ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA BEZPEČNOSTNÉHO INŽINIERSTVA
*KRÍZOVÝ MANAŽMENT - 2/2017*
*ISSN:1336 - 0019*
*str. 83-88*

# ASPEKTY KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU A VO SVETE

# ASPECTS OF CYBER SECURITY IN SLOVAKIA AND IN THE WORLD

Ján BREZULA[1]

***ABSTRACT:***

*Cyber security is becoming one of the most important challenges nowadays, and it is therefore essential for all states at national level to adopt an obligatory legal regulation on the protection of national cyberspace, which would ensure an adequate level of protection of critical infrastructure and essential security areas of state functioning. IT specialists from both private and government sector responsible for cyber security are aware of increasing number of sophisticated threats in recent years. This change is caused by the change of the global security space. Therefore, cyber security is apprehended as the subsystem of the national security and the cyber space such as new operational domain.*

***KEYWORDS:*** *cyber security, cyber risk, cyber threat, cyber terrorism, cyber-attack, critical infrastructure, cyber space*

## ÚVOD

Exponenciálny nárast používania informačných a komunikačných technológií veľmi 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. 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.

## 1. DEFINÍCIA KYBERNETICKÉHO PRIESTORU

Pojem kybernetický priestor slúžil pôvodne na označenie prostredia, v ktorom prebieha prenos a spracovanie digitálne zaznamenanej informácie. V súčasnosti označuje informačnú a komunikačnú infraštruktúru organizácie, štátu, alebo globálnu informačnú a komunikačnú infraštruktúru [1]. Kybernetický priestor je v zmysle Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 vymedzený ako virtuálny priestor bez hraníc, zložený z celosvetovo prepojených sietí z hardvéru, softvéru a dát [2].

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

Za najznámejší kybernetický priestor možno bezpochyby považovať sieť Internet, globálnu počítačovú sieť, ktorá je v súčasnej dobe prítomná a denne využívaná v každej krajine sveta, vrátane krajín s autoritárskymi režimami akými sú Severná Kórea, Kuba, Irán alebo Čína. Internet je síce najznámejším kybernetickým priestorom, ale nie jediným. V kontexte organizácií je kybernetickým priestorom akýkoľvek súbor jednej alebo viacerých vzájomne prepojených lokálnych počítačových sietí LAN (Local Area Network). Sieti, ktorá prepája tieto lokálne siete, sa potom hovorí WAN (Wide Area Network). Ako príklad kybernetických priestorov, ktoré nie sú pripojené k sieti Internet, je možné uviesť armádne počítačovej siete, technologické siete, policajné dátové siete a podobne.

[1] Ján Brezula, Ing., externý doktorand, Katedra bezpečnosti a obrany, Akadémia ozbrojených síl gen. M.R. Štefánika, Demänová 393, 031 06 Liptovský Mikuláš, jan.brezula@gmail.com.

## 2. KYBERNETICKÉ HROZBY VS. KYBERNETICKÉ RIZIKÁ

Kybernetická bezpečnosť predstavuje systém, ktorého úlohou je poskytnúť prostrediu spoločensko-ekonomickej štruktúry štátu bezpečný, chránený a v primeranom rozsahu otvorený kybernetický priestor a garanciu bezpečnosti elektronickým, informačným, komunikačným a riadiacim systémom, ktoré sa v tomto priestore nachádzajú.

Úlohou kybernetickej bezpečnosti je chrániť kybernetické systémy pred kybernetickými hrozbami. Kybernetická hrozba je hrozba, ktorá ťaží z existencie kybernetického priestoru [3]. Kybernetické hrozby môžu byť úmyselné (Malicious) a neúmyselné (non-Malicious). Medzi úmyselné hrozby možno zaradiť napríklad útoky vedené so zámerom preťažiť komunikačné a informačné systémy a zamedziť tak ich fungovaniu (Denial of Service, DoS). Neúmyselné hrozby môžu vzniknúť napríklad zlyhaním pevného disku z dôvodu jeho opotrebovania alebo vplyvom chyby v programovom kóde (reštart počítačového systému v dôsledku neošetrenej situácie v programe riadiacich komponentov počítačového systému).

Povaha hrozieb a rizík, ktoré sa môžu v kybernetickom priestore objaviť, je svojím spôsobom špecifická. Jedným zo špecifík kybernetických rizík je to, že ak riziko nastane, bude vždy mať negatívny vplyv na chod organizácie.

Rovnako tak sú špecifické aj metódy a techniky, ktoré sa pre riadenie a hodnotenie kybernetických rizík používajú. Jedným zo špecifík kybernetického priestoru je jeho potenciálny dosah, tz. pôvodca hrozby sa môže nachádzať kdekoľvek na svete a aj napriek tomu má dostatočný potenciál napadnúť a hlboko zasiahnuť analyzovaný kybernetický systém. Podobne desivo môže pôsobiť aj fakt, že nemalá časť kybernetických hrozieb vzniká s úmyslom uškodiť. Protivníci, ktorí sú pôvodcami týchto hrozieb, majú svoje motívy a úmysly často nečisté. Na druhej strane sa denne stretávame aj s hrozbami neúmyselnými.

Kybernetické riziko možno definovať ako riziko spôsobené kybernetickú hrozbou [3]. Zdefinície potom možno odvodiť, že kybernetické riziko nezahŕňa všetky riziká, ktorým môže byť kybernetický systém vystavený. Napríklad požiar miestnosti so servermi nie je kybernetickým rizikom (požiar zvyčajne nie je spôsobený kybernetickou hrozbou), zatiaľ čo nedostupnosť dát umiestnených na serveroch v dôsledku úmyselného preťaženia dátovej siete už kybernetickým rizikom je.

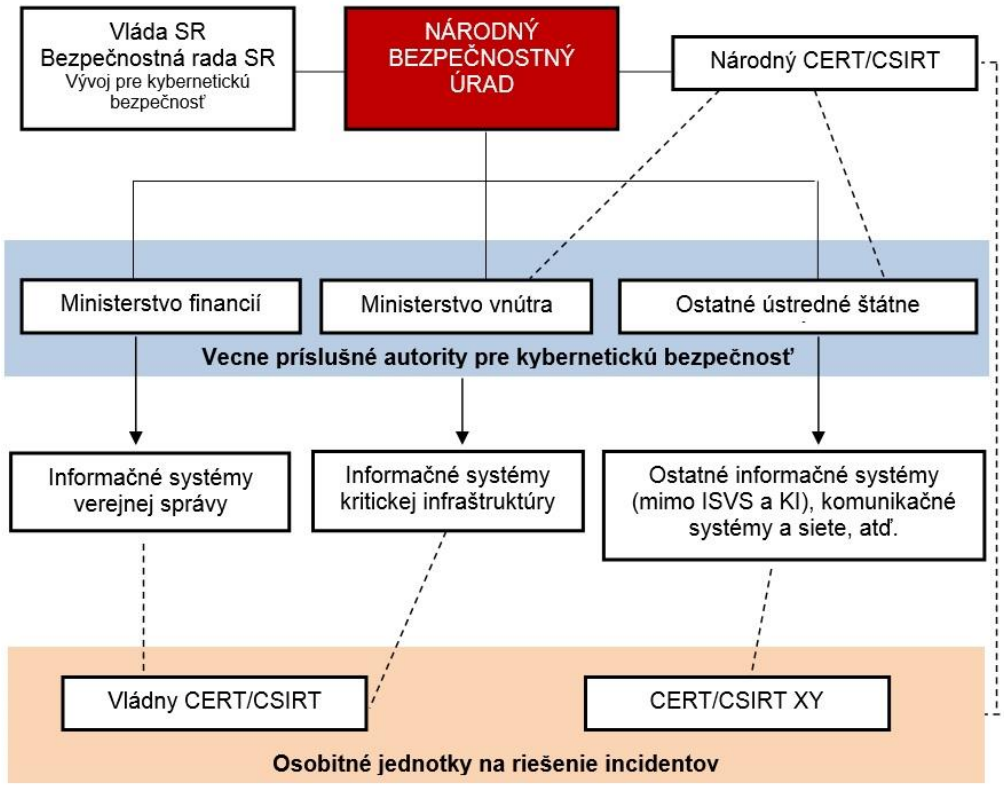
## 3. ZÁKONNÁ ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 je základným a východiskovým dokumentom pre tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zabezpečeniu kybernetickej bezpečnosti v rámci Slovenskej republiky.

Ústredným orgánom štátnej správy pre oblasť kybernetickej bezpečnosti na Slovensku bol na základe tejto koncepcie určený Národný bezpečnostný úrad. V rámci svojich kompetencií je zodpovedný najmä za:

- koordináciu, sledovanie, kontrolu a vyhodnocovanie plnenia úloh v oblasti kybernetickej bezpečnosti na národnej úrovni;
- vypracovanie Správy o stave kybernetickej bezpečnosti v Slovenskej republike a jej predloženie na schválenie Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR;
- návrh a predloženie postupu v prípade kybernetického útoku v rámci krízového riadenia Slovenskej republiky;
- priebežné monitorovanie národného kybernetického priestoru a analýzu potenciálnych a aktuálnych hrozieb;
- je národným kontaktným bodom pre EÚ a NATO v oblasti.

V súvislosti s určením Národného bezpečnostného úradu za ústredný orgán štátnej správy pre kybernetickú bezpečnosť prevádzkuje od 1. januára 2016 špecializovaný útvar pre riešenie počítačových incidentov s názvom Slovak Computer Security Incident Response Team (SK-CSIRT). Útvar zabezpečuje služby spojené najmä s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov.




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

Obrázok 1 **Rámcová štruktúra riadenia kybernetickej bezpečnosti** [2].

Od vzniku Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020 naďalej pokračovala práca na tvorbe legislatívneho rámca pre kybernetickú bezpečnosť a v súčasnej dobe je v medzirezortnom pripomienkovom konaní návrh Zákona o kybernetickej bezpečnosti.

Jeho príprava bola komplikovaná, nakoľko sa na jeho reálnej podobe podieľali nie len odborníci zo štátnej správy, ale aj z akademickej obce či mimovládni experti a analytici, ktorí vznášali pripomienky k jeho obsahu. Centrálnym orgánom určujúcim štandardy, operačné postupy, zásady predchádzania kybernetickým bezpečnostným incidentom a zásady riešenia kybernetických bezpečnostných incidentov sa podľa návrhu zákona stane Národný bezpečnostný úrad.

Národný bezpečnostný úrad má podľa tohto návrhu postavenie jednotky CSIRT [4], ktorá je nadradená ostatným jednotkám s rovnakým zameraním, ktoré už na Slovensku pôsobia. Jednotka CSIRT vo svojej pôsobnosti bude zodpovedať za riešenie kybernetických bezpečnostných incidentov a vykonávať reaktívne a preventívne služby.

Preventívne služby sa budú zameriavať najmä na prevenciu kybernetických bezpečnostných incidentov vytváraním bezpečnostného povedomia, výcvikom a spoluprácou s ostatnými jednotkami CSIRT.

Reaktívne služby budú určené na riešenie kybernetických bezpečnostných incidentov a to najmä na analýzu kybernetických bezpečnostných incidentov, podporu reakcie na kybernetické bezpečnostné incidenty, koordináciu reakcií na kybernetické bezpečnostné incidenty a návrhov opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

Okrem posilneného postavenia Národného bezpečnostného úradu zavádza navrhovaný zákon taktiež pojem „Stav kybernetického ohrozenia“, ktorý nastáva v prípade závažného zníženia úrovne kybernetickej bezpečnosti alebo bezprostrednej hrozby alebo rizika ohrozenia kybernetickej bezpečnosti, ak by v jeho dôsledku mohlo dôjsť k narušeniu bezpečnosti. Stav kybernetického ohrozenia vyhlasuje Národný bezpečnostný úrad

najdlhšie na 10 za sebou nasledujúcich dní s možnosťou jeho opakovaného predĺženia najviac na dobu 30 za sebou nasledujúcich dní [4].

Návrh zákon ďalej určuje Ministerstvu obrany SR vykonávať v potrebnom rozsahu štátnu správu na úseku kybernetickej bezpečnosti a to najmä [4]:

- po vypovedaní vojny alebo vyhlásení vojnového stavu;
- v čase krízovej situácie, ak kybernetický bezpečnostný incident ohrozuje systém obrany štátu a spôsobilosť zabezpečiť obranu štátu;
- ak informácie o kybernetickom bezpečnostnom incidente nasvedčujú, že kybernetický bezpečnostný incident môže byť kybernetickým terorizmom, alebo môže byť použitý ako prostriedok teroristického útoku a prijaté opatrenia neviedli k jeho odstráneniu v čase, ustanovenom pre daný typ ohrozenia alebo daný sektor všeobecne záväzným právnym predpisom.

Návrh zákona tvorí dobrý základ pre ďalšie legislatívne snahy v oblasti kybernetickej bezpečnosti. Jasne rozdeľuje kompetencie a určuje práva a povinnosti do právnej praxe a zavádza terminológiu používanú EÚ, čím uľahčuje medzinárodnú spoluprácu, pričom treba oceniť aj zapojenie súkromných spoločností do procesu jeho prípravy a jeho finálneho návrhu.

## 4. KYBERNETICKÁ BEZPEČNOSŤ V PONÍMANÍ EURÓPSKEJ ÚNIE A USA

Prvou celoeurópskou legislatívnou úpravou v oblasti kybernetickej bezpečnosti bolo prijatie smernice Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii (ďalej len „smernica NIS“). Smernica NIS sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov, zvyšuje ich vzájomnú koordináciu a je kľúčovou súčasťou celkovej stratégie kybernetickej bezpečnosti.

Smernica NIS najmä:

- zavádza bezpečnostné požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb a pre poskytovateľa digitálnych služieb;
- ukladá členským štátom povinnosť určiť vnútroštátne príslušné orgány, jednotné kontaktné miesta a bezpečnostné tímy jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“);
- ukladá členským štátom povinnosť prijať národnú stratégiu kybernetickej bezpečnosti;
- ustanovuje skupinu pre spoluprácu, za účelom podpory strategickej spolupráce a výmeny informácii medzi členskými štátmi a budovania vzájomnej dôvery;
- stavuje sieť jednotiek CSIRT, ktorej účelom je prispievať k budovaniu dôvery medzi členskými štátmi a podporovať účinnú spoluprácu.

V smernici NIS sa dodržiavajú základné práva a zásady uznané Chartou základných práv Európskej únie, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie.

Podľa smernice NIS každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré zodpovedajú za riešenie rizík a incidentov podľa presne stanoveného postupu. Základné požiadavky na jednotky CSIRT sú v zmysle smernice NIS nasledovné:

- jednotky CSIRT zabezpečujú vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, že zlyhajú ako celok, ak zlyhá ich ľubovoľný jediný bod, a majú k dispozícii niekoľko spôsobov, ktorými ich možno kontaktovať a ktorými môžu oni kedykoľvek kontaktovať iných. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany a spolupracujúci partneri sú o nich dobre informovaní;
- pracoviská jednotiek CSIRT a podporné informačné systémy sú umiestnené na zabezpečených miestach;
- jednotky CSIRT majú zavedený vhodný systém riadenia a zasielania žiadostí v záujme jednoduchšieho odovzdávania;
- jednotky CSIRT sú primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb;
- jednotky CSIRT využívajú infraštruktúru, ktorej kontinuita je zabezpečená. Na tento účel sú k dispozícii záložné systémy a záložný pracovný priestor;
- jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce, pokiaľ majú v úmysle byť ich súčasťou.

Na účely zabezpečenia kybernetickej bezpečnosti a účinného reagovania na kybernetické bezpečnostné incidenty je nevyhnutné zabezpečiť, aby v štáte existovali dobre fungujúce jednotky CSIRT, ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné spôsobilosti na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Európskej únie.

Bývalý americký prezident Barack Obama podpísal 18. decembra 2014 päť návrhov zákonov týkajúcich sa kybernetickej bezpečnosti, vrátane právnych predpisov, ktoré aktualizujú federálne riadenie informačnej bezpečnosti.

Po prvý raz sa tak v USA stala kybernetická legislatíva aj právnym predpisom. Poslednou významnou udalosťou v otázkach kybernetickej bezpečnosti bol totiž prezidentom podpísaný zákon E-Government ešte z roku 2002.

V decembri päť schválených zákonov zahŕňa nasledujúce oblasti pôsobenia:

- **Zákon o modernizácii federálnej informačnej bezpečnosti:** kodifikuje už existujúcu administratívnu prax riadenia správy a rozpočtu, ktoré podmieňujú bezpečnostné politiky federálnych agentúr. Ďalej tento zákon udeľuje Ministerstvu vnútornej bezpečnosti právo implementovať tieto operačné aspekty aj do civilných agentúr.
- **Zákon o posúdení pracovníkov národnej bezpečnosti:** je dodatkom Zákona o platovej reforme pracovníkov pohraničnej stráže a identifikuje a dopĺňa kyberneticko-bezpečnostné pracovné pozície na Ministerstve vnútornej bezpečnosti. Na základe IT schopností jednotlivých zamestnancov im ministerstvo zabezpečí konkurenčné ohodnotenie.
- **Zákon o posúdení pracovníkov kybernetickej bezpečnosti:** požaduje od Ministerstva vnútornej bezpečnosti posúdiť svojich pracovníkov v oblasti kybernetickej bezpečnosti a rozvíjanie stratégie na zdokonalenie ich pripravenosti a odbornosti tak, aby dokázalo v budúcnosti zabezpečiť ich dostatočné kapacity, kvalitný nábor a zabezpečiť stabilitu ich pracovných miest.
- **Zákon o ochrane národnej bezpečnosti:** kodifikuje Národnú kybernetickú bezpečnosť a Integračné komunikačné centrá, neustálu kybernetickú ostražitosť, systém rýchlej reakcie a manažment riadenia centier, ktoré majú tvoriť základ pre kybernetickú a komunikačnú integráciu federálnej vlády, presadzovania práva a spravodajskej komunity.
- **Zákon o zdokonalení kybernetickej bezpečnosti:** oprávňuje Ministerstvo obchodu uľahčovať a podporovať rozvoj dobrovoľných štandardov prostredníctvom Národného inštitútu pre štandardy a technológie za účelom zníženia potenciálnych kybernetických rizík v kritickej infraštruktúre. Zákon tiež vyžaduje, aby Úrad pre vedu a technológie vytvoril federálny kyberneticko-bezpečnostný výskum a plán jeho rozvoja.

Slovenská republika sa v roku 2004 stala plnohodnotným členom Severoatlantickej aliancie NATO. Úlohou tejto organizácie je chrániť slobodu a bezpečnosť svojich členov politickými a vojenskými prostriedkami, pričom je založená na spoločných hodnotách demokracie a ľudských práv, pri zachovávaní plnej suverenity a nezávislosti všetkých členských štátov.

Slovenská republika, ako právoplatný člen aliancie NATO, musí byť pripravená primerane reagovať aj na kybernetické hrozby, ktoré sa jej priamo netýkajú, ak to vyplýva z medzinárodných zmlúv a dohôd, ktorými je viazaná. Vzhľadom na to, že pri vedení súčasných medzinárodných konfliktoch využívajú sofistikované kybernetické útoky, sa čoraz častejšie spomína aplikácia čl. 5 Severoatlantickej zmluvy, ak by bol kybernetický útok svojou intenzitou, škodami a nepriateľským úmyslom porovnateľný s ozbrojeným útokom vedeným konvenčnými zbraňami.

## ZÁVER

Enormné zavádzanie informačných a komunikačných technológií prináša mnohé pozitíva, ktoré vedú k rozvoju informačnej spoločnosti, urýchleniu komunikácie a rozvoju služieb. Na druhej strane závislosť spoločnosti a jej fungovanie na týchto technológiách prináša so sebou mnoho hrozieb v podobe kybernetických útokov, ktoré sú čím ďalej sofistikovanejšie a komplikovanejšie.

Kybernetická bezpečnosť pomáha identifikovať, hodnotiť a riešiť hrozby v kyberpriestore, znižovať kybernetické riziká a eliminovať dopady kybernetických útokov, ktoré sa realizujú prostredníctvom informačnej kriminality, kyberterorizmu a kybernetickej špionáže v zmysle posilňovania dôvernosti, integrity a dostupnosti dát, systémov a ďalších

prvkov informačnej a komunikačnej infraštruktúry. Kybernetická bezpečnosť sa stáva jednou z najvýznamnejších výziev dnešnej doby a preto je nevyhnutné, aby štáty na národnej úrovni prijímali záväznú právnu reguláciu v oblasti ochrany národného kybernetického priestoru, ktorá by zabezpečila primeranú úroveň ochrany kritickej infraštruktúry a základných bezpečnostných oblastí fungovania štátu.

**LITERATÚRA**


[1] OLEJÁR, D. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. [on line] [cit. 2017-07-21]. Dostupné z: <http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s>.

[2] *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.*

[3] REFSDAL, A., SOLHAUG, B., STOLEN, K. *Cyber-Risk Management*. Springer International Publishing, 2015. 145 p. ISBN 978-3-319-23569-1.

[4] *Návrh zákona o kybernetickej bezpečnosti.*