SLOVENSKO VO VZŤAHU K NOVEJ REALITE KYBERNETICKEJ BEZPEČNOSTI

AUTORI:
Marian Majer, Jaroslav Naď, Monika Masariková

ÚVOD A STRATEGICKÝ RÁMEC

Problematike kybernetickej bezpečnosti sa na Slovensku ešte donedávna venovala veľmi obmedzená pozornosť, a to tak na úrovni štátnej správy ako i širokej verejnosti. Zmena prišla až v roku 2008 s prijatím *Národnej stratégie pre informačnú bezpečnosť* a *Akčného plánu jej implementácie v rokoch 2009-2013*, ktoré odštartovali odbornú diskusiu o koncepčnom rámci riešenia otázok nielen informačnej ale i kybernetickej bezpečnosti. Napriek tomu, že v platnosti boli aj ďalšie strategické dokumenty, ktoré sa aspoň okrajovo dotýkali problematiky kybernetickej bezpečnosti, ako napríklad *Stratégia informatizácie spoločnosti v podmienkach SR*, či *Cestovná mapa zavádzania elektronických služieb verejnej správy*, ich primárnym cieľom bola úprava „informatizácie" spoločnosti. Nevenovali teda pozornosť úprave kybernetickej bezpečnosti ako takej. Absentovalo tiež všeobecné povedomie o kybernetických hrozbách a výzvach s nimi spojených.

Preto *Národná stratégia pre informačnú bezpečnosť* (ďalej len „stratégia") predstavovala významný míľnik i z pohľadu kybernetickej bezpečnosti. Prvýkrát špecifikovala strategické ciele a priority pre túto oblasť. Okrem iného stanovila tri hlavné ciele, ktoré mali napomôcť adekvátnemu stupňu informačnej bezpečnosti Slovenska:

1. Prevencia – zabezpečenie vysokej úrovne ochrany slovenského digitálneho priestoru, ktorá minimalizuje riziko vzniku bezpečnostných incidentov;
2. Pripravenosť – zabezpečenie efektívnej reakcie na bezpečnostné incidenty s cieľom minimalizovať ich dopad a skrátiť čas potrebný na obnovu činnosti informačných a komunikačných systémov po bezpečnostných incidentoch;
3. Udržateľnosť – dosiahnutie, udržiavanie a rozširovanie kompetencie Slovenska v oblasti informačnej bezpečnosti.

S ohľadom na zadefinované ciele sa strategickými prioritami stali:

1. Ochrana ľudských práv a slobôd vo vzťahu k používaniu informačno-komunikačných systémov;
2. Budovanie povedomia a kompetentnosti v oblasti informačnej bezpečnosti;
3. Vytváranie bezpečného prostredia;
4. Zefektívnenie riadenia informačnej bezpečnosti;
5. Zaistenie dostatočnej ochrany štátnej informačno-komunikačnej infraštruktúry a informačno-komunikačnej infraštruktúry podporujúcej kritickú infraštruktúru štátu;
6. Zlepšovanie medzirezortnej a medzinárodnej spolupráce;

7. Rozširovanie národnej kompetencie.[1]

Stratégia zároveň vymedzila kompetencie pre jednotlivé štátne orgány pôsobiace v oblasti informačnej (i kybernetickej) bezpečnosti, pričom toto rozdelenie pôsobnosti pretrvalo v platnosti až do jesene roku 2015. Na rozdiel od súčasnosti bol Národný bezpečnostný úrad podľa nej zodpovedný iba za bezpečnosť utajovaných skutočností. Zodpovednosť za informačnú bezpečnosť verejnej správy a úlohu národného koordinačného orgánu zastávalo Ministerstvo financií SR - Sekcia informatizácie spoločnosti, ktoré spolu s pracovnou skupinou Ministerstva financií SR známou ako Komisia pre informačnú bezpečnosť, bolo zároveň zodpovedné za prípravu strategických a odborných dokumentov. Podľa stratégie bolo Ministerstvo financií SR tiež hlavným komunikačným a riadiacim uzlom vo vzťahu k ostatných štátnym orgánom pôsobiacim v oblasti informačnej bezpečnosti, medzi ktoré patrí: Ministerstvo vnútra SR, Ministerstvo obrany SR, CSIRT.sk (v rámci štruktúry Ministerstva financií SR), Ministerstvo hospodárstva SR, Úrad na ochranu osobných údajov a Slovenská národná akreditačná služba. Úlohy Ministerstva financií SR mal v budúcnosti podľa stratégie prebrať nový štátny útvar – Národný úrad pre informačnú bezpečnosť SR. Dodnes však nedošlo k jeho zriadeniu, prípadne zriadeniu iného centrálneho koordinačného orgánu a otázka kompetencií štátnych orgánov bola nateraz vyriešená inak.

Už z predošlej časti vyplýva, že jedným z problémov sú nejasnosti ohľadom vymedzenia pojmu „informačná bezpečnosť" a „kybernetická bezpečnosť", ktoré sa až do roku 2015 používali v oficiálnych dokumentoch ako stratégie, zákony, či ďalšie nariadenia bez jednoznačnej definície. Stratégia z roku 2008 usilovala o zadefinovanie oblasti informačnej bezpečnosti štátu, ktorou je podľa nej ochrana digitálneho priestoru, teda celého informačného priestoru a ochrana informačnej a komunikačnej infraštruktúry štátu a jej informačného obsahu. Súčasťou digitálneho priestoru je podľa stratégie kybernetický priestor, čím však zužuje kybernetickú bezpečnosť len na utajované skutočnosti, čo je v rozpore s tradičným chápaním tohto pojmu.

Pojem „kybernetická bezpečnosť" sa v odbornej diskusii objavil intenzívnejšie iba nedávno, najmä z dôvodu preberania a ďalšieho šírenia zahraničných odborných článkov a dokumentov medzi odbornou aj laickou verejnosťou. Ale tiež v súvislosti s dianím na európskej úrovni, ktoré rámcuje najmä zverejnenie Stratégie pre oblasť kybernetickej

[1] *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike*, http://www.informatizacia.sk/ext_dok-narodna_strategia_pre_ib/6167c , 4.6.2010.

bezpečnosti EÚ: "otvorený, bezpečný a chránený kybernetický priestor" a návrhu Smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v celej Únii Európskou komisiou vo februári 2013.[2] Istá diskrepancia vo vnímaní pojmov však naďalej pretrváva. Hoci existuje zhoda, že informačná bezpečnosť je vedecko-technický odbor a kybernetická bezpečnosť je len jednou z jeho riešených tém, zároveň tiež existuje istá tendencia zamieňania alebo prelínania týchto pojmov.

Je preto pozitívne, že so snahou o terminologické rozlíšenie prišla aj nová *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020* (ďalej len „koncepcia"), ktorú Vláda SR schválila v septembri 2015, a ktorá čaká na schválenie Národnou radou Slovenskej republiky. Podľa koncepcie je „informačná bezpečnosť" súhrn opatrení na zabezpečenie integrity, dôvernosti a dostupnosti informácií, sietí a informačných a komunikačných systémov. „Kybernetická bezpečnosť" je podľa koncepcie súhrn právnych, organizačných a technických prostriedkov na zaistenie ochrany kybernetického priestoru. Z pohľadu tvorby a formulácie politík je v nej kybernetická bezpečnosť považovaná za jeden z určujúcich prvkov bezpečnostného prostredia Slovenskej republiky a podsystém národnej bezpečnosti. Na úrovni štátu predstavuje podľa dokumentu systém nepretržitého a plánovaného 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[3]. Samotný dokument na rokovanie vlády SR prekvapivo predložil Úrad vlády SR, ktorý dovtedy nebol aktívne zapojený do prípravy legislatívy v oblasti informačnej a kybernetickej bezpečnosti.

Za pozitívny krok možno považovať aj zriadenie postu digitálneho lídra, ktorý vznikol v roku 2013 na podnet Európskej komisie, ktorá k takémuto kroku vyzvala všetky krajiny Európskej únie. Digitálny líder mal na národnej úrovni dohliadať a realizovať ciele Digitálnej agendy EÚ v piatich kľúčových oblastiach: podpora internetovej ekonomiky, efektívna elektronická verejná správa, digitálna bezpečnosť, vzdelávanie a zvyšovanie digitálnych zručností a širokopásmový internet a infraštruktúra. I keď je možné pochybovať o vplyve a reálnych možnostiach digitálneho lídra aktívne formovať agendu informačnej bezpečnosti,

[2] Pozri viac *EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive,* http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, 7.2.2013.
[3] *Návrh Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020,* http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702, 17.6.2015.

zaradenie „digitálnej bezpečnosti" medzi priority lídra aspoň poukazuje na závažnosť danej témy, ktorá si zasluhuje adekvátnu pozornosť zo strany štátu.

KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SR NA ROKY 2015-2020

Prijatie *Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020* predstavuje po rokoch stagnácie v oblasti koncepčného ukotvenia kybernetickej bezpečnosti na Slovensku významný krok vpred hneď z niekoľkých dôvodov.

V prvom rade navrhuje Národný bezpečnostný úrad za ústredný orgán štátnej správy pre kybernetickú bezpečnosť s vymedzenými kompetenciami, čím vytvára predpoklady na zamedzenie duplikácii úloh a prelínaniu zodpovedností viacerých štátnych inštitúcií. Nové vymedzenie kompetencií potvrdila aj novelizácia tzv. „Kompetenčného zákona" (Zákon č. 575/2001 o organizácii činnosti vlády a organizácii ústrednej štátnej správy) z novembra 2015, teda v súlade so záväzkom koncepcie, aby sa tak stalo do konca roka 2015. Zákon s účinnosťou od 1. januára 2016 vymedzil generálnu kompetenciu v oblasti kybernetickej bezpečnosti a zveril ju do pôsobnosti Národného bezpečnostného úradu ako ústrednému orgánu štátnej správy pre kybernetickú bezpečnosť.

Po druhé, koncepcia určuje hlavné ciele pre oblasť kybernetickej bezpečnosti na Slovensku. Cieľom koncepcie je dosiahnutie stavu, kedy:

- Ochrana národného kybernetického 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.[4]

Po tretie, koncepcia vymenúva úlohy na nasledujúce obdobie. Navrhuje prijať a prioritne riešiť sedem kľúčových opatrení, medzi ktoré patrí napríklad vybudovanie inštitucionálneho rámca riadenia kybernetickej bezpečnosti s prislúchajúcou legislatívou.

[4] *Návrh Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020*, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=24702, 17.6.2015.

Po štvrté, zodpovednosť za riadenie bezpečnostných incidentov vkladá do rúk národnej jednotky pre riešenie incidentov (národný CSIRT), ktorá bude okrem monitorovania bezpečnostnej situácie tiež zodpovedná za koordinované riešenie incidentov, resp. koordinovanú reakciu na kybernetický útok. Na rozdiel od súčasného stavu by národná jednotka mala byť súčasťou Národného bezpečnostného úradu SR.

Hoci je schválenie prvej koncepcie kybernetickej bezpečnosti úspechom, kritici koncepcii vyčítajú prílišnú vágnosť, najmä v častiach, kde definuje strategické ciele a opatrenia. Práve preto očakávajú riešenie týchto nedostatkov v akčnom pláne implementácie koncepcie, ktorý mal do konca roka 2015 pripraviť nový centrálny orgán (Národný bezpečnostný úrad) a ktorý vstúpil do medzirezortného pripomienkového konania v decembri roku 2015.

Čiastočné obavy tiež vyvoláva posilnenie a rozšírenie právomocí Národného bezpečnostného úradu, ktorý podľa niektorých hodnotení aktuálne nedisponuje všetkými potrebnými spôsobilosťami a skúsenosťami pre ich jednoznačné a úspešné napĺňanie. Niektoré štátne orgány tiež namietali včlenenie národnej jednotky pre riešenie incidentov do Národného bezpečnostného úradu. Nedostatočné kapacity a ľudské zdroje sú pritom všeobecne vnímané ako jeden z hlavných problémov zabezpečenia kybernetickej bezpečnosti Slovenska, čomu však koncepcia nevenuje dostatočnú pozornosť.

Koncepcii tiež aktuálne chýba mechanizmus kontroly jej implementácie. Istým nedostatkom je aj jednostranné zameranie koncepcie na operatívnu stránku kybernetickej bezpečnosti na úkor analytickej a strategickej roviny. V neposlednom rade koncepcia opomína potrebu rýchlej reakcie na technologické (a ďalšie) zmeny, ktoré majú dopad na jednotlivé bezpečnostné opatrenia a strategické ciele. V koncepcii tak chýbajú riešenia s dlhodobým výhľadom a zameriava sa skôr na riešenie aktuálneho stavu. Paradoxne tiež vyznieva záväzok o aktívnej účasti súkromného a akademického sektora a občianskej spoločnosti na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti, nakoľko samotná koncepcia bola pripravovaná bez účasti spomínaných aktérov, za čo si Úrad vlády SR vyslúžil negatívnu spätnú väzbu.

Ako už bolo spomínané vyššie, koncepcia predstavuje prvý koncepčný a strategický dokument, ktorý sa zaoberá problematikou kybernetickej bezpečnosti. Je teda pochopiteľné, že Slovensko nemá ucelený a komplexný systém kybernetickej bezpečnosti na národnej/strategickej úrovni. Jedným z negatívnych dôsledkov tohto stavu je teda aj chýbajúci zastrešujúci zákon, ktorý by upravoval všetky súvisiace oblasti. Napriek tomu, že v priebehu niekoľkých posledných rokov prebiehali práce na zákone o informačnej bezpečnosti, ktorý sa aj v roku 2013 ocitol v legislatívnom pláne vlády, dodnes nebol

rozpracovaný do finálnej podoby a schválený. V platnosti je tak jedine vládou schválený *Legislatívny zámer zákona o informačnej bezpečnosti* z roku 2010. Ten uvádza, že v dôsledku absencie komplexného zákona, ktorý by upravoval všetky aspekty informačnej bezpečnosti, dochádza k ďalším problémom, medzi ktoré patrí nejasná terminológia, nedostatočné využívanie bezpečnostných štandardov, prekrývanie sa zodpovedností viacerých štátnych orgánov a nedostatočné legislatívne a kompetenčné pokrytie informačnej bezpečnosti.

Ďalším negatívom, ktoré vyplýva z chýbajúceho komplexného legislatívneho rámca v oblasti kybernetickej bezpečnosti, je nejasné vymedzenie povinnosti chrániť informačno-komunikačné systémy. Povinnosti upravuje hneď niekoľko rôznych dokumentov, prípadne je rozhodnutie o stupni ochrany ponechané na vlastníkoch týchto systémov. Zabezpečenie informačno-komunikačných technológií tak dosahuje rôzny stupeň ochrany, čo znižuje predpoklady na bezpečnú spoluprácu či ich efektívnejšie využívanie. Táto situácia by sa ale mala v nasledujúcich mesiacoch zmeniť. Koncepcia uložila Národnému bezpečnostnému úradu ako novému centrálnemu orgánu povinnosť vypracovať do konca februára 2016 nový zákon, ktorý by sa už ale po novom mal volať *Zákon o kybernetickej bezpečnosti*. Doplňať by ho mala novelizácia Zákona o informačných systémoch verejnej správy z roku 2006. Vzhľadom na rozsah jeho rozpracovanosti v čase písania tohto textu je však pravdepodobné, že bude termín schválenia posunutý na neskôr.

INŠTITUCIONÁLNY RÁMEC

Trieštenie zodpovednosti medzi viaceré štátne orgány predstavuje popri absentujúcom legislatívnom rámci jeden z najväčších problémov zabezpečenia kybernetickej bezpečnosti na Slovensku. Nejasné rozdelenie úloh spôsobilo, že nie je jednoznačné, ktorý orgán je zodpovedný za ktorú časť úloh. To malo za následok nežiadúcu rivalitu medzi štátnymi inštitúciami, ktorá tiež sťažila tvorbu politík na národnej úrovni. Tento fakt potvrdila aj *Informácia o vykonaní cvičenia kybernetickej obrany NATO Cyber Coalition 2013*, ktorá uvádza, že mnohé národné tímy uprednostňujú medzinárodnú spoluprácu pred spoluprácou na národnej úrovni. To v praxi znamená, že mnohé informácie častokrát putujú k partnerom do NATO bez prednostného zdieľania informácií na národnej úrovni.[5]

[5] *Informácia o vykonaní cvičenia kybernetickej obrany NATO Cyber Coalition 13*, https://lt.justice.gov.sk/Document/DocumentDetails.aspx?instEID=-1&matEID=7404&docEID=372572&docFormEID=-1&docTypeEID=1&langEID=1, 18.8.2014.

Ustanovenie Národného bezpečného úradu za ústredný orgán štátnej správy pre kybernetickú bezpečnosť (ako navrhuje koncepcia) by mohlo byť prínosné z pohľadu vyjasnenia kompetencií. Na druhej strane však teraz nie je možné predpovedať, aké kompetencie bude NBÚ v budúcnosti v skutočnosti mať a či bude mať záujem vystupovať ako jednotiaca medzirezortná inštitúcia. Kybernetická bezpečnosť je tiež úzko previazaná s viacerými diametrálne odlišnými oblasťami, ako napríklad obrana a vojenstvo (MO SR, Vojenské spravodajstvo), boj proti terorizmu (MV SR, SIS), ochrana kritickej infraštruktúry, kyberzločiny (MV SR), medzinárodné právo (MZVaEZ SR), riešenie incidentov (CSIRT, MF SR) a spolupráca a ďalšími. Názory na to, či by mal problematiku národnej kybernetickej bezpečnosti riešiť jeden alebo viacero štátnych orgánov sa preto rôznia. Niektorí tvrdia, že vytvorenie iba jednej inštitúcie s plnými kompetenciami pre oblasť kybernetickej politiky/bezpečnosti by mohlo vyriešiť problémy spojené s fragmentáciou kompetencií. Centralizácia (vrátane medzinárodnej spolupráce) by podľa tejto skupiny zvýšila efektívnosť celého systému a prispela by k adresnejším výsledkom národných aktivít. Odporcovia tohto názoru naopak považujú za nepravdepodobné, že by jeden centrálny orgán dokázal úspešne riadiť a zastrešovať všetky vyššie menované oblasti kybernetickej bezpečnosti. Ako možný funkčný model pre Slovensko sa teda ponúka kombinovaný systém s jedným ústredným orgánom zodpovedným za strategické riadenie a koordináciu národných politík, ktorý by v obmedzenom rozsahu delegoval časť operačných spôsobilostí ďalším orgánom. Aj zavádzanie tohto modelu do praxe, či zriaďovanie ďalších nových orgánov v oblasti kybernetickej bezpečnosti, však musí byť realizované dôsledne a rozvážne.

Nebolo tomu tak v prípade zriadenia nového Výboru pre kybernetickú bezpečnosť v rámci Bezpečnostnej rady Slovenskej republiky. Okrem vyhodnocovania bezpečnostnej situácie je výbor poverený predkladaním návrhov opatrení, ktoré znížia pravdepodobnosť vzniku krízových situácii v súvislosti s kybernetickými hrozbami. Má tiež prispievať k formulácii politík v oblasti kybernetickej bezpečnosti na národnej úrovni. Napriek istému logickému zdôvodneniu takéhoto návrhu hrozí, že nový orgán prispeje k neprehľadnosti aktuálnej situácie na Slovensku, nakoľko jeho právomoci sú formulované veľmi vágne a hrozí, že sa bude kompetenčne prekrývať s ďalšími inštitúciami. Členmi výboru je tiež až 13 zamestnancov viacerých štátnych orgánov, čo môže znižovať akcieschopnosť samotného výboru. Pomerne náročné môže byť aj obsadenie výboru, nakoľko od členov sa vyžaduje disponovanie bezpečnostnou previerkou tretieho stupňa („tajné“) od Národného bezpečnostného úradu a obdobne aj bezpečnostnou previerkou NATO a EÚ.

AKTUÁLNE VÝZVY NÁRODNEJ POLITIKY KYBERNETICKEJ BEZPEČNOSTI

Ak porovnáme situáciu v oblasti kybernetickej bezpečnosti pred piatimi rokmi a dnes, dostaneme rozpačité výsledky. Z pohľadu kvantity (počet aktivít, odborných článkov, stretnutí, atď.) je pokrok jednoznačný. Z pohľadu kvality, teda posunu od zvyšovania povedomia o kybernetickej bezpečnosti ku tvorbe komplexných stratégií a ich efektívnej implementácii, je trend prinajmenšom otázny. V niektorých oblastiach je možné dokonca konštatovať negatívny vývoj, ako napríklad v prípade zrušenia odboru bezpečnosti, legislatívy a štandardov na Sekcii informatizácie spoločnosti Ministerstva financií SR, či v prípade prieťahov pri prijímaní Zákona o informačnej bezpečnosti/o kybernetickej bezpečnosti. *Správa o implementácii Národnej stratégie pre informačnú bezpečnosť v rokoch 2008-2013* konštatuje iba malé pokroky v danej oblasti, pričom tie nezodpovedajú identifikovaným potrebám a výzvam. Napriek niektorým menším zlepšeniam konštatuje stagnáciu či zhoršenie situácie v iných aspektoch. Zhoršenie sa týka najmä:

1. Neschopnosti štátnych orgánov prispôsobiť sa aktuálnym regulačným mechanizmom;
2. Nedostatočného počtu odborníkov;
3. Nízkeho bezpečnostného povedomia relevantných orgánov vo verejnej správe.

Mnohé negatívne javy podľa hodnotenia viacerých expertov vyplývajú najmä z nedostatočného ľudského kapitálu vo verejnej sfére. Mladých absolventov univerzít oveľa viac láka práca v súkromnom sektore z dôvodu vyššieho finančného ohodnotenia práce. To znemožňuje kvantitatívny ale aj kvalitatívny nárast personálnych kapacít verejného sektora. Bez dostatku zamestnancov s adekvátnou kvalifikáciou, alebo aspoň s jasnou víziou a snahou napredovať, nie je možné očakávať vybudovanie efektívneho systému kybernetickej bezpečnosti na Slovensku.

O to prekvapujúcejšie vyznieva fakt, že v posledných rokoch došlo aj k uvedenému znižovaniu počtu zamestnancov sekcie Ministerstva financií SR, ktorá má dohľad nad informatizáciou spoločnosti. S výnimkou Národného bezpečnostného úradu a niektorých ministerstiev v súčasnosti iba malý počet štátnych inštitúcií disponuje aspoň obmedzenou (strategickou) expertízou či personálnymi kapacitami.

Dichotómiu medzi očakávaniami a negatívnou realitou spôsobuje najmä neadekvátny systém vzdelávania. Systém vzdelávania, ktorý navrhoval strategický dokument *Návrh systému vzdelávania v oblasti informačnej bezpečnosti* z roku 2009, zatiaľ bohužiaľ nebol implementovaný napriek tomu, že sám dokument považoval vzdelávanie za jednu

z dlhodobých výziev. Základné ciele na dosiahnutie a udržanie potrebnej úrovne bezpečnostného povedomia a kompetentnosti sú podľa návrhu:

a) zvyšovanie úrovne poznania občanov, komerčných a nekomerčných organizácií, verejných inštitúcií o rizikách spojených s používaní IKT a možnostiach ochrany pred hrozbami pomocou internetu, masovokomunikačných prostriedkov a metodických materiálov,
b) rozšírenie vzdelávania začlenením základov IB do vyučovania informatiky na školách a jeho zavedením do štátnych vzdelávacích programov (zaradením do vzdelávacieho štandardu),
c) zavedenie programov zvyšovania bezpečnostného povedomia a kompetentnosti používateľov IKT so zvláštnymi nárokmi na IB (postgraduálne štúdium, kurzy celoživotného vzdelávania).[6]

Zlepšovanie kvality vzdelávania je tiež nevyhnutným predpokladom zvyšovania povedomia o informačnej bezpečnosti, ktoré je na Slovensku všeobecne veľmi nízke. Napriek tomu, že v posledných rokoch dochádza ku kvalitatívnym spoločenským zmenám, strategické uvažovanie v oblasti informačnej a kybernetickej bezpečnosti na Slovensku sa riadi skôr princípmi z minulosti, ktoré nereflektujú aktuálne dianie a vývoj. Aj keď štatistiky naznačujú mierny nárast všeobecného povedomia (napríklad počet nahlásených priestupkov v kybernetickom priestore) – k čomu prispievajú aj rastúce aktivity v mimovládnej sfére - prehnaný optimizmus nie je na mieste a je typický skôr pre osoby, ktoré považujú kybernetické hrozby za málo pravdepodobné. Zabezpečenie vysokého stupňa ochrany ani nebolo primárnou snahou či hlavným pilierom pri tvorbe nových informačných systémov (e-government, e-health atď.). Úroveň ochrany jednotlivých štátnych inštitúcií sa líši, pričom kybernetická ochrana býva najčastejšie prvou obeťou krátiacich sa rozpočtov ako v štátnej, tak i v súkromnej sfére. Inými slovami, na Slovensku existuje len obmedzená obava zo zlyhania štátnej infraštruktúry. Nesúlad medzi vytvorením virtuálneho priestoru na jednej strane a absencie efektívnych pravidiel jeho užívania na strane druhej je očividný.

V poslednom desaťročí tiež možno badať postupné zbavovanie sa zodpovednosti štátnej sféry za kybernetickú bezpečnosť, čím došlo ku rozšíreniu mylného názoru o schopnosti štátu realizovať politiky len prostredníctvom prenájmu služieb od súkromného sektora. To zapríčinilo pokles snáh o budovanie vlastných kapacít a hľadanie komplexných riešení, ktoré by štátu umožnili schopnosť adekvátnej reakcie na dnešné aj budúce výzvy.

[6] Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR, http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=6876, 27.5.2009.

Rovnako tak neexistuje zhoda na tom, ktoré úlohy by mali byť v zodpovednosti štátu, ktoré by mali byť predmetom spolupráce medzi verejným a súkromným sektorom a ktoré oblasti by mali zostať výlučne v súkromnom sektore.

Spolupráca verejného sektora so súkromnými spoločnosťami je tiež nedostatočná. I keď je možné vo všeobecnosti povedať, že v súkromnej sfére pôsobí viac odborníkov, ide skôr o odborníkov zameraných na technickú a procedurálnu stránku informačnej bezpečnosti, ktorí majú menší záujem prispievať do tvorby kybernetickej politiky na národnej úrovni, najmä v dôsledku nedostatočného tlaku z verejného sektora.

Vzájomná kritika nezáujmu druhej strany o spoluprácu zaznieva aj v diskusiách odborníkov štátneho a verejného sektora. Zatiaľ čo štátni aktéri argumentujú transparentnosťou pripravovanej legislatívy, ktorá sa nachádza na webových sídlach medzirezortného pripomienkového konania a tak je prístupná oponentúre, súkromný sektor upozorňuje, že by malo byť úlohou štátnych orgánov aktívne osloviť vybraných aktérov (tzv. „klientov štátu"), pre ktorých je daná legislatíva určená za účelom spätnej väzby a poskytnutia vlastného know-how z danej oblasti. Faktom teda zostáva, že v prípade snahy štátu o vytvorenie efektívneho systému kybernetickej či informačnej bezpečnosti, ale aj pri realizácii jednotlivých projektov, by to mal byť práve štát, ktorý by mal proaktívne oslovovať predstaviteľov súkromného sektora. Proaktívny prístup verejného sektora a vytvorenie podmienok pre rovnocenné partnerstvo oboch strán by bol osobitne prínosný pri príprave strategických dokumentov, či legislatívnych opatrení. Táto spolupráca by mala byť nadväzovaná už v procese prípravy a nie až pri medzirezortnom (verejnom) pripomienkovom konaní.

Tento negatívny trend poznačil aj oblasť medzinárodnej spolupráce. Slovensku chýbajú styční pracovníci v medzinárodných inštitúciách (s výnimkou ENISA), ktorí by na týchto fórach dokázali úspešne hájiť slovenské záujmy, prezentovať nové národné iniciatívy a zároveň spätne informovať o medzinárodných aktivitách naspäť na Slovensku. Pozitívnejšia situácia je v prípade zastúpenia SR v NATO, kde danú problematiku pokrývajú až dvaja pracovníci – jeden z NBÚ a druhý z MO SR. Výnimkou je aj Stredoeurópska platforma kybernetickej bezpečnosti (Central European Cyber Security Platform) so zástupcami zo slovenského CSIRT. Z pohľadu medzinárodného pôsobenia tiež možno vyzdvihnúť zapracovanie priorít v oblasti kybernetickej bezpečnosti do Programu slovenského predsedníctva V4 na roky 2014-2015. Bohužiaľ ich formulácia bola veľmi všeobecná a tak je obtiažne vyhodnotiť úspešnosť ich implementácie.

ODPORÚČANIA PRE POLITIKU V OBLASTI KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU

Z poznania súčasnej situácie v oblasti informačnej a kybernetickej bezpečnosti a s uvedomením si normatívnych požiadaviek na požadovaný stav je možné identifikovať nasledovné kľúčové problémy a súvisiace odporúčania:

- Terminologické ukotvenie oblastí informačnej a kybernetickej bezpečnosti je naďalej nedostatočné napriek tomu, že v uplynulom období došlo k opakovaným pokusom o nápravu tohto stavu. Preto je potrebné dôsledné vyjasnenie používaného názvoslovia a jeho zjednotenie vo vzťahu k navrhovanej legislatíve i praktickým opatreniam.
- Nie je dostatočne definovaná šírka informačných aktív štátu a dôvodov na ich ochranu. Preto je potrebné urobiť dôsledné opatrenia smerom k jasnejšiemu určeniu spravovaných aktív, ich hodnoty a postupov pre ich ochranu. Rovnako tak je potrebné určiť, ochrana ktorých aktív bude výlučne v zodpovednosti štátu a ktorá bude otvorená na spoluprácu s tretími subjektmi.
- Inštitucionálne usporiadanie prvkov s kľúčovými zodpovednosťami v daných oblastiach je naďalej nejednoznačné, hoci v uplynulom období došlo k viacerým úpravám smerom k jeho stabilizácii. Aj napriek zdanlivej centralizácii zodpovedností za oblasť kybernetickej bezpečnosti naďalej zostáva veľká časť problematiky fragmentovaná podľa kompetencií jednotlivých ústredných orgánov štátnej správy. Preto nie je ani jasné určené, ktoré z týchto kompetencií prejdú na centralizovaný orgán, alebo zostanú v zodpovednosti jednotlivých úradov. Bude potrebné definitívne rozhodnúť, akou cestou sa Slovensko vydá – či cestou úplnej decentralizácie alebo centrálneho orgánu a udržaním decentralizácie výkonu politiky v jednotlivých parciálnych oblastiach.
- Pozícia digitálneho lídra je v súčasnosti výrazne marginalizovaná a neprispieva k dosahovaniu tých cieľov, ktoré boli pri jej kreovaní nastavené. Preto je potrebné prehodnotiť úlohy, aktivity a funkciu digitálneho lídra v súčasnom inštitucionálnom systéme. V prípade jej zachovania je potrebné pozíciu personálne obsadiť tak, aby nebola kumulovaná s inými funkciami a bola vykonávaná „denne".
- Legislatívne ukotvenie rozsahu kritickej infraštruktúry nedostatočne odzrkadľuje súčasné potreby a ohrozenia informačného priestoru. Je preto potrebné posúdiť

vhodnosť a podmienky pre rozšírenie tohto rozsahu o oblasti, ktoré dnes nie sú súčasťou kritickej infraštruktúry (napr. informačný sektor).

- Mnohé problémy súčasnej situácie súvisia s nedodržiavaním a nedostatočnou implementáciou už existujúceho legislatívneho rámca. Z toho dôvodu je potrebné zamerať sa na lepšiu kontrolu a prípadné sankcionovanie podľa platnej legislatívy (napr. ustanovení o povinnosti nahlasovania incidentov definovanej v zákone o elektronických komunikáciách č. 351/2011 Z.z.).
- Jedným z kritických prvkov úspechu efektívneho systému kybernetickej bezpečnosti na Slovensku je zosúladenie a koordinácia jednotlivých aktivít, projektov a iniciatív. Osobitne zabránenie duplicitnému realizovaniu projektov, duplicitnému vynakladaniu zdrojov a nekompatibilite jednotlivých systémov v dôsledku ich realizácie rozličnými subjektami bez vzájomného dialógu a spolupráce.
- Koordinácia štátneho, súkromného, mimovládneho a akademického sektora pri tvorbe politík a rozhodnutí je v mnohých aspektoch nedostatočná. Odporúča sa preto zvýšiť inštitucionálnu koordináciu medzi sektormi, osobitne pri príprave a implementácii strategických dokumentov a ďalších opatrení. A to najmä v záujme včasnej identifikácie potenciálnych ohrození a vytvorenia efektívneho systému kybernetickej bezpečnosti na Slovensku.
- Prostredie pôsobenia relevantných aktérov štátneho i súkromného sektora vykazuje neustále vysoké znaky konkurencie a vzájomnej nedôvery, až kritiky. Je preto nevyhnutné zasadiť sa o zintenzívnenie budovania vzájomnej dôvery, spolupráce a rovnocenného partnerstva, okrem iného aj cez lepšie zapojenie združení súkromného sektora do mechanizmov tvorby legislatívy i mimo formálneho medzirezortného pripomienkového konania. Nemenej dôležité je, osobitne na strane štátu, nadviazanie formálnej i neformálnej spolupráce pri implementácii stratégií a konkrétnych krokov.
- Oblasti informačnej a kybernetickej bezpečnosti sú neustále „uzavretým" systémom s nedostatočným vnímaním ich dôležitosti zo strany širšej (najmä laickej) verejnosti. Z toho dôvodu sa odporúča prehĺbenie aktivít smerom k získaniu väčšieho záujmu a povedomia obyvateľov SR vo vzťahu k týmto oblastiam, s osobitným dôrazom na stredné a vysoké školstvo

- Jedným z kľúčových problémov pre rozvoj informačnej a kybernetickej bezpečnosti je nedostatok kvalifikovaného personálu využiteľného vo všetkých sektoroch štátu. Vzdelávanie nových profesionálov, ale aj širšie vzdelávanie mladého obyvateľstva sa preto musí stať absolútnou prioritou. Na zváženie je prijatie osobitnej úpravy zameranej na prilákanie expertov z akademického, privátneho či mimovládneho sektora.
- Nevyhnutným predpokladom prijímania rozhodnutí je tiež dostupnosť údajov a tvrdých dát pre oblasť kybernetickej bezpečnosti, preto treba venovať adekvátnu pozornosť ich systematickému zberu a analýze.
- Oblasť zabezpečenia informačnej a kybernetickej bezpečnosti vyžaduje dlhodobé riešenia, ktoré v aktuálne platných dokumentoch chýbajú. Odporúča sa preto venovať zvýšenú pozornosť analytickej a strategickej rovine informačnej a kybernetickej bezpečnosti v pripravovaných strategických dokumentoch za účelom hľadania dlhodobých a efektívnych riešení.

SLOVAK SECURITY POLICY INSTITUTE
SLOVENSKÝ INŠTITÚT PRE BEZPEČNOSTNÚ POLITIKU
Na vŕšku 8
811 01 Bratislava
Slovenská republika
Tel.: (+421) (02) 4319 1592
Email: info@slovaksecurity.org
www.slovaksecurity.org

ISBN 978-80-972228-0-2
Vydal Slovak Security Policy Institute, január 2016.

MINISTERSTVO ZAHRANIČNÝCH VECÍ
A EURÓPSKYCH ZÁLEŽITOSTÍ
SLOVENSKEJ REPUBLIKY

Realizované s finančnou podporou Ministerstva zahraničných vecí a európskych záležitostí SR v rámci dotačného programu v oblasti medzinárodných vzťahov a zahraničnej politiky. Za obsah tohto dokumentu je výlučne zodpovedný Slovenský inštitút pre bezpečnostnú politiku.