DOI: https://doi.org/10.52651/vr.a.2021.1.47-60
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2021, Číslo 1, Strana 47-60

KYBERNETICKÁ BEZPEČNOSŤ – ANALÝZA LEGISLATÍVNEHO PROSTREDIA SLOVENSKEJ REPUBLIKY A AKTIVÍT NA NÁRODNEJ A MEDZINÁRODNEJ ÚROVNI

Michaela ŠIMONOVÁ

CYBER SECURITY - ANALYSIS OF THE LEGISLATIVE ENVIRONMENT OF THE SLOVAK REPUBLIC AND ACTIVITIES AT THE NATIONAL AND INTERNATIONAL LEVEL

HISTÓRIA ČLÁNKU

Doručený: *08. 03. 2021*
Schválený: *31. 05. 2021*
Vydaný: *30. 06. 2021*

ABSTRACT

The arrival of information and communication technologies is nothing new. The number of people using these technologies and moving in cyberspace is growing, and therefore it is an important role of the state to respond sufficiently to such developments. A fundamental role of the state is to create a stable security system consisting of complex legislation as well as creation of a legislative environment capable of responding flexibly to the growing number of diverse incidents in cyberspace. Sufficient legal regulation consisting of unambiguous determination of competencies and tasks of individual subjects represents the basic pillar for the creation of a stable security system. The role of the state is also to maintain existing and create new partnerships with organizations that are able to provide relevant information and knowledge in the field of cyber security.

KEYWORDS

Cyber attacks, hacker, cyber-security incidents, legislation, cyber environment, education.

ÚVOD

Informatizácia spoločnosti sa stáva bežnou súčasťou našich životov. Nové technológie prispievajú k zjednodušovaniu každodenných činností, avšak prinášajú aj nové riziká. Často si ani neuvedomujeme, aké informácie o sebe zdieľame v kybernetickom priestore a často ani nemáme na výber, nakoľko používanie nových technológií nám neumožňuje urobiť krok späť. Nové technológie nás doslova obklopujú a už dávno nie sú výsadou iba niektorých používateľov. V kybernetickom priestore odovzdávame časť svojej identity a súkromia. Cez

elektronické siete komunikujeme s rodinou a priateľmi, pracujeme, platíme účty, využívame osobných asistentov, či hľadáme zábavu. Informatizácia spoločnosti nie je žiadnou novinkou, avšak neustále dochádza k modernizácii, k zhotovovaniu nových technológií, a preto je dôležité, aby bol štát natoľko pružným, aby vedel na tieto zmeny reagovať. Je nevyhnutné nastaviť procesy v štáte tak, aby bolo možné predvídať, prípadne včas odhaliť kybernetické útoky, snažiť sa im zabrániť, alebo ich eliminovať. Nie je to ľahké, nakoľko aktéri kybernetických útokov na rozdiel od iných môžu útočiť priamo z domu, teda neočakávane, anonymne. Je Slovenská republika pripravená reagovať na takúto bezpečnostnú hrozbu?

Motiváciou autorky článku je snaha upozorniť na dôležitosť, resp. nevyhnutnosť vytvárania takého systému (legislatívneho prostredia, inštitucionálneho systému a aktivít štátu), ktorý dokáže flexibilne reagovať na vznikajúce hrozby. Snahou autorky je začať verejný dialóg a poukázať na dôležitosť výmeny informácií a vzdelávania v oblasti kybernetickej bezpečnosti a to práve z dôvodu zmeny bezpečnostného prostredia.

Hlavným cieľom článku je zanalyzovať aktuálny stav legislatívneho prostredia a aktivity Slovenskej republiky v oblasti kybernetickej bezpečnosti a poukázať na ich dôležitosť v kontexte vyvíjajúceho sa bezpečnostného prostredia. Na základe potreby splnenia hlavného cieľa boli zadefinované nasledovné čiastkové ciele:

- Charakteristika základných pojmov týkajúcich sa kybernetickej bezpečnosti a súvisiacich bezpečnostných hrozieb.
- Charakteristika aktuálneho legislatívneho rámca a inštitucionálneho systému v Slovenskej republike vo vzťahu k zabezpečeniu kybernetickej bezpečnosti.
- Národné a medzinárodné aktivity Slovenskej republiky v oblasti kybernetickej bezpečnosti.

Na splnenie cieľov boli použité kvalitatívne metódy analýzy a syntézy informácií, dedukcie a indukcie, ktoré sa používajú vo všetkých etapách, ako aj na všetkých stupňoch vedeckého bádania.

1 TEORETICKÉ VÝCHODISKÁ SKÚMANEJ PROBLEMATIKY

Pre možnosť analýzy skúmanej problematiky je nutné vysporiadať sa so zadefinovaním základných pojmov v oblasti kybernetickej bezpečnosti. Podľa Kampovej a Hollej *„význam definovania základných prvkov systému bezpečnosti je v poznaní ich vzťahov a identifikovaní možných nedostatkov a následnom určení prostriedkov na zaistenie požadovanej bezpečnosti. Bez dôkladného poznania systému nie je možné zaručiť jeho správne fungovanie a teda ani požadovanú úroveň bezpečnosti"* (Kampová a Hollá, 2013, s. 9).

Základným pojmom, ktorý je potrebné zadefinovať je samotná bezpečnosť. Podľa Hofreitera *„potreba bezpečnosti je čoraz naliehavejšia, stáva sa nielen existenčným problémom, ale i problémom vedeckým"* (Hofreiter, 2016a, s.7). Podľa čl. 1 ods. 3 ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného

stavu a núdzového stavu v znení neskorších predpisov je bezpečnosť *„stav, v ktorom je zachovaný mier a bezpečnosť štátu, jeho demokratický poriadok a zvrchovanosť, územná celistvosť a nedotknuteľnosť hraníc štátu, základné práva a slobody a v ktorom sú chránené životy osôb, majetku a životné prostredie"*. Podľa Hofreitera bezpečnosť predstavuje *„stav vedomia človeka, v ktorom sa necíti byť ohrozený, život bez ohrozenia, stav bez strachu a nepokoja o seba a iných, istotu do budúcnosti, absenciu ohrozenia zdravia, straty majetku či života; psychický stav, umožňujúci realizáciu životných cieľov a zámerov, situáciu, v ktorej človeka nič neohrozuje a v neočakávaných, nepredvídaných situáciách sa môže spoľahnúť na pomoc iných ľudí, ustanovenie orgánov a inštitúcií, ktoré svojou činnosťou garantujú občanovi stav istoty a bezpečnosti"* (Hofreiter, 2016b, s. 17). Bezpečnosť jednotlivca, skupiny, štátu alebo ľudstva ohrozujú hrozby, ktoré predstavujú blízkosť niečoho nepríjemného, nebezpečného, čomu je vystavený človek a prostredie, v ktorom žije (Porada a kol., 2019). Tieto bezpečnostné hrozby pôsobia v danom bezpečnostnom prostredí.

Bezpečnostné prostredie musíme zadefinovať s ohľadom na skúmanú problematiku. V kontexte k zvolenej téme je relevantným pojmom jednak informačné prostredie, ktoré podľa Terminologického slovníka krízového riadenia predstavuje *„prostredie pozostávajúce z informácií, prostriedkov a štruktúr na vykonávanie informačných činností a pravidiel upravujúcich tieto činnosti"* (Bezpečnostná rada Slovenskej republiky, 2017) a kybernetický priestor, ktorý podľa § 3 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.") predstavuje *„globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi"*. Už na základe samotných definícií je možné vidieť rozdiel medzi informačným prostredím a kybernetickým priestorom. Informačná bezpečnosť sa zaoberá potrebou zaručenia dôvernosti, integrity a sledovateľnosti informácií všeobecne, zatiaľ čo kybernetická bezpečnosť je užším pojmom, nakoľko sa zaoberá ochranou aktív, ktoré sú spracúvané výhradne vo virtuálnom priestore (Sivák, 2019).

V danom osobitnom priestore rozumieme podľa § 3 písm. h) a i) zákona č. 69/2018 Z. z. hrozbou *„každú primerane rozpoznateľnú okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť"* a rizikom *„mieru kybernetického ohrozenia vyjadrenú pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami"*.

Za účelom vytvorenia vhodného bezpečnostného systému (či už z pohľadu vytvorenia legislatívneho prostredia alebo inštitucionálneho systému) je dôležité poznať druhy aktérov a hrozieb, resp. incidentov, ktoré sú títo aktéri spôsobilí vytvárať. Podľa Volnera *„je veľmi problematické určiť, kedy kybernetický útok má podstatné znaky vojenského útoku a kedy nie. Kedy je to politický akt a kedy kriminálny akt, psychopatický výplod, alebo obyčajná chyba, omyl a náhoda"* (Volner, 2005, s. 309). Čoraz častejšie sa vo svete môžeme stretnúť s kybernetickými útokmi ako nástrojmi mocenského súperenia medzi štátmi. Spôsob a dopad

kybernetického útoku je spôsobilý naznačiť informácie o aktérovi a o jeho motivácii k útoku. Národné centrum kybernetickej bezpečnosti vo svojej Správe o kybernetickej bezpečnosti v Slovenskej republike za rok 2019 vníma prítomnosť piatich druhov aktérov pôsobiacich v kybernetickom priestore, a to s prihliadnutím na ich motiváciu a schopnosti: „scriptkiddies", „kyberkriminálnici", „hacktivisti", štátom sponzorované skupiny a „kyberteroristi". Za takzvaných *„scriptkiddies"* považuje neskúsených alebo príležitostných útočníkov často bez motivácie, resp. útoky spôsobujúcich zo zábavy. *„Kyberkriminálnici"* sú neskúsení a väčšinou ľahko vystopovateľní. Ich motiváciou je finančný zisk. Sú nebezpeční najmä pre bežných používateľov, nakoľko používajú sofistikované spôsoby útokov. *„Hacktivisti"* pôsobia najmä v skupinách, pričom sa nezameriavajú na bežných používateľov, ale na získavanie citlivých a utajených informácií z vládnych inštitúcií. Ich motiváciou je etický aspekt a „náprava krívd" prostredníctvom kybernetického priestoru. *Štátom sponzorované skupiny* sú profesionálni hackeri, ktorí majú buď ekonomickú motiváciu, alebo politicko-vlasteneckú motiváciu. Útočia sofistikovane a je veľmi náročné ich odhaľovanie. Poslednou skupinou aktérov sú *„kyberteroristi"*, ktorí sú nebezpečnou skupinou v službách teroristických organizácií. Ich cieľom je navodiť strach, či znefunkčniť prvky kritickej infraštruktúry. Ich motiváciou je finančný zisk alebo náboženstvo (Správa o kybernetickej bezpečnosti v Slovenskej republike za rok 2019, 2020).

Motivácia vyššie uvedených aktérov nám môže naznačiť typ hrozieb, resp. incidentov, ktoré aktéri vytvárajú v kybernetickom priestore. Národné centrum kybernetickej bezpečnosti v priebehu roka 2019 zbieralo a zaznamenávalo informácie o nasledujúcich druhoch (kategóriách) incidentov v slovenskom kybernetickom priestore: *botnet* (útok, pri ktorom útočník infikuje zariadenie obete a využíva ho na ďalšie účely), *neoprávnená modifikácia informácie* (zmena alebo zmazanie informácie v systéme/službe), *nežiaduci obsah* (spam, scam, defacement stránok a pod), *podvod* (konanie útočníka, na ktoré využíva rôzne nástroje v kybernetickom priestore), *nedostupnosť* (zneprístupnenie služby útočníkom pomocou viacerých nástrojov, vrátane distribuovaných útokov), *pokus o prienik* (dostať sa do chránených sietí a zariadení), *škodlivý obsah* (šírenie tzv. malvéru – napr. ransomvér, trójske kone, advér a pod.), *získavanie informácií* (využívaním sociálneho inžinierstva napr. phishing, spear-phishing a pod.), *neoprávnený prístup k informáciám/únik informácií* (útočník sa neoprávnene dostane k citlivým alebo utajeným informáciám), *prienik do systému* (úspešné preniknutie do systému alebo zariadenia), *zraniteľnosť* (zneužívanie, ale aj samotná existencia zraniteľností na systémoch a službách, ktoré môže útočník využiť na úspešný útok), *ostatné* (všetky ostatné incidenty, ktoré nespadajú do ostatných kategórií) (Správe o kybernetickej bezpečnosti v Slovenskej republike za rok 2019, 2020). Pri uvedenom type incidentov je možné vidieť, akým spôsobom sa okruh hrozieb v kybernetickom priestore vyvíja a aké riziká vznikajú vývojom nových technológií.

Spoznaním motivácie aktérov a druhov incidentov je možné konštatovať, že cieľom kybernetických útokov nie sú len podnikateľské subjekty či štátne inštitúcie, ale aj bežní používatelia internetu a nových technológií. Nakoľko jednotliví aktéri prichádzajú s neustále

novými technikami a spôsobmi kybernetických útokov, je dôležité tieto sledovať a vyvíjať nové bezpečnostné riešenia. Reakcia štátu musí byť komplexná, ale aj cielená. Štát musí vedieť zabezpečiť taký systém ochrany, aby sa všetci, ktorí vstupujú do kybernetického priestoru, cítili bezpečne.

2 ANALÝZA LEGISLATÍVNEHO PROSTREDIA

V kybernetickom priestore musia byť rešpektované základné práva a slobody občanov. Tieto je potrebné zabezpečiť vytvorením a dodržiavaním právnych predpisov, a to jednak Ústavy Slovenskej republiky, všeobecne záväzných právnych predpisov, zachovávajúc základné princípy uvedené v bezpečnostnej a obrannej stratégii Slovenskej republiky, či Programovom vyhlásení vlády. Legislatívne prostredie v oblasti kybernetickej bezpečnosti prešlo od roku 2015 väčšími zmenami, ktoré mali vplyv na tvorbu novej a cielenej legislatívy v danej oblasti. Cieľom bolo reagovať na nové bezpečnostné hrozby a vytvoriť právny rámec, ktorý by dal možnosť štátu flexibilne reagovať na situácie vznikajúce v kybernetickom priestore.

2.1 Kybernetická bezpečnosť na Slovensku od roku 2015

„Právna úprava kybernetickej bezpečnosti má ambíciu zastrešiť tú časť informatickej bezpečnosti, ktorá sa realizuje prostredníctvom elektronických informačno-komunikačných systémov" (Sivák, 2019, s. 15). Ucelený rámec úpravy a riešenia kybernetickej bezpečnosti priniesla smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Úlohou Slovenskej republiky ako členského štátu Európskej únie bolo transponovať predmetnú smernicu, pričom Slovenská republika tak urobila prijatím zákona č. 69/2018 Z. z. Zákon č. 69/2018 Z. z. ustanovil minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, a v rámci splnomocňovacieho ustanovenia § 32 sa zaviazal k vydaniu niekoľkých vykonávacích predpisov. V súčasnosti sú podľa Správy o kybernetickej bezpečnosti v Slovenskej republike v roku 2019 v platnosti:

- Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov.
- Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.
- Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).

- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Zákon č. 69/2018 Z. z. predstavuje ucelený právny rámec definujúci základné pojmy v oblasti kybernetickej bezpečnosti, upravuje organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, kde vymedzuje pôsobnosť Národného bezpečnostného úradu ako ústredného orgánu štátnej správy pre kybernetickú bezpečnosť[1], ústredných orgánov[2] a iných orgánov štátnej správy[3]. Zákon č. 69/2018 Z. z. zaviedol taktiež dôležitý inštitút a to povinnosť hlásenia kybernetických bezpečnostných incidentov. Uvedené bezpečnostné opatrenie je dôležité z hľadiska monitorovania, riadenia, riešenia kybernetických bezpečnostných incidentov. Obete kybernetických útokov však musia mať motiváciu nahlasovať vznik incidentu, a to za účelom následného vhodného nastavenia bezpečnostných procesov tak, aby sa takýmto incidentom mohlo v budúcnosti predísť.

Zákon č. 69/2018 Z. z. upravuje taktiež povinnosť spracovávať Národnú stratégiu kybernetickej bezpečnosti, ktorá určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Táto vychádza z poznatkov získaných z predchádzajúcich období. Nadväzuje na ňu akčný plán, ktorý predstavuje súhrn čiastkových úloh na dané obdobie v oblasti kybernetickej bezpečnosti. Na roky 2015 – 2020 bola spracovaná Koncepcia kybernetickej bezpečnosti Slovenskej republiky (spracovaná ešte pred účinnosťou zákona č. 69/2018 Z. z.). Koncepcia navrhovala prijať sedem kľúčových opatrení v oblasti kybernetickej bezpečnosti: *„vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti, vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti, rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru, podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti, stanovenie a aplikácia kultúry riadenia rizík systému komunikácie*

[1] *Prijatím a účinnosťou zákona č. 69/2018 Z. z. začal Národný bezpečnostný úrad plniť úlohy národnej jednotky pre riešenie kybernetických bezpečnostných incidentov (CSIRT). Dňa 1. septembra 2019 bola CSIRT transformovaná na Národné centrum kybernetickej bezpečnosti SK-CERT. Prostredníctvom SK-CERT Národný bezpečnostný úrad zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a obnovou činností informačných systémov (https://www.nbu.gov.sk/kyberneticka-bezpecnost/sk-csirt/index.html).*

[2] *Ústredným orgánom sa pre účely zákona č. 69/2018 Z. z. podľa ustanovenia § 4 písm. b) rozumie Národný bezpečnostný úrad, Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Slovenská informačná služba, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Vojenské spravodajstvo.*

[3] *Iným orgánom štátnej správy sa pre účely zákona č. 69/2018 Z. z. podľa ustanovenia § 4 písm. c) rozumejú ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad na reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti*.

medzi zainteresovanými stranami, aktívna medzinárodná spolupráca, podpora vedy a výskumu v oblasti kybernetickej bezpečnosti" (Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020, s. 11 - 19). Vypracovaný bol taktiež akčný plán realizácie koncepcie so stanovením zodpovednosti a časového rozmedzia plnenia úloh. Predmetné dokumenty výrazne napomohli k vybudovaniu koncepcie v oblasti kybernetickej bezpečnosti, a to najmä z pohľadu vytvorenia komplexnej legislatívy a vytvoreniu inštitucionálneho rámca riadenia kybernetickej bezpečnosti.

Na Koncepciu kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 aktuálne nadväzuje Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá vo svojom návrhu identifikuje 13 hrozieb:

- *„neustály rozvoj nových techník a spôsobov útokov,*
- *zraniteľní používatelia,*
- *narastajúci počet technologických zraniteľností,*
- *nedostatok odborného personálu,*
- *laxný prístup k požiadavkám vyplývajúcich z legislatívy alebo štandardov,*
- *nízka úroveň bezpečnostného povedomia,*
- *zneužívanie nových technológií na vykonávanie útokov,*
- *slabá detekcia,*
- *zneužívanie pokročilých techník šifrovania pri kybernetických útokoch,*
- *pomalý výkon trestného práva v oblasti počítačovej kriminality s neistým výsledkom,*
- *útoky zamerané na bežných používateľov s veľkými finančnými stratami,*
- *útoky na kritickú infraštruktúru štátu, orgány štátu a obranné mechanizmy s mocensko-politickým pozadím,*
- *nelegálne aktivity, presahujúce kybernetický priestor"* (návrh Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025, s. 7 - 10).

Po jej schválení bude nasledovať vypracovanie akčného plánu jej realizácie[4]. Spracovanie stratégie, ktorá vychádza z nahlásených incidentov, vedomostí získaných v rámci členstva v organizáciách a účasti na cvičeniach je dôležitou pre určenie ďalšieho smerovania v oblasti zabezpečovania kybernetického priestoru. Nadväzujúci akčný plán so stanovením terminovaných úloh v pôsobnosti stanovených subjektov je následne kľúčovým dokumentom pre vytváranie stabilného bezpečného kybernetického prostredia.

2.2 Informácie nachádzajúce sa v kybernetickom priestore

Pri analýze legislatívneho prostredia Slovenskej republiky v oblasti kybernetickej bezpečnosti je potrebné identifikovať jednotlivé typy informácií, ktoré sa nachádzajú v kybernetickom priestore. Ide o informácie, s ktorými pracujú bežní používatelia, ale aj štátne inštitúcie, a ktoré je potrebné v rámci vytvoreného bezpečnostného systému chrániť.

[4] *Návrh národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 predložený do medzirezortného pripomienkového konania.*

Tieto informácie sú objektom kybernetických útokov a za nimi stojacich aktérov. Podľa Siváka je ich ochranu možné rozdeliť do niekoľkých základných oblastí: ochrana utajovaných skutočností, ochrana osobných údajov, ochrana daňových, bankových a telekomunikačných informácií tvoriacich tajomstvo, ochrana citlivých informácií, ochrana citlivých informácií, ktoré nie sú predmetom právnej úpravy (Sivák, 2019). Vytváranie, spracovávanie, zdieľanie či ochrana uvedeného druhu informácií, ktoré sú súčasťou elektronických informačno-komunikačných systémov, je obsiahnuté v samostatnej právnej úprave.

Ochrana utajovaných skutočností je upravená v zákone č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Predmetný zákon upravuje ochranu utajovaných skutočností v oblastiach personálnej bezpečnosti, priemyselnej bezpečnosti, fyzickej a objektovej bezpečnosti, bezpečnosti technických prostriedkov a administratívnej bezpečnosti. Ochranu osobných údajov upravuje zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES. Ochrana osobných údajov patrí medzi základné ľudské práva a slobody. Ide o skupinu informácií týkajúcich sa osôb, pričom tieto sú v súčasnosti vo veľkej miere spracovávané prostredníctvom automatizovaných prostriedkov, ktoré sú súčasťou informačného systému. Preniknutím do takýchto informačných systémov sa aktéri môžu dostať k citlivej skupine informácií týkajúcich sa osôb, preto práca s nimi musí byť zodpovedná a ich zabezpečenie musí byť v súlade s právnymi predpismi. Obchodné, daňové, bankové a telekomunikačné informácie tvoriace tajomstvo upravuje niekoľko právnych predpisov, najmä zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov (Sivák, 2019). Problematiku citlivých informácií nachádzame podľa Siváka v dvoch podobách: ochrana citlivých informácií z prostredia jadrového priemyslu podľa zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ochrana citlivých informácií podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov (Sivák, 2019).

Všetky vyššie uvedené typy informácií musia byť v kontexte kybernetickej bezpečnosti spracovávané, prenášané alebo uchovávané v elektronickej podobe.

Je dôležité, aby právny poriadok Slovenskej republiky poskytoval dostatočnú právnu úpravu v oblasti vymožiteľnosti zákona č. 69/2018 Z. z. prípadne ďalších vyššie uvedených všeobecne záväzných právnych predpisov. Takýmto predpisom je zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov, ktorý vo svojej 2. časti, 4. hlave upravuje Trestné činy proti majetku. Predmetný zákon v rámci ustanovení § 247 až §247d upravuje trestné

činy neoprávneného prístupu do počítačového systému, neoprávneného zásahu do počítačového systému, neoprávneného zásahu do počítačového údaja, neoprávneného zachytávania počítačových údajov a neoprávnenej výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov (Sivák, 2019).

3 AKTIVITY SLOVENSKEJ REPUBLIKY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Dosiahnutie kybernetickej bezpečnosti je národným záujmom. Kybernetické útoky sú však globálnou hrozbou, a preto musí byť v záujme každého štátu vytvárať silné partnerstvá a spolupráce, vymieňať si skúsenosti a vedomosti v danej oblasti. Slovenská republika udržiava vzťahy v oblasti kybernetickej bezpečnosti najmä v rámci Európskej únie a Severoatlantickej aliancie. Podľa informácií z internetovej stránky Národného bezpečnostného úradu Slovenská republika v rámci Európskej únie aktuálne:

- spolupracuje s Agentúrou Európskej únie pre bezpečnosť sietí a informácií (ENISA), ktorá členské štáty Európskej únie podporuje v riešení problémov v oblasti kybernetickej bezpečnosti (NBÚ SR, Kybernetická bezpečnosť (organizácie a partneri), EÚ a NATO);
- zapája sa do aktivít Európskej organizácie pre kybernetickú bezpečnosť (ECSO). ECSO má za cieľ podporovať iniciatívy členských štátov zamerané na rozvoj a podporu kybernetickej bezpečnosti, ochranu európskeho jednotného digitálneho trhu pred kybernetickými hrozbami, rozvoj a rast konkurencieschopnosti v oblasti informačno-komunikačných technológií (NBÚ SR, Kybernetická bezpečnosť (organizácie a partneri), ECSO);
- spolu s Českou republikou, Poľskom, Maďarskom a Rakúskom je členom Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP). CECSP má za cieľ udržiavanie spolupráce susedných krajín v oblasti kybernetickej bezpečnosti formou výmeny informácií a skúseností týkajúcich sa kybernetických hrozieb, ako aj potencionálnych a vykonaných kybernetických útokoch (NBÚ SR, Kybernetická bezpečnosť, CECSP);
- spolupracuje s Organizáciou pre bezpečnosť a spoluprácu v Európe (OBSE). OBSE zahŕňa 57 účastníckych štátov Európy, Strednej Ázie a Severnej Ameriky. Jej cieľom je podpora ľudských práv a základných slobôd, prevencia konfliktov, obnova stability, presadzovanie kolektívnej bezpečnosti a ďalších oblastí (NBÚ SR, Kybernetická bezpečnosť, OBSE);
- je členom Európskeho centra výnimočnosti pre boj proti hybridným hrozbám.

Podľa informácií z internetovej stránky Národného bezpečnostného úradu Slovenská republika v rámci Severoatlantickej aliancie aktuálne:

- pôsobí v rámci platformy MISP (Malware Information Sharing Platform), kde má možnosť vymieňať si aktuálne informácie v oblasti kybernetickej bezpečnosti;
- zúčastňuje sa prostredníctvom zástupcu Stálej delegácie Slovenskej republiky pri NATO v Bruseli na zasadnutiach Výboru pre kybernetickú obranu;

- zúčastňuje sa cvičení kybernetickej obrany NATO Cyber Coalition a vzdelávacích aktivít zastrešovaných lisabonskou NCI Academy (NBÚ SR, Kybernetická bezpečnosť (organizácie a partneri), EÚ a NATO).

V rámci predmetných organizácií zastupuje Slovenskú republiku Národný bezpečnostný úrad.

Slovenská republika má taktiež bilaterálnych partnerov v oblasti kybernetickej bezpečnosti, ktorými sú podľa internetovej stránky Národného bezpečnostného úradu:

- Národná agentúra pre bezpečnosť informačných systémov (ANSSI), ktorá v rámci kybernetickej obrany monitoruje, varuje a reaguje na počítačové útoky;
- Národný úrad pre kybernetickú a informačnú bezpečnosť (NÚKIB), ktorý spolupracuje s medzinárodnými tímami CERT a CSIRT, podporuje vzdelávanie a výskum v oblasti kybernetickej bezpečnosti, ochranu utajovaných skutočností a šifrovú ochranu;
- Tím na reakciu pre počítačové bezpečnostné incidenty (GOVCERT.LU), ktorý dohliada na proces riadenia incidentov v oblasti kybernetickej bezpečnosti (NBÚ SR, Kybernetická bezpečnosť, organizácie a partneri, bilaterálni partneri).

Slovenská republika (Ministerstvo obrany Slovenskej republiky) taktiež spolupracuje s občianskym združením AFCEA Slovakia, ktorá sa okrem iného zaoberá aj problematikou kybernetickej bezpečnosti.

Spolupráca na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti je samozrejme rozsiahlejšia ako je vyššie uvedené a je pre Slovenskú republiku veľmi dôležitá. Kybernetický priestor sa neustále vyvíja a získavanie informácií, vedomostí a poznatkov v danej oblasti predstavuje predpoklad pre zavádzanie vhodných bezpečnostných procesov a vytvorenie stabilného a funkčného bezpečnostného systému. Získané poznatky je následne nutné prezentovať na niekoľkých úrovniach. Jednak zabezpečiť odovzdanie informácií odborníkom a umožniť im rozvoj výskumu a vývoja v oblasti kybernetickej bezpečnosti. Taktiež je potrebné zabezpečiť vzdelávanie zamestnancov verejnej správy, aby vedeli dostatočne aplikovať bezpečnostné zásady v praxi.

V súčasnosti zamestnávatelia preferujú u svojich zamestnancov prácu z domu, a týchto treba dostatočne oboznámiť so základnými pravidlami pri práci s elektronickými informačno-komunikačnými prostriedkami, aby eliminovali potencionálne bezpečnostné hrozby v kybernetickom priestore. V neposlednom rade je potrebné zvýšiť bezpečnostné povedomie medzi bežnými používateľmi internetu, či nových technológií, aby si dostatočne uvedomovali bezpečnostné hrozby a riziká a tomu prispôsobili správanie v kybernetickom priestore. Takáto „informačná kampaň" musí byť veľká, nakoľko v súčasnosti volia aktéri rôzne typy útokov, od zasielania podvodných e-mailov so zámerom získania osobných údajov či bankových účtov, hoaxov, šíria dezinformácie s politickým či iným zámerom a mnoho ďalších.

ZÁVER

Na základe analýzy výskumom získaných informácií je možné ponúknuť niekoľko zistení a opatrení. Tak ako vyplýva z predchádzajúcich častí, informatizácia sa už dnes týka každého. Počet používateľov nachádzajúcich sa v kybernetickom priestore narastá a v súčasnosti by sme možno mali problém označiť niekoho, kto sa v danom priestore nepohybuje. Preto nastupuje dôležitá úloha štátu vytvoriť a nastaviť také procesy, aby bol život v kybernetickom priestore bezpečný pre bežných používateľov, bezpečný pre verejnú správu, kritickú infraštruktúru, bezpečný pre štát. O bezpečnosti v kybernetickom priestore už dávno nehovoríme iba vo vzťahu k štátnym inštitúciám, či právnickým osobám, ale týka sa každého používateľa, ktorý využíva informačno-komunikačné technológie.

Slovenská republika je plnohodnotným partnerom v otázkach riešenia kybernetickej bezpečnosti a kybernetických útokov. Slovenskej republike sa úspešne podarilo transponovať smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, kedy bol vydaný zákon č. 69/2018 Z. z. Tento významnou mierou prispel k vytvoreniu jednak inštitucionálneho systému, ktorý dokáže detekovať bezpečnostné hrozby v oblasti kybernetickej bezpečnosti, vyhodnotiť ich riziko a zároveň je spôsobilý flexibilne reagovať na vzniknuté incidenty. Presne stanovuje pôsobnosť jednotlivých subjektov v oblasti vytvárania kybernetickej bezpečnosti, čo je správnym predpokladom na vytváranie stabilného bezpečnostného systému. Vychádzajúc z aplikačnej praxe je však potrebné aj naďalej vytvárať bezpečnostné pravidlá a zásady v podobe všeobecne záväzných právnych predpisov.

Rýchlou zmenou bezpečnostného prostredia – kybernetického priestoru spôsobenou vývojom nových technológií, prípadne aktualizáciou už existujúcich, vznikajú nové druhy incidentov a spôsob ich prevedenia. Ukazuje to samotný vývoj, resp. forma kybernetických útokov. Za účelom rýchlej a správnej reakcie je nevyhnutné zabezpečiť vzdelávanie odborníkov a vyčlenenie dostatočného rozsahu finančných prostriedkov na vedu a výskum v oblasti kybernetickej bezpečnosti. Uvedené opatrenie si kladie za úlohu aj návrh novej národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Vyrastá nová generácia technicky nadaných ľudí, ktorých je potrebné vzdelávať, motivovať a umožniť im zapojiť sa do procesu vytvárania bezpečnostného systému.

V neposlednom rade je dôležité stavať na vytváraní nových a udržiavaní už existujúcich partnerstiev, resp. členstiev v medzinárodných organizáciách, ktoré sú nesmierne dôležité pre získavanie a odovzdávanie si informácií a vedomostí. Dôležitou súčasťou je taktiež účasť na domácich aj medzinárodných cvičeniach, ktoré preveria pripravenosť Slovenskej republiky na globálnu bezpečnostnú hrozbu 21. storočia, akou kybernetické útoky bezpochyby sú.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

BEZPEČNOSTNÁ RADA SR. 2017. Terminologický slovník krízového riadenia a zásady jeho používania [online]. Bratislava : Bezpečnostná rada SR, s. 12 [cit. 2020-12-30]. Dostupné na internete: <https://www.vlada.gov.sk/data/files/7616_terminologicky-slovnik-uprava260919.pdf>.

HOFREITER, Ladislav. 2016a. *Bezpečnostné prostredie súčasného sveta.* Zlín : Radim Bačuvčík – VeRBuM, 160 s. ISBN 978-80-87500-79-8.

HOFREITER, Ladislav – BYRTUSOVÁ, Andrea. 2016b. *Indikátory bezpečnosti.* Zlín : Radim Bačuvčík – VeRBuM, 136 s. ISBN 978-80-87500-82-8.

KAMPOVÁ, Katarína – HOLLÁ, Katarína. 2013. *Manažment sociálnych rizík.* Žilina : Žilinská univerzita v Žiline, 108 s. ISBN 978-80-554-0754-8.

KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ REPUBLIKY NA ROKY 2015 – 2020 [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf>.

MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY. 2019. *Podpisom dohody s občianskym združením AFCEA Slovakia chce rezort obrany pokračovať vo vytváraní vhodných podmienok v oblasti informačnej bezpečnosti* [online]. Bratislava : Ministerstvo obrany Slovenskej republiky [cit. 2020-12-30]. Dostupné na internete: <https://www.mosr.sk/48718-sk/podpisom-dohody-s-obcianskym-zdruzenim-afcea-slovakia-chce-rezort-obrany-pokracovat-vo-vytvarani-vhodnych-podmienok-v-oblasti-informacnej-bezpecnosti/>.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE ZA ROK 2019 [online]. Bratislava : Národný bezpečnostný úrad SR (Národné centrum kybernetickej bezpečnosti) s. 1-52 [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-SR-2019.pdf>.

Národný bezpečnostný úrad Slovenskej republiky. Národná jednotka CSIRT. In *Národný bezpečnostný úrad Slovenskej republiky* [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/sk-csirt/index.html>.

Návrh národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 predložený do medzirezortného pripomienkového konania. In *Slov-Lex* [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2020/583>.

Národný bezpečnostný úrad Slovenskej republiky. Kybernetická bezpečnosť (organizácie a partneri). EÚ a NATO [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/organizacie-a-partneri/europska-organizacia-kybernetickej-bezpecnosti/index.html>.

Národný bezpečnostný úrad Slovenskej republiky. Kybernetická bezpečnosť (organizácie a partneri). ECSO [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/organizacie-a-partneri/europska-organizacia-kybernetickej-bezpecnosti/index.html>.

Národný bezpečnostný úrad Slovenskej republiky. Kybernetická bezpečnosť (organizácie a partneri). CECSP [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/organizacie-a-partneri/stredoeuropska-platforma-pre-kyberneticku-bezpecnost/index.html>.

Národný bezpečnostný úrad Slovenskej republiky. Kybernetická bezpečnosť (organizácie a partneri). OBSE [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/organizacie-a-partneri/organizacia-pre-bezpecnost-a-spolupracu-v-europe/index.html>.

Národný bezpečnostný úrad Slovenskej republiky. Kybernetická bezpečnosť (organizácie a partneri). Bilaterálni partneri [online]. [cit. 2020-12-30]. Dostupné na internete: <https://www.nbu.gov.sk/kyberneticka-bezpecnost/organizacie-a-partneri/bilateralni-partneri/index.html>.

PORADA, Viktor. a kol. 2019. *Bezpečnostní vědy: Úvod do teorie, metodologie a bezpečnostní terminologie*. Plzeň : Aleš Čeněk, s. r. o., 780 s. ISBN 978-80-7380-758-0.

SIVÁK, Jaroslav. 2019. Kybernetická bezpečnosť. In *Hybridné hrozby na Slovensku. Analýza legislatívy, štruktúr a procesov v šiestich tematických oblastiach* [online]. Bratislava : GLOBSEC, s. 10-20 [cit. 2020-12-30]. Dostupné na internete: <https://www.globsec.org/wp-content/uploads/2018/01/Hybridne-hrozby-na-Slovensku.pdf>.

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov

VOLNER, Štefan. 2005. *Nová teória bezpečnosti: Teoreticko-metodologické východiská.* Zvolen : Bratia Sabovci, s. r. o., 340 s. ISBN 80-89029-99-X.

Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)

Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov

Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

Zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov

Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov

Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov

Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

por. JUDr. Michaela ŠIMONOVÁ
Externá doktorandka Katedry bezpečnosti a obrany,
Akadémia ozbrojených síl generála M. R. Štefánika Liptovský Mikuláš,
Demänová 393, 031 01, Liptovský Mikuláš,
telefón: 0960 316 060
e-mail: michaela.simonova1@gmail.com