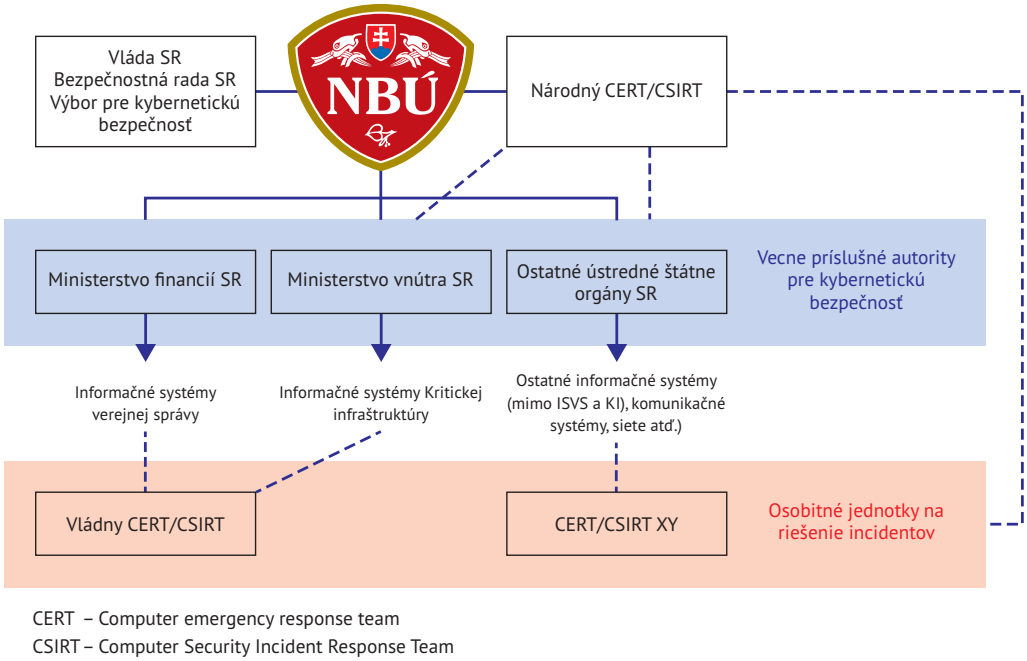
Opatrenie 5: Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.

Opatrenie 6: Aktívna medzinárodná spolupráca.

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

3.1 Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti

Koncepcia navrhuje štruktúru riadenia kybernetickej bezpečnosti, ktorá je uvedená na obrázku č. 1.



CERT – Computer emergency response team
CSIRT – Computer Security Incident Response Team

Obrázok č. 1: Návrh rámcovej štruktúry riadenia kybernetickej bezpečnosti

Kybernetická bezpečnosť na národnej úrovni, patrí do pôsobnosti príslušného ústredného orgánu štátnej správy, ktorého kompetencie a pôsobnosť všeobecne vymedzí kompetenčný zákon a konkrétne stanoví osobitný právny predpis (zákon o kybernetickej bezpečnosti). Rozsah a spôsob výkonu verejnej moci na úseku kybernetickej bezpečnosti, príslušnými ústrednými štátnymi orgánmi a ďalšími štátnymi orgánmi, v rámci konkrétnych vecných oblastí správy spoločensko-ekonomického prostredia štátu (ďalej len „vecné oblasti“) stanoví osobitný predpis (zákon o kybernetickej bezpečnosti).

Komplexné zabezpečenie kybernetickej bezpečnosti v rámci jednotlivých vecných oblastí musí pokryť výkon verejnej moci a výkon odborných činností. Koncepcia predpokladá zriadenie Národnej jednotky pre riešenie incidentov a niekoľkých jednotiek pre riešenie incidentov v rámci osobitne významných vecných oblastí (ďalej len „jednotky“). Z dôvodu racionálneho využitia ľudských kapacít a efektívneho využitia technologického vybavenia jednotiek koncepcia predpokladá pre ostatné vecné oblasti vytvorenie spoločných jednotiek, resp. touto pôsobnosťou pre niektoré vecné oblasti poveriť Národnú jednotku pre riešenie incidentov.

Kompetencie a pôsobnosť Národnej jednotky pre riešenie incidentov, ako aj jednotiek stanoví zákon o kybernetickej bezpečnosti.

Koncepcia navrhuje nasledujúce rámcové vymedzenie pôsobností a kompetencií subjektov verejnej správy na úseku kybernetickej bezpečnosti na centrálnej úrovni:

Ústredný orgán štátnej správy pre kybernetickú bezpečnosť – rozšírená pôsobnosť existujúceho odvetvovo nezávislého ústredného orgánu štátnej správy[18] o ďalší úsek štátnej správy. Koncepcia odporúča aby túto pôsobnosť zákonodarca zveril Národnému bezpečnostnému úradu.

18 T. j. štátny orgán v pôsobnosti ktorého nie je žiadna vecná oblasť správy spoločensko-ekonomického prostredia štátu. Napríklad: Úrad vlády Slovenskej republiky, Národný bezpečnostný úrad.

Vecná pôsobnosť: kybernetická bezpečnosť na národnej úrovni. V rámci tejto pôsobnosti plní tiež povinnosti „príslušného vnútroštátneho orgánu pre oblasť bezpečnosti sietí a informačných systémov“ v zmysle článku 6 návrhu smernice[19].

Kompetencie a zodpovednosti:

- vypracúva koncepciu štátnej politiky v oblasti kybernetickej bezpečnosti a usmerňuje jej realizáciu v rámci jednotlivých odvetví správy,
- pripravuje návrhy všeobecne záväzných predpisov a metodiku, vytvára pravidlá pre akreditáciu jednotiek pre riešenie incidentov,
- metodicky usmerňuje vypracúvanie operačných postupov reakcie na kybernetické hrozby na národnej úrovni,
- koordinuje vypracovávanie akčných plánov vecných oblastí s príslušnými ústredným štátnymi orgánmi,
- koordinuje, sleduje, kontroluje a vyhodnocuje plnenie úloh v oblasti kybernetickej bezpečnosti na národnej úrovni,
- je národným kontaktným bodom pre EÚ a NATO v oblasti kybernetickej bezpečnosti/obrany,
- zabezpečuje a koordinuje plnenie úloh, vyplývajúcich z medzinárodnej spolupráce, reprezentuje Slovenskú republiku na medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
- na základe podkladov ostatných rezortov spracúva a predkladá konsolidované stanoviská za Slovenskú republiku pre oblasť kybernetickej bezpečnosti,
- vypracúva Správy o stave kybernetickej bezpečnosti v Slovenskej republike a predkladá ich na schválenie Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady Slvenskej republiky,
- v rámci krízového riadenia Slovenskej republiky navrhuje a predkladá postup v prípade kybernetického útoku,
- priebežne monitoruje národný kybernetický priestor a analyzuje potenciálne a aktuálne hrozby,
- vykonáva štátny dohľad nad činnosťou jednotiek pre riešenie incidentov.

19 Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii.

Národná jednotka pre riešenie incidentov (národný CERT/CSIRT) – osobitné pracovisko s vecnou pôsobnosťou v oblasti kybernetickej bezpečnosti na národnej úrovni v riadiacej pôsobnosti Ústredného štátneho orgánu pre kybernetickú bezpečnosť (plní tiež úlohy „tímu reakcie na núdzové počítačové situácie“ v zmysle článku 7 návrhu smernice19).

Kompetencie a zodpovednosti:

- systematicky sleduje stav bezpečnosti a dodržiavania bezpečnostných štandardov informačných systémov verejnej správy, priebežne o tom informuje Ústredný orgán štátnej správy pre kybernetickú bezpečnosť,
- zabezpečuje a zodpovedá za koordinované riešenie incidentov, resp. koordinovanú reakciu na kybernetický útok,
- zasiela včasné varovania, vyhlasuje pohotovosti, oznamuje a šíri informácie príslušným zainteresovaným aktérom o rizikách a incidentoch,
- zabezpečuje odbornú prípravu jednotiek pre riešenie incidentov a systematicky riadi cvičenia v oblasti kybernetickej bezpečnosti v rámci svojej pôsobnosti,
- zabezpečuje plnenie úloh, vyplývajúcich z medzinárodnej spolupráce v rámci svojej pôsobnosti,
- buduje rozsiahle verejné povedomie o rizikách spojených s aktivitami vykonávanými on-line a organizuje kampane v oblasti bezpečnosti sietí a informácií,
- pre určené vecné oblasti, resp. na základe poverenia vecne príslušného ústredného štátneho orgánu plní úlohy jednotky pre riešenie incidentov.

Vecne príslušná autorita pre kybernetickú bezpečnosť – organizačný útvar existujúcich ústredných štátnych orgánov. V rámci svojej vecnej pôsobnosti zaisťuje kybernetickú bezpečnosť.

Kompetencie a zodpovednosti:

- zodpovedá za realizáciu štátnej politiky v oblasti kybernetickej bezpečnosti vo svojej pôsobnosti,
- zabezpečuje výkon štátnej správy v oblasti kybernetickej bezpečnosti v rámci svojej pôsobnosti,
- poskytuje súčinnosť Ústrednému orgánu štátnej správy pre kybernetickú bezpečnosť pri formovaní štátnej politiky na úseku kybernetickej bezpečnosti,
- spolupracuje s ostatnými vecne príslušnými autoritami pre kybernetickú bezpečnosť,
- vykonáva dohľad nad činnosťou vecne príslušnej jednotky pre riešenie incidentov,
- zabezpečuje zvyšovanie úrovne bezpečnostného povedomia a koordinuje spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti vo svojej pôsobnosti.

Jednotka pre riešenie incidentov (vládny CERT/CSIRT, CERT/CSIRT XY) – osobitné pracovisko ústredného štátneho orgánu - vecne príslušnej autority pre kybernetickú bezpečnosť. Nepredpokladá sa fyzické zriadenie odvetvových jednotiek v každom odvetví správy. Je však potrebné zabezpečiť realizáciu týchto funkcionalít v rámci jednotlivých odvetví správy[20].

Kompetencie a zodpovednosti:

- systematicky sleduje stav bezpečnosti a dodržiavania bezpečnostných štandardov informačných systémov v rámci svojej vecnej oblasti,
- zabezpečuje a zodpovedá za výkon reakcie na incident, alebo kybernetický útok vo svojej pôsobnosti,
- vypracováva operačné postupy reakcie na incidenty v rámci svojej pôsobnosti a predkladá ich na schválenie Ústrednému orgánu štátnej správy pre kybernetickú bezpečnosť,
- vykonáva okamžitú výstrahu a včasné upovedomovanie o kybernetických hrozbách vo svojej pôsobnosti,
- posudzuje mieru spoľahlivosti a bezpečnostnej odolnosti bezpečnostných mechanizmov vo vzťahu na nové bezpečnostné hrozby a riziká vo svojej pôsobnosti,
- vypracováva pravidelné hlásenia o bezpečnostných incidentoch v rámci svojej pôsobnosti,
- zabezpečuje odbornú prípravu a systematicky riadi cvičenia v oblasti kybernetickej bezpečnosti v rámci svojej pôsobnosti,
- spolupracuje s ostatnými jednotkami pre riešenie incidentov.

Na základe skúseností vyplývajúcich z medzinárodnej spolupráce, z členstva v medzinárodných organizáciách, ako aj skúseností iných krajín je základným predpokladom na efektívny výkon opatrení kybernetickej bezpečnosti širokospektrálna spolupráca nielen štátnej správy a územnej samosprávy, ale aj akademickej obce, vedeckých kruhov a súkromnej sféry. Koncepcia navrhuje vytvoriť **formálnu platformu pre spoluprácu na národnej úrovni**, ktorá umožní účasť reprezentantov podnikateľskej a akademickej sféry na príprave a vytváraní vládnych rozhodnutí formou predkladania odporúčaní, alebo názorov na rozvoj a nepretržité zlepšovanie systému zabezpečenia kybernetickej bezpečnosti v Slovenskej republike.

20 Podmienky zriadenia jednotiek pre riešenie incidentov, ako aj rozsah ich pôsobnosti, kompetencií a povinností stanoví zákon o kybernetickej bezpečnosti.

3.2 Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti

V súčasnosti najvyššou prioritou významného zvýšenia účinnosti a efektívnosti ochrany kybernetického priestoru v podmienkach Slovenskej republiky **je formálno-právne nastavenie systému riadenia kybernetickej bezpečnosti.** Za tým účelom je potrebné:

1. prijať osobitný *zákon o kybernetickej bezpečnosti,* ktorý najmä:
    - formálne zabezpečí koordináciu formovania a realizácie jednotnej štátnej politiky v oblasti kybernetickej bezpečnosti,
    - explicitne stanoví vecnú pôsobnosť a kompetencie orgánov verejnej moci, ako aj rozsah a spôsob výkonu ich kompetencií,
    - explicitne vymedzí aj ostatným aktérom pôsobnosť a kompetencie, ako aj rozsah a spôsob ich aplikácie,
    - stanoví povinnosti pre subjekty využívajúce informačné a komunikačné technológie v kybernetickom priestore,
    - bude garantovať práva, právom chránené záujmy ostatných právnických a fyzických osôb a zároveň upraví ich povinnosti.
2. stanoviť záväznú *terminológiu a štandardy* pre oblasť kybernetickej bezpečnosti.
3. v rámci jednotlivých odvetví správy vydať *metodické usmernenia* pre praktickú aplikáciu zákona a štandardov v systéme riadenia a fungovania príslušného odvetvia.

3.3 Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru

Z dôvodu zabezpečenia odborných úloh na účely dosiahnutia odolnosti kybernetického priestoru Koncepcia identifikuje a navrhuje aplikáciu a rozpracovanie nasledujúcich základných mechanizmov:

1. mechanizmus rozhodovania a riadenia - nepretržité prierezové plánovanie, organizovanie, koordinovanie, realizovanie a kontrolovanie opatrení na minimalizáciu kybernetických bezpečnostných hrozieb a rizík a na zabránenie ich prerastania do krízových situácií:
    - vypracovávanie krízových plánov riešenia krízových situácií,
    - sumarizácia potrieb a požiadaviek, nutných na riešenie identifikovaných hrozieb a ich konfrontácia s možnosťami štátu, regiónov, právnických/fyzických osôb,
    - stanovovanie síl, prostriedkov a zdrojov potrebných na riešenie krízových situácií.
2. mechanizmus prevencie - ochranné opatrenia, ktorých cieľom je pôsobiť proti vzniku krízovej situácie a minimalizovať potenciálne riziká plynúce najmä pre informačné a komunikačné technické prostriedky:
    - národná politika správania sa v kybernetickom priestore,
    - odborná príprava odborného personálu v oblasti informačných a komunikačných technických prostriedkov, ako aj posilňovanie bezpečnostného povedomia obyvateľstva v oblasti informačných a komunikačných technológií,
    - technická/technologická podpora - dostupná pre širokú verejnosť, zodpovedajúca požadovaným úrovniam ochrany, zahŕňajúca odporúčania, opatrenia a technické prostriedky vrátane adekvátnych softvérových, hardvérových a režimových štandardov, ich nastavení a aktualizácie,

- spravodajské aktivity zamerané na získavanie, sústreďovanie a vyhodnocovanie spravodajských informácií využiteľných pri prevencii (napr. spravodajské informácie o kybernetických hrozbách),

- spolupráca s členskými štátmi EÚ a NATO, príslušnými orgánmi týchto organizácií a s partnerskými štátmi s cieľom nepretržite monitorovať, analyzovať a vyhodnocovať bezpečnostnú situáciu v kybernetickom priestore, včas zistiť hrozbu vzniku krízovej situácie a koordinovať prijatie preventívnych opatrení na odstránenie takejto hrozby.

3. mechanizmus reakcie - opatrenia, ktorých cieľom je kvalifikovane a efektívne reagovať v prípade incidentu, alebo vzniku krízovej situácie, a ktoré je potrebné uskutočniť v prípade prebiehajúceho útoku s cieľom odraziť, alebo zmariť útok, a tak zabrániť útočníkovi v spôsobovaní škôd:

    - defenzívne aktivity zamerané na zabránenie útočníkovi uskutočňovať, resp. pokračovať v kybernetickom útoku, v rámci toho je potrebné aktivovať subjekty činné pri riešení krízovej situácie a v prípade potreby včas varovať obyvateľstvo, ďalej vykonať opatrenia zamerané na zastavenie eskalácie krízového stavu a vytvorenie podmienok na návrat do stabilizovaného stavu,

    - ofenzívne aktivity s cieľom oslabovať, alebo úplne eliminovať, protivníkove kybernetické, alebo aj fyzické spôsobilosti a odradiť ho od pokračovania v útokoch,

    - spravodajské aktivity zamerané na podporu defenzívnych, alebo ofenzívnych aktivít (napr. spravodajské informácie o kybernetických spôsobilostiach protivníka).

4. mechanizmus obnovy - záchranné opatrenia, ktorých cieľom je zmiernenie následkov škôd spôsobených kybernetickými útokmi a návrat do pôvodného stavu:

    - odstránenie následkov krízovej situácie a návrat do stabilizovaného stavu,

    - organizačné, personálne, technologické a ďalšie konkrétne opatrenia k zabráneniu opakovania krízovej situácie, alebo ohrozenia.

Z charakteru boja proti kybernetickým útokom vyplýva nevyhnutnosť využívania všetkých bezpečnostných mechanizmov a nástrojov s efektívnou medzirezortnou a medzinárodnou spoluprácou.

3.4 Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti

Kvalita, efektívnosť a účinnosť plnenia opatrení a úloh v oblasti kybernetickej bezpečnosti významnou mierou závisia od úrovne spoločenského povedomia, vzdelanostnej úrovne spoločnosti, ako aj od spôsobilostí aktérov v tejto oblasti. Za tým účelom je potrebné identifikovať konkrétne úlohy Akčného plánu pre oblasti:

1. šírenie osvety a zvyšovanie povedomia.
2. všeobecný vzdelávací systém v Slovenskej republike na úrovni:
    a. základného stupňa vzdelania,
    b. stredného stupňa vzdelania.
3. odborný vzdelávací systém na úrovni:
    a. stredného stupňa vzdelania,
    b. vysokoškolského stupňa vzdelania,
    c. špecialistov.

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

Efektívny bezpečný a kompetenčne optimálne nastavený systém on-line komunikácie a výmeny informácií medzi subjektmi riadiacej štruktúry kybernetickej bezpečnosti navzájom, ako aj s ostatnými relevantnými aktérmi v národnom kybernetickom priestore je nevyhnutným predpokladom zabezpečenia jeho ochrany. Za tým účelom je potrebné na národnej a odvetvovej úrovni, ako aj na úrovni kľúčových aktérov súkromnej sféry:

- optimálne nastaviť riadiace a výkonne štruktúry s jasne vymedzenými pôsobnosťami a kompetenciami,
- vypracovať a zaviesť príslušné metodiky a štandardy,
- implementovať príslušné podporné informačné, komunikačné a riadiace systémy, ako aj bezpečné systémy: výmeny informácií, včasného varovania a koordinovanej reakcie.

3.6 Medzinárodná spolupráca

Kybernetická bezpečnosť vzhľadom na svoj globálny charakter vyžaduje intenzívne spoločné využívanie informácií a koordináciu aktivít nielen na národnej, ale aj medzinárodnej úrovni. Slovenská republika ako členská krajina NATO a EÚ sa bude aj podieľať na tvorbe medzinárodných strategických a koncepčných dokumentov, medzinárodných politík a štandardov a zároveň bude budovať čo najefektívnejší model spolupráce, výmeny a spoločného využívania informácií medzi pracoviskami typu CERT a CSIRT. Popri aktívnej medzinárodnej spolupráci v rámci medzinárodných organizácií a štruktúr bude zároveň aj nadväzovať a prehlbovať bilaterálnu spoluprácu s krajinami, ktoré vyznávajú rovnaké hodnoty ako Slovenská republika. Bude organizovať a zúčastňovať sa na medzinárodných kybernetických cvičeniach a školeniach.

3.7 Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti

V rámci spolupráce verejného sektora so súkromným sektorom a akademickým obcou hodlá Slovenská republika podporovať rozvoj spolupráce aj na výskumných projektoch (vrátane kvalitatívneho a kvantitatívneho výskumu). Bude podporovať účasť na národných, ako aj európskych výskumných projektoch a aktivitách v oblasti kybernetickej bezpečnosti s dôrazom na čerpanie finančných prostriedkov z Operačného programu Výskum a inovácie pre programové obdobie 2014-2020. Výskumné aktivity v tejto oblasti bude koordinovať ústredný orgán štátnej správy pre kybernetickú bezpečnosť.

Slovenská republika zároveň hodlá podporovať súkromný sektor a akademickú obec pri vývoji a implementácii informačných a komunikačných technológií slúžiacich k zabezpečeniu ochrany kybernetického priestoru a v rámci ich vývoja bude národnou prioritou stimulovať investície do tejto oblasti.

4 Závery a odporúčania

Za účelom ochrany národného kybernetického priestoru, plnenia záväzkov Slovenskej republiky ako členskej krajiny EÚ a NATO, ako aj plnenia iných medzinárodných záväzkov, na základe skúseností z ostatných členských krajín, z dôvodu optimalizácie spolupráce medzi orgánmi verejnej moci navzájom, ako aj medzi verejnou mocou a súkromnou a akademickou sférou a tiež v záujme odstránenia duplicít sa Slovenská republika rozhodla prijať na národnej úrovni koncepčný materiál pre oblasť kybernetickej bezpečnosti v podobe tejto Koncepcie.

Koncepcia je základným východiskovým dokumentom pre následnú tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zabezpečeniu kybernetickej bezpečnosti. Keďže je určujúcim prvkom bezpečnostného prostredia Slovenskej republiky a podsystémom národnej bezpečnosti je nutné ho neustále vyhodnocovať a dotvárať. Slovenská republika vníma problematiku kybernetickej bezpečnosti ako dôležitú súčasť každodenného využívania informačných a komunikačných technológií a bude preto klásť dôraz na realizáciu opatrení smerujúcich k jej zabezpečeniu.

Slovenská republika bude pravidelne vyhodnocovať a posudzovať medzinárodnú legislatívu, medzinárodné zmluvy, ako aj trendy a štandardy v oblasti kybernetickej bezpečnosti a tieto bude zavádzať do praxe a aplikovať pri prijímaní právnych predpisov v oblasti kybernetickej bezpečnosti. Slovenská republika sa hodlá aktívne zúčastňovať aj prípravy legislatívy, noriem a štandardov v rámci inštitúcií EÚ, NATO a ďalších medzinárodných organizácií.

Na základe prijatých návrhov Koncepcie sa odporúča vypracovať a predložiť na rokovanie Bezpečnostnej rady Slovenskej republiky a vlády Slovenskej republiky:

1. **Návrh zákona o kybernetickej bezpečnosti,** ktorý ucelene pokryje oblasť kybernetickej bezpečnosti.

2. **Návrh Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020,** ktorý určí vecný, časový a finančný plán realizácie Koncepcie. Obsahom tohto dokumentu bude vecný, časový a finančný plán úloh jednotlivých ústredných štátnych orgánov v rozsahu ich pôsobnosti a kompetencií v rámci základných bezpečnostných oblastí fungovania štátu. Realizáciou týchto úloh sa má dosiahnuť splnenie opatrení Koncepcie pri aplikácii základných princípov kybernetickej bezpečnosti Rámcový návrh úloh obsahuje príloha č. 4 Koncepcie.

Z dôvodu zadefinovania, ustálenia a používania jednotnej terminológie súvisiacej s kybernetickou bezpečnosťou sa odporúča:

3. **Terminológiu, použitú v Koncepcii,** prerokovať v Medzirezortnej terminologickej komisii Bezpečnostnej rady Slovenskej republiky a následne zverejniť v Terminologickom slovníku krízového riadenia.

Pre neutajované skutočnosti, podobne ako to stanovujú vyhlášky pre utajované skutočnosti, sa odporúča v primeranom rozsahu formálne stanoviť:

4. **Požiadavky na fyzickú, objektovú, personálnu a administratívnu bezpečnosť, ako aj podmienky bezpečnosti technických a systémových prostriedkov a šifrovej ochrany informácií.**

Za účelom vytvorenia podmienok pre systematickú spoluprácu verejnej správy, akademickej obce, vedeckých kruhov a súkromnej sféry na zaistení kybernetickej bezpečnosti v Slovenskej republike sa odporúča vytvoriť na národnej úrovni:

5. **Formálnu platformu pre spoluprácu.**

Zoznam príloh

Príloha č. 1: Význam vybraných v praxi používaných a kľúčových pojmov pre účely Koncepcie.

Príloha č. 2: Dokumenty schválené vládou Slovenskej republiky v súvislosti s realizáciou Národnej stratégie pre informačnú bezpečnosť Slovenskej republiky a ďalšie strategické, resp. koncepčné dokumenty.

Príloha č. 3: Závery Správ o plnení úloh Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a úloh akčného plánu za roky 2008 až 2013.

Príloha č. 4: Rámcový návrh úloh Akčného plánu realizácie Koncepcie.

Príloha č. 1: Význam vybraných v praxi používaných pojmov

„aktívum“[21] je čokoľvek, čo má pre jednotlivca, organizáciu, alebo verejnú správu hodnotu.

„asymetrická hrozba“[22] je hrozba vyplývajúca z možného použitia odlišných prostriedkov alebo metód na obídenie alebo potlačenie silných miest protivníka, pri súčasnom využití jeho slabých miest na dosiahnutie neprimeraného výsledku.

„bezpečnosť informačného systému“[23] znamená schopnosť siete alebo informačného a komunikačného systému odolávať na určitom stupni spoľahlivosti náhodným udalostiam alebo úmyselnému konaniu, ktoré ohrozuje dostupnosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov alebo súvisiacich služieb poskytovaných prostredníctvom tejto siete a informačného systému alebo prístupných prostredníctvom tejto siete a informačného systému.

„bezpečnostná hrozba“[21] je potenciálna príčina nežiadúcej udalosti, ktorá môže mať za následok poškodenie systému a jeho aktív, napr. zničenie, nežiadúce sprístupnenie, modifikáciu, nedostupnosť služieb a pod.

„bezpečnostný incident“[21] je porušenie alebo bezprostredná hrozba porušenia bezpečnostných politík, bezpečnostných zásad alebo štandardných bezpečnostných pravidiel prevádzky informačného a komunikačného systému alebo siete.

„bezpečnostné opatrenie“[21] je ochranné opatrenie pre zaistenie bezpečnostných požiadaviek kladených na systém. Môžu mať rôzny charakter (fyzická ochrana zariadenia a informácie, personálna bezpečnosť – kontrola pracovníkov, organizačné opatrenia – prevádzkové predpisy a pod.).

„bezpečnostná udalosť“[21] je udalosť, ktorá môže spôsobiť, alebo viesť k narušeniu informačných systémov a technológií a pravidiel bezpečnostnej politiky.

„bezpečnostná zraniteľnosť“[21] je úmyselná chyba alebo neúmyselný nedostatok či chyba softwaru alebo vo firmwaru zariadení infraštruktúry, ktoré môžu byť zneužité potenciálnym útočníkom pre škodlivú činnosť. Tieto zraniteľnosti sú buď známe a publikované, ale výrobcom ešte neošetrené alebo skryté a neobjavené.

„incident“[21] v prostredí informačných a komunikačných technológií (ďalej len „IKT“) znamená každú okolnosť alebo udalosť, ktorá je obvykle spájaná s výpadkom siete, služby, alebo zhoršením ich kvality.

„riešenie incidentov“[23] znamená všetky postupy na podporu analýzy, monitorovania a reakcie na incident.

„informačné prostredie“ je súhrn jednotlivcov, organizácií a systémov, ktoré zbierajú, spracovávajú, šíria alebo pracujú s informáciami.

„informačná bezpečnosť“[24] je súhrn opatrení na zabezpečenie integrity, dôvernosti a dostupnosti informácií, sietí a informačných a komunikačných systémov.

„infraštruktúra“ všeobecne predstavuje množinu prepojených komponentov, ktoré poskytujú rámcovú podporu celku, t. j. vzájomne závislé siete a systémy všeobecne prepojené na rôznych stupňoch, zahrňujúce priemyselné odvetvia, inštitúcie a distribučné kapacity, ktoré poskytujú tok produktov a služieb. Predstavuje materiálno-technické zázemie štátu t. j. odvetvia zabezpečujúce ekonomické a sociálne systémové funkcie ako napr. energetika, doprava a pod.

---

21 *Výkladový slovník kybernetické bezpečnosti, Druhé aktualizované vydání pod záštitou Národního centra kybernetické bezpečnosti České republiky a Národního bezpečnostního úřadu České republiky, © Jirásek, Novák, Požár, Praha 2013.*

22 *Vojenský terminologický slovník Ozbrojených síl Slovenskej republiky, Bratislava, 2007.*

23 *mernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne sietí a informácií v Únii, COM (2013) 48 FINAL, Brusel, 2013.*

24 *ISO IEC 27000:2014 Information technology-Security techniques – Information security management systems – Overview and vocabulary.*

„kritická infraštruktúra“[21] predstavuje systémy a služby, ktorých nefunkčnosť, alebo chybná funkčnosť by mala závažný dopad na bezpečnosť štátu, jeho ekonomiku, verejnú správu a v konečnom dôsledku na zabezpečenie základných životných potrieb obyvateľstva.

V rámci kritickej infraštruktúry je často definovaných týchto 5 sektorov: sektor informačných a komunikačných technológií, energetický sektor, bankový a finančný sektor, fyzická distribúcia (čiže hlavne prepravné a dopravné systémy) a sektor významných služieb pre ľudí.

„kritická informačná a komunikačná infraštruktúra“[21] predstavuje sústavu systémov, infraštruktúr, sietí a služieb informačných a komunikačných technológií, ktorých narušenie, zničenie alebo nedostupnosť by mali vážny dosah na fungovanie ďalších sektorov kritickej infraštruktúry a životne dôležitých spoločenských funkcií, vrátane národnej, ekonomickej a verejnej bezpečnosti.

„kybernetický priestor“[25] je virtuálny priestor bez hraníc zložený z celosvetovo prepojených sietí z hardvéru, softvéru a dát.

„kybernetická bezpečnosť“[25] je súhrn právnych, organizačných a technických prostriedkov na zaistenie ochrany kybernetického priestoru.

„kybernetická obrana“[26] je súbor aktívnych a pasívnych opatrení zameraných na zabránenie kybernetickému útoku a zmierňovanie jeho následkov. Tiež rezistencia subjektu na útok a schopnosť sa účinne brániť.

„kybernetický útok“[26] je útok na IKT infraštruktúru za účelom jej poškodenia, zničenia, získania citlivých či strategických dôležité informácií, alebo ovplyvňovania rozhodovacích procesov obete. Kybernetický útok má vplyv na všetky operačné domény a používa sa najčastejšie v kontexte politicky či vojensky motivovaných.

„odolnosť systému“[21] schopnosť systému odolať hrozbám a čeliť vplyvom výpadkov.

„riziko“[23] znamená každú okolnosť alebo udalosť, ktorá má prípadný nepriaznivý vplyv na bezpečnosť.

„útok“[24] je pokus zničiť, ohroziť, zmeniť, vyradiť, odcudziť alebo získať nejaký prospech neoprávneným prístupom alebo neoprávneným použitím. Je vykonanie ofenzívnej akcie proti stanovenému cieľu[6].

„zraniteľnosť“[21] predstavuje slabé miesto aktíva alebo riadenia, ktoré môže byť využité hrozbou.

Význam kľúčových pojmov pre účely Koncepcie

Kybernetická bezpečnosť vo všeobecnosti predstavuje schopnosť ľubovoľnej elektronickej komunikačnej siete, elektronického informačného, alebo riadiaceho systému odolávať na určitom stupni spoľahlivosti náhodným udalostiam alebo škodlivým aktivitám, ktoré môžu negatívne ovplyvniť integritu, pravosť, dôvernosť a dostupnosť uchovávaných, spracovávaných, alebo prenášaných dát a služieb, poskytovaných prostredníctvom siete, informačného, alebo riadiaceho systému a tým narušiť, alebo negatívne ovplyvniť funkčnosť najmä niektorého sektoru kritickej infraštruktúry[27], resp. niektorej zo základných bezpečnostných oblastí fungovania štátu.

25 *https://ccdcoe.org/cyber-definitions.html*

26 *Národný bezpečnostný úrad.*

27 *Zákon č.45/2011 o kritickej infraštruktúre v znení neskorších predpisov podľa § 2, písm. c) pod „kritickou infraštruktúrou“ rozumie systém, ktorý sa člení na sektory a prvky. Význam týchto komponentov zákon definuje v § 2, písmeno a), resp. písmeno b).*

Kybernetická bezpečnosť z procesného hľadiska, na úrovni štátu, predstavuje **systém** nepretržitého a plánovitého zvyšovania politického, právneho, hospodárskeho, bezpečnostného, obranného a vzdelanostného povedomia, ktorý zahŕňa aj zvyšovanie účinnosti prijatých a aplikovaných technicko-organizačných opatrení riadenia rizík v kybernetickom priestore za účelom jeho transformácie do dôveryhodného prostredia, ktoré umožnia bezpečné fungovanie spoločenských a hospodárskych procesov pri zaistení akceptovateľnej úrovne rizík v kybernetickom priestore[28].

Kybernetický priestor je virtuálny priestor bez hraníc, považovaný za globálnu interaktívnu doménu v rámci informačného prostredia, ktorá je charakteristická používaním elektronického a elektromagnetického spektra pre vytváranie, ukladanie, modifikovanie a výmenu dát a využívanie služieb. Kybernetický priestor znamená aj kombinovaný fenomén globálneho prepojenia, decentralizovaných a stále sa rozširujúcich elektronických informačných, komunikačných a riadiacich systémov, ako aj prepojenia spoločenských a hospodárskych procesov objavujúcich sa vo forme dát a informácií prostredníctvom týchto systémov, vrátane dát v nich uložených, resp. spracovávaných.

Národný kybernetický priestor Slovenskej republiky zahŕňa časť vyššie uvedených systémov kybernetického priestoru, ktoré sa nachádzajú na území Slovenskej republiky, ako aj ďalšie systémy kybernetického priestoru, ktoré obsahujú dáta a informácie smerované na Slovenskú republiku, alebo majúce vplyv na Slovenskú republiku[29].

Pod ***informačným prostredím*** sa rozumie súhrn jednotlivcov, organizácii a systémov, ktoré zbierajú, spracovávajú, šíria alebo pracujú s informáciami ako takými bez ohľadu na to, či ide o fyzicky zhmotnené informácie, alebo informácie v zvukovej alebo v elektronické podobe".

Pod ***informačnou bezpečnosťou*** sa rozumie: súhrn a uplatnenie bezpečnostných opatrení a postupov[30] slúžiacich v rámci konkrétneho informačného prostredia k ochrane informácií pred ich znehodnotením/stratou, alebo kompromitáciou (strata dôvernosti, integrity a ďalších vlastností ako napr. autenticita, dôveryhodnosť, nepopierateľnosť a spoľahlivosť) a taktiež k zachovaniu dostupnosti informácií a schopnosti s nimi pracovať v rozsahu pridelených oprávnení.

---

28 Pod pojmom kybernetická bezpečnosť je potrebné chápať aj určené mechanizmy, definované politiky, ako aj procesy, ktorých úlohou je chrániť systémy a dáta pred kybernetickou hrozbou, alebo útokom.

29 Definícia obsahu tohto pojmu má zásadný význam z formálno-právneho hľadiska, keďže jurisdikcia Slovenskej republiky nemôže byť aplikovaná v rámci bezhraničného, t.j. globálneho kybernetického priestoru, musí byť ohraničená na jeho časť, teda na národný kybernetický priestor.

30 Bezpečnostný projekt podľa štandardov ISO 27000.

Príloha č. 2: Dokumenty schválené vládou Slovenskej republiky v súvislosti s realizáciou Národnej stratégie pre informačnú bezpečnosť Slovenskej republiky a ďalšie strategické, resp. koncepčné dokumenty

V súvislosti s realizáciou Stratégie vláda Slovenskej republiky schválila uznesením:

- č. 479/2009 Organizačné, personálne, materiálno-technické a finančné zabezpečenie na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov (CSIRT.SK),
- č. 46/2010 Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike,
- č. 136/2010 Legislatívny zámer zákona o informačnej bezpečnosti[1],
- č. 391/2009 Systém vzdelávania v oblasti informačnej bezpečnosti v Slovenskej republike.

Ministerstvo financií Slovenskej republiky, na základe bodu B4 uznesenia vlády Slovenskej republiky č. 570/2008, v rokoch 2010 – 2014 každoročne vypracovalo a na rokovanie vlády predložilo Správy o plnení úloh Stratégie a Akčného plánu[2].

Ďalšími strategickými, resp. koncepčnými dokumentmi, ktorých obsah sa čiastočne venuje problematike ochrany kybernetického priestoru resp. kybernetickej bezpečnosti sú:

- Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany, schválená uznesením vlády Slovenskej republiky č. 120/2007.
- Národná politika pre elektronické komunikácie na roky 2009 - 2013, schválená uznesením vlády Slovenskej republiky č. 360/2009.
- Správy o plnení úloh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, materiály vláda Slovenskej republiky vzala každoročne na vedomie od roku 2010 do roku 2014.
- Biela kniha o obrane Slovenskej republiky, schválená uznesením vlády Slovenskej republiky č. 326/2013.
- Správa o bezpečnosti Slovenskej republiky za rok 2012, schválená uznesením vlády Slovenskej republiky č. 325/2013.
- Operačný program Integrovaná infraštruktúra 2014 - 2020, schválený uznesením vlády Slovenskej republiky č. 171/2014.
- Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany, vyplývajúcich z cieľov spôsobilostí Slovenskej republiky, schválený uznesením vlády č. 497/2014.
- Správa o bezpečnosti Slovenskej republiky za rok 2013, schválená uznesením vlády Slovenskej republiky č. 276/2014.

---

1 *Podľa bodu B.3. uznesenia vlády č. 570/2008 na rokovanie vlády Slovenskej republiky mal byť predložený návrh legislatívneho zámeru zákona o informačnej bezpečnosti verejnej správy v Slovenskej republike.*

2 *http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s*

Príloha č. 3: Závery Správ o plnení úloh národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a úloh akčného plánu za roky 2008 až 2013

Správa 2009

Neobsahuje záver. V závere správy je uvedený „Návrh plnenia úloh na rok 2009“

Správa 2010

Porovnaním výsledkov monitoringu s výsledkami kontrol možno skonštatovať, že boli identifikované rovnaké problémové okruhy a rovnaké kritické faktory. Proces riadenia informačnej bezpečnosti vykazuje systémové nedostatky v oblasti prípravy krízových plánov, prenosu kompetencií a krízového manažmentu. Pre efektívnejšie odstránenie nedostatkov je potrebné urýchliť zavedenie systematického vzdelávania v uvedenej oblasti na všetkých úrovniach a dôsledne uplatniť mechanizmus sankcií za porušovanie zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vrátane jeho vykonávacích predpisov.

Správa 2011

Hlavnou úlohou v oblasti IB je vytvoriť jednotnú platformu budovania informačnej spoločnosti postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru Slovenska.

Pre dosiahnutie a udržanie požadovaného stavu IB je potrebné riešiť v roku 2011 prioritné úlohy najmä v oblasti legislatívy, vedomostných štandardov pre IB a koordinácie cvičení pre prípad reakcie a obnovy na bezpečnostné incidenty na národnej úrovni a s nimi súvisiace aktivity.

Správa 2012

Hlavnou úlohou v oblasti IB je vytvoriť jednotnú platformu budovania IB postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru Slovenskej republiky. Pre dosiahnutie a udržanie požadovaného stavu IB je v ďalšom období nevyhnutné riešiť prioritné úlohy najmä v oblasti legislatívy, vedomostných štandardov pre IB a koordinácie cvičení pre prípad reakcie a obnovy na bezpečnostné incidenty na národnej a medzinárodnej úrovni a s nimi súvisiace aktivity.

Správa 2013

Hlavnou úlohou v oblasti IB je vytvoriť jednotnú platformu budovania IB postavenú na právnych základoch so zabezpečením primeranej ochrany a dôveryhodnosti digitálneho priestoru Slovenskej republiky. Pre dosiahnutie a udržanie požadovaného stavu IB je v ďalšom období nevyhnutné riešiť prioritné úlohy najmä v oblasti legislatívy, vedomostných štandardov pre IB a koordinácie cvičení pre prípad reakcie a obnovy na bezpečnostné incidenty na národnej a medzinárodnej úrovni a s nimi súvisiace aktivity. Uvedené aktivity plne korešpondujú s cieľmi návrhu „Smernice o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii“, kde bude nevyhnutné legislatívne zakotviť absentujúce kompetencie a povinnosti už vytvorenému útvaru „CSIRT.SK“, a to pod gesciou Ministerstva financií Slovenskej republiky. Cieľom je, aby tento útvar mal minimálne takú úroveň, akú majú útvary obdobného typu vo vyspelých členských štátoch EÚ. Transpozícia smernice na území Slovenskej republiky bude riešená v pripravovanom zákone o informačnej bezpečnosti, ktorá si vyžiada aj novelizáciu ďalších s ním súvisiacich všeobecne záväzných predpisov.

Správa 2014

Z porovnania stavu za obdobie roku 2013 z predchádzajúcim obdobím je možné konštatovať, že mierne zlepšenia v niektorých oblastiach v porovnaní s predchádzajúcim obdobím nezodpovedajú dostupným možnostiam zlepšovania. Aj napriek zlepšeniam v niektorých oblastiach, vo väčšine oblastí bola zaznamenaná stagnácia stavu, resp. jeho zhoršenie. Tento negatívny jav je možné zdôvodniť nedodržiavaním jestvujúceho regulačného rámca, nedostatkom odborného personálu a všeobecne nízkym bezpečnostným povedomím subjektov pôsobiacich v oblasti IB vo verejnej správe.

Zlepšenie stavu v tejto oblasti sa dá očakávať po zavedení právnych a organizačných opatrení, štandardizovaných postupov a kontrolných mechanizmov. Ide predovšetkým o ustanovenie povinnej kategorizácie informácií a informačných systémov verejnej správy a následné zavedenie minimálnych bezpečnostných opatrení na ich ochranu, s ustanovením zákonnej zodpovednosti orientovanej aj na dodávateľov týchto služieb. Ďalšou podmienkou zlepšenia celkového stavu je zavedenie procesu riadenia IB v organizáciách, riadenie rizík a nepochybne zvýšenie bezpečnostného povedomia a spôsobilosti personálu. Príprava prostredia pre zavedenie požadovaných opatrení si vyžiada legislatívne zmeny, ktoré boli definované v legislatívnom zámere zákona o informačnej bezpečnosti schválenom vládou, a ktorého zámer sa premietne do pripravovaného zákona o informačnej bezpečnosti.

Príloha č. 4: Rámcový návrh úloh Akčného plánu realizácie Koncepcie

Opatrenie 1:
Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti

Gestor: Úrad vlády

Úlohy:

1. Pripraviť návrh novely kompetenčného zákona, ktorou bude kompetencia ústredného orgánu štátnej správy v oblasti kybernetickej bezpečnosti zverená do pôsobnosti Národného bezpečnostného úradu.

2. Pripraviť návrh na vytvorenie formálnej platformy pre spoluprácu v oblasti kybernetickej bezpečnosti na národnej úrovni.

Súčinnosť: ÚŠO

Úlohy:

3. Vytvoriť personálne a materiálno technické predpoklady pre výkon kompetencií vecne príslušnej autority pre kybernetickú bezpečnosť v rámci svojej pôsobnosti.

4. Vytvoriť personálne a materiálno-technické predpoklady pre výkon kompetencií jednotky pre riešenie incidentov.

5. Vypracovať návrh metodického usmernenia pre výkon kompetencií jednotky pre riešenie incidentov.

Opatrenie 2:
Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti

Gestor: Ústredný orgán štátnej správy pre kybernetickú bezpečnosť

Úlohy:

1. Vytvoriť personálne a materiálno technické predpoklady pre výkon kompetencií ústredného orgánu štátnej správy pre kybernetickú bezpečnosť.

2. Vytvoriť personálne a materiálno-technické predpoklady pre výkon kompetencií Národnej jednotky pre riešenie incidentov.

3. Vypracovať návrh metodického usmernenia pre výkon kompetencií Národnej jednotky pre riešenie incidentov.

4. Pripraviť návrh terminologického slovníka pre oblasť kybernetickej bezpečnosti.

5. Pripraviť návrh zákona o kybernetickej bezpečnosti.

6. Pripraviť návrh štandardov pre kybernetickú bezpečnosť.

Súčinnosť: ÚŠO

Úlohy:

7. Predkladať konkrétne návrhy a aktívne pôsobiť v pracovných skupinách, zriadených gestorom.

8. Vypracovať návrh ustanovení návrhu zákona o kybernetickej bezpečnosti, týkajúcich sa špecifík spravovaného odvetvia z hľadiska kybernetickej bezpečnosti.

9. Poskytnúť aktívnu odbornú súčinnosť pri príprave návrhov: terminologického slovníka, zákona o kybernetickej bezpečnosti, štandardov pre kybernetickú bezpečnosť. Predložiť gestorovi na stanovisko vypracovaný návrh metodického usmernenia pre výkon kompetencií odvetvovej jednotky pre riešenie incidentov.

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

Gestor: Ústredný orgán štátnej správy pre kybernetickú bezpečnosť

Úlohy:

1. Rozpracovať základné mechanizmy zabezpečenia správy kybernetického priestoru a zabezpečiť ich aplikáciu na národnej úrovni.

Súčinnosť: ÚŠO

Úlohy:

2. Rozpracovať základné mechanizmy zabezpečenia správy kybernetického priestoru a zabezpečiť ich aplikáciu na úrovni príslušnej spravovanej oblasti.

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

Gestor: Ministerstvo školstva, vedy, výskumu a športu

Úlohy:

1. Spracovať návrh komplexného zabezpečenia vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov:
    a. všeobecného vzdelávania v Slovenskej republike na rovni:
        - základného stupňa vzdelania,
        - stredného stupňa vzdelania,
    b. odborného vzdelávania na úrovni:
        - stredného stupňa vzdelania,
        - vysokoškolského stupňa vzdelania,
        - špecialistov.

Súčinnosť: ÚŠO

Úlohy:

2. Predložiť návrh Ministerstvu školstva, vedy, výskumu a športu na riešenie zabezpečenia špecifických potrieb odvetvia.

Gestor: Ministerstvo kultúry

Úlohy:

3. Spracovať návrh zabezpečenia systematického šírenia osvety v oblasti kybernetickej bezpečnosti.

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

Gestor: Ústredný orgán štátnej správy pre kybernetickú bezpečnosť

Úlohy:

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.

Súčinnosť: ÚŠO

Úlohy:

5. Navrhnúť a vytvoriť riadiace a výkonné štruktúry s jasne vymedzenými pôsobnosťami, kompetenciami a stanovenými pravidlami vzájomnej komunikácie a súčinnosti na úrovni spravovanej vecnej oblasti.

6. Špecifikovať požiadavky na systémy uvedené v bodoch 2 a 3 tohto opatrenia.

7. V potrebnom rozsahu poskytnúť súčinnosť v rámci jednotlivých fáz projektovania a implementácie uvedených systémov.

Koncepcia kybernetickej bezpečnosti Slovenskej republiky

na roky 2015 - 2020