Akadémia Policajného zboru v Bratislave

Katedra verejnej správy a krízového manažmentu

KYBERNETICKÁ BEZPEČNOSŤ AKO NOVÝ PRVOK V REALIZÁCII OPATRENÍ KRÍZOVÉHO MANAŽMENTU

ZBORNÍK

Z medzinárodnej vedeckej konferencie,
ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave

Bratislava
2018

Akadémia Policajného zboru v Bratislave

Katedra verejnej správy a krízového manažmentu

KYBERNETICKÁ BEZPEČNOSŤ AKO NOVÝ PRVOK V REALIZÁCII OPATRENÍ KRÍZOVÉHO MANAŽMENTU

ZBORNÍK

Z medzinárodnej vedeckej video konferencie,
ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave

Bratislava
2018

RECENZENTI:
prof. Dr. Jacek DWORZECKI, PhD.
doc. Dr. Mgr. Vladimír BLAŽEK, CSc.
doc. Ing. Karol FABIÁN, CSc.

GARANT: plk. Ing. Stanislav ŠIŠULÁK, PhD.- Prorektor pre informatizáciu a koordináciu s policajnou praxou APZ v Bratislave

VEDECKÝ VÝBOR:
plk. Ing. Stanislav ŠIŠULÁK, PhD. - APZ v Bratislave
prof. Ing. Rudolf URBAN, CSc. - UO Brno
prof. Ing. Bedřich ŠESTÁK, DrSc. - PA ČR
prof. PhDr. Ján BUZALKA, CSc. - APZ v Bratislave
doc. Dr. Mgr. Vladimír BLAŽEK, CSc. . - APZ v Bratislave
JUDr. Miroslav BRVNIŠTAN, PhD. - APZ v Bratislave
doc. JUDr. Štěpán KALAMÁR, PhD. - PA ČR
Ing. Josef NAVRÁTIL, CSc. - UO Brno
Ing. Vladimír ANDRASSY, PhD. - AOS L.M.
Ing. Matúš GREGA, PhD. - AOS L.M.

ORGANIZAČNÝ VÝBOR:
pplk. Ing. Igor PAVLOVIČ - APZ v Bratislave
doc. RNDr. Josef POŽÁR, CSc. - PA ČR
Ing. Marek ČANDÍK, PhD. - PA ČR
mjr. Ing. Marian SUJA, PhD. - APZ v Bratislave
mjr. Ing. Milan MARCINEK, PhD. - APZ v Bratislave
Bc. Katarína JUNASOVÁ - APZ v Bratislave
Ing. Jiří BARTA, PhD. - UO Brno

Z prednesených a dodaných príspevkov zborník zostavil:
mjr. Ing. Marian SUJA, PhD., pplk. Ing. Igor Pavlovič

Technický garant: mjr. Ing. Marian SUJA, PhD., pplk. Ing. Igor Pavlovič

ISBN 978-80-8054-750-9
EAN 9788080547509

OBSAH:

CIEĽ A ÚLOHY KONFERENCIE

Cieľ konferencie:

Analyzovať problémy a zovšeobecniť teoretické prístupy a praktické skúsenosti zúčastnených subjektov ako súčasť plnenia parciálnej časti integrovanej vedeckovýskumnej úlohy „Teória a metodológia krízového manažmentu vo verejnej správe ako aplikovanej vednej disciplíny a transfer jeho poznatkov do praxe subjektov verejnej správy“ a aktuálnych potrieb bezpečnostnej praxe v oblasti zvyšovania úrovne kybernetickej bezpečnosti.

Úlohy konferencie:

- Analýza vzťahu krízového manažmentu a formujúcej sa oblasti kybernetickej bezpečnosti;
- Možné problémy a výzvy využívania krízových scenárov pri ochrane kybernetického priestoru;
- Možnosti využitia opatrení krízového manažmentu v oblasti kybernetickej bezpečnosti;
- Identifikácia a prognóza možnosti ďalšieho využitia opatrení krízového manažmentu v oblasti kybernetickej bezpečnosti.

Tematické okruhy:

- Vedecké základy vzťahu krízového manažmentu a oblasti kybernetickej bezpečnosti;
- Teoretické východiská riešenia krízových scenárov v oblasti kybernetickej bezpečnosti;
- Možné oblasti spolupráce APZ, NBÚ, PA ČR, UO Brno a AOS v L. Mikuláši v oblasti kybernetickej bezpečnosti, vplyv na systém vzdelávania policajných manažérov.

ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI

Lubomír ALMER

Univerzita obrany v Brně

Abstrakt: *Kybernetická bezpečnost a její legislativní vymezení v právním řádě České Republiky hraje velice významnou roli v bezpečnosti. Jelikož se z kybernetické bezpečnosti stává "pojem", který je ze strany legislativy vyžadován, dochází tak k posunu problematiky kybernetické bezpečnosti do popředí a je jí věnována patřičná důležitost. Článek vymezuje legislativu vztahující se k problematice řízení rizik kybernetické bezpečnosti a tuto legislativě porovnává s mezinárodní ISO/IEC 27001 ze které Zákon o kybernetické bezpečnosti vychází. Dále je v článku sumarizována aktuální situace kybernetické bezpečnosti z hlediska hlášených kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.*

Klíčová slova: *Kybernetická bezpečnost, Zákon o kybernetické bezpečnosti, Bezpečnostní událost, Bezpečnostní incident.*

ÚVOD

Článek Úvod do kybernetické bezpečnosti je sumarizací poznatků z oblasti kybernetické bezpečnosti, tak jak jsou platné a používané v České republice. Článek je rozdělen do tří dílčích částí, kde první část je věnována legislativě vztahující se ke kybernetické bezpečnosti, druhá část je věnována kybernetické situaci v České republice a třetí řízení rizik dle Zákonu o kybernetické bezpečnosti v porovnání s řízením rizik definovaným ISO/IEC 27001. V části legislativa vztahující se ke kybernetické bezpečnosti jsou vyjmenovány hlavní zákony, vyhlášky a normy vztahující se k dané problematice, rovněž je zde stanovena kybernetická bezpečnosti za normálního a válečného stavu a její gestoři a jednotlivé organizační útvary, které tuto bezpečnost za daného stavu reprezentují. V části kybernetické situace v ČR jsou sumarizovány kybernetické bezpečnostní incidenty a to hlášené a identifikované Národním Centrem Kybernetické Bezpečnosti a jsou zde i znázorněny pro jednotlivé roky. Část řízení rizik dle ZoKB vs ISO/IEC 27001 znázorňuje proces řízení rizik a vzájemně je mezi sebou komparuje.

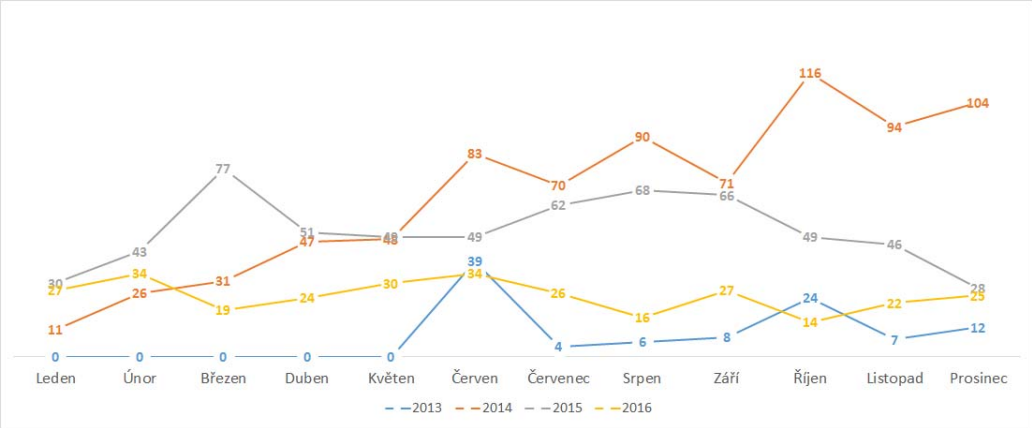
LEGISLATIVA VZTAHUJÍCÍ SE KE KYBERNETICKÉ BEZPEČNOSTI

Hlavním legislativním pilířem v oblasti kybernetické bezpečnosti je Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). K tomuto zákonu se dále vážou provázející vyhlášky a nařízení vlády. Jedná se o vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a Nařízení vlády č. 315/2015, kterým se mění nařízení vlády č. 432/2010 o kritériích určení prvků kritické infrastruktury. Tento zákon, provázející vyhlášky a nařízení vlády můžeme považovat za základní pilíř české kybernetické bezpečnosti. Avšak s kybernetickou bezpečností jsou dále spojeny i další zákony a nařízení vlády. Příkladem zákonů a nařízení vlády mohou být: Zákon č. 127/2005 Sb., o elektronických komunikacích, Zákon č. 412/2005 Sb., o ochraně utajovaných informací, Zákon č. 240/2000 Sb., o krizovém řízení, Zákon 480/2004 Sb., o některých službách informační společnosti, Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a mnoho dalších. Jelikož problematika kybernetické bezpečnosti se v dnešní době týká téměř každého systému či subjektu musí být na tuto bezpečnost pohlíženo velice

komplexně napříč veškerou legislativou. Dále musí být rozlišena kybernetické bezpečnost za normálního a válečného stavu. Gestorem kybernetické bezpečnosti za normálního stavu, stavu kybernetického nebezpečí a stavu nouze je Národní bezpečnostní úřad. Národní bezpečnostní úřad si v rámci své činnosti zřizuje organizační útvar, který působí na úseku kybernetické bezpečnosti a je označován jako Národní centrum kybernetické bezpečnosti (NCKB). Dále se v rámci NCKB zřizuje Vládní CERT/GovCERT jakožto součást NCKB sloužící primárně pro ochranu služeb a sítí elektronických komunikací a informačních systému před kybernetickými bezpečnostními událostmi. Jako další v rámci kybernetické bezpečnosti se zřizují Národní CERT/CSIRT pracoviště. Tyto pracoviště jsou provozovány soukromoprávními subjekty na základě veřejnoprávní smlouvy, která zajišťuje a zprostředkovává sdílení informací (hlášení bezpečnostních událostí, zranitelností a další) v národním i mezinárodním kontextu (i jako kontaktní místo poslední instance), a to zejména pro soukromoprávní subjekty, akademickou sféru, oblast samosprávy, neziskový sektor, za předpokladu, že subjekty z těchto oblastí nepodléhají zcela nebo v některých částech působnosti NBÚ. Národní CERT/CSIRT pracoviště koordinují svoji činnost s Národním bezpečnostním úřadem. Gestorem kybernetické bezpečnosti za stavu ohrožení státu a válečného stavu se stává vojenské zpravodajství a konkrétně Národní centrum kybernetických sil.

KYBERNETICKÁ SITUACE V ČR

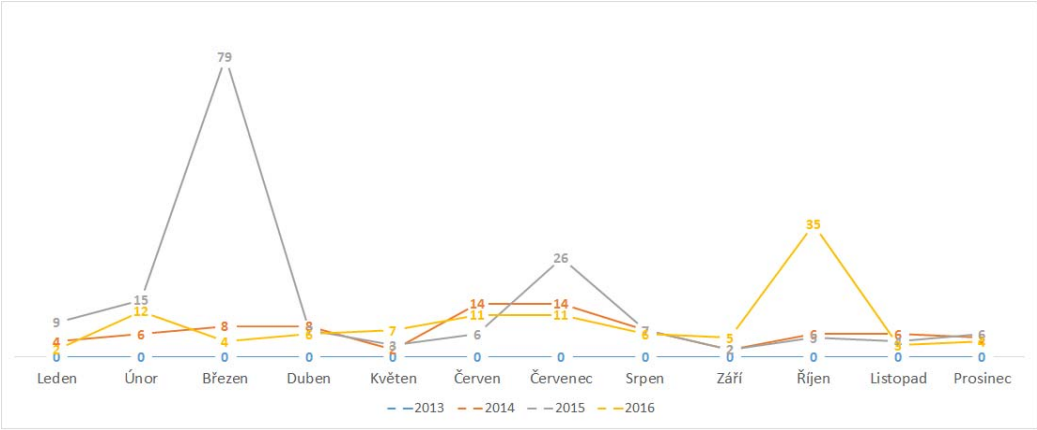
Národní centrum kybernetické bezpečnosti, zaznamenává v rámci své činnosti kybernetické incidenty, které dále zpracovává. Graf číslo jedna Incident reporty znázorňuje hlášené kybernetické incidenty od subjektů spadajících do působnosti zákona o kybernetické bezpečnosti. Tyto incidenty jsou NCKB hlášeny od roku 2013. Konkrétně byly první incidenty nahlášeny v červnu 2013. Graf znázorňuje incidenty od června 2013 do prosince 2016.



Obr. 1 Hlášené kybernetické incidenty

Zdroj: Upraveno autorem.

Jak je z obrázku Hlášené kybernetické incidenty patrné, bylo nejméně incidentů hlášeno v roce 2013 a nejvíce v roce 2014. Tento graf však znázorňuje pouze hlášené incidenty, nikoliv incidenty vyhodnocené NCKB. Následující graf: Identifikované bezpečnostní incidenty, znázorňuje vyhodnocené kybernetické incidenty, které byly NCKB vyhodnoceny jako incidenty nikoliv jako události. Z výše uvedeného vyplývá, že první graf znázorňuje sice hlášené kybernetické incidenty, ale po analýze NCKB se nejedná ve valné většině o kybernetické incidenty, ale o kybernetické události.

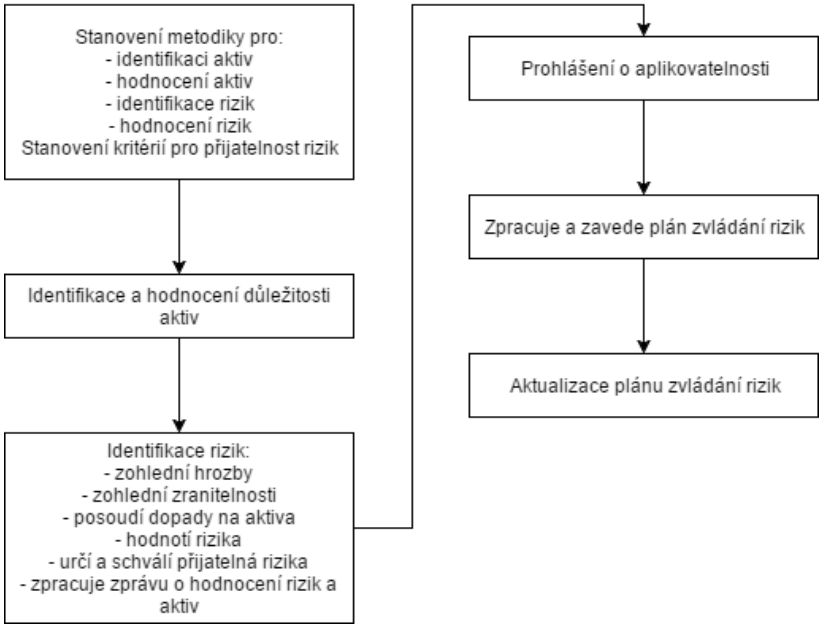


Obr. 2 Identifikované kybernetické incident

Zdroj: Upraveno autorem.

ŘÍZENÍ RIZIK ZoKB vs ISO/IEC 27005

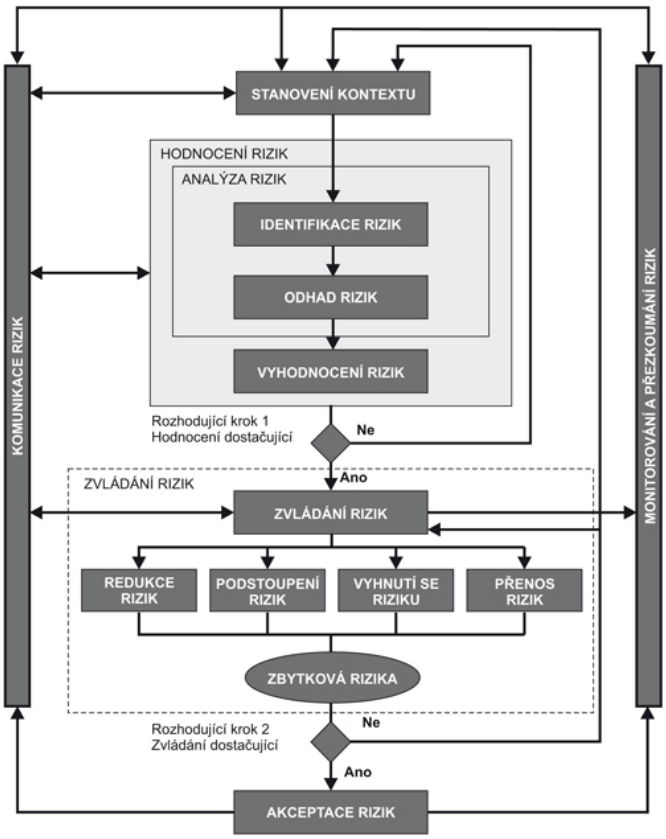
Obrázek číslo tři, řízení rizk dle Zákonu o kybernetické bezpečnosti znázorňuje provázanost jednotlivých kroků řízení rizik v jejich logické posloupnosti, tak, jak jsou uvedeny v zákonu. Jak je z obrázku patrné jedná se o šest dílčích kroků a to Stanovení metodiky, Identifikace a hodnocení důležitosti aktiv, Identifikace rizik, Prohlášení o aplikovatelnosti, Zpracování a zavedení plánu zvládání rizik a Aplikace plánu zvládání rizik. Každá z těchto částí má další dílčí pod části a dohromady tvoří komplexní pohled na problematiku řízení rizik, tak jak je stanovena zákonem o kybernetické bezpečnosti.



Obr. 3 Řízení rizik dle ZoKB

Zdroj: Upraveno autorem.

Obrázek číslo čtyři znázorňuje logické schéma řízení rizik dle ISO/IEC 27005. Jak je z obrázku patrné jedná se komplexnější postup, než v případě zákona o kybernetické bezpečnosti.



Obr. 4 Řízení rizik dle ISO/IEC 27005

Zdroj: ČSN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

V případě komparace řízení rizik dle ZoKB a ISO/IEC 27005 dojdeme k závěru, že ZoKB přímo vychází z ISO norem rodiny 27k. Jedná se o Obecný a nekonkrétní postup řízení rizik. Z rámci ISO norem je proces řízení rizik velmi detailně popsán, krok po kroku a je zde větší provázanost jednotlivých procesů. V případě ISO normy se jedná o cyklický proces, který je velice konkrétní a mezinárodně uznávaný. ZoKB je naproti tomu jedinečný, ale je omezen pouze národní působností a nadále by mělo docházet k jeho novelizacím a následnému zlepšování a rozšiřování.

ZÁVĚR

Problematika kybernetické bezpečnosti je v České Republice velice diskutovaným a řešeným tématem. Jak je z článku patrné problematice kybernetické bezpečnosti se v České Republice přiřazuje patřičná důležitost a Česká Republika bere problematiku kybernetické bezpečnosti velice vážně. Tento fakt je podpořen vznikem a novelizací zákonů, vyhlášek a norem vztahujících se k této problematice. Při pohledu na kybernetickou situaci České republiky, je možné usoudit, že kybernetické bezpečnostní incidenty jsou s Českou Republikou provázány, a budou se stávat i nadále, proto je patřičná bezpečnost zcela nepostradatelná. Při komparaci Zákonu o kybernetické bezpečnosti s mezinárodní ISO normou můžeme dojít k závěrům, že se sice jedná o velký krok vpřed v případě zákonu, avšak je třeba jej ještě více specifikovat, konkrétně v případě řízení rizik.

SEZNAM POUŽITÉ LITERATURY

ČSN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

Národní bezpečnostní úřad. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky.

Národní bezpečnostní úřad. Vyhláška č. 316 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: Sbírka zákonů České republiky.

Seznam použitých zkratek

ČR	Česká Republika
ZoKB	Zákon o kybernetické bezpečnosti
NCKB	Národní centrum kybernetické bezpečnosti
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
GovCERT	Governance Computer Emergency Response Team

ADRESA
Ing. Lubomír ALMER
Katedra krizového řízení
Fakulta vojenského leadershipu
Univerzita obrany
Kounicova 65, 66210 Brno, Czech Republic
lubomir.almer@unob.cz

PASIBO - NÁSTROJ PRE ANALÝZU A SIMULÁCIU INFORMAČNÝCH A BEZPEČNOSTNÝCH OHROZENÍ

Vladimír ANDRASSY / Matúš GREGA

Akadémia ozbrojených síl generála Milana Rastislava Štefánika

Abstract: *Vznik celosvetovej komunikačnej a informačnej siete, masívne využívanie počítačov, internetizácia spoločnosti, digitálne spracovanie informácií a obchodovanie s nimi ako aj prenos dát a informácií prostredníctvom sietí na veľké vzdialenosti vedú k prehlbujúcej sa závislosti vyspelých štátov sveta a ich ekonomík na komunikačných a informačných technológiách, k zvyšovaniu vzájomnej prepojenosti i závislosti a zároveň k "zmenšovaniu" vzdialeností medzi nimi. Tento technologický pokrok však prináša nielen nové príležitosti, výzvy a prosperitu, ale aj nové bezpečnostné riziká a hrozby. Preto sa čoraz dôležitejšou a naliehavejšou stáva ochrana kybernetického priestoru a kritickej informačnej infraštruktúry, čiže zaistenie kybernetickej bezpečnosti.*

Aj Slovenská republika prostredníctvom svojej bezpečnostnej politiky aktívne pôsobí na bezpečnostné prostredie v euroatlantickom priestore tak, aby chránila, obhajovala a presadzovala svoje bezpečnostné záujmy. Flexibilne reaguje na meniace sa bezpečnostné hrozby a výzvy s cieľom obmedziť až eliminovať ich negatívny dosah na bezpečnosť a život občana, na zabezpečenie jeho ochrany pred násilnými hrozbami, ohrozeniami, živelnými pohromami, priemyselnými haváriami, inými katastrofami, na zaistenie jeho bezpečnosti v rámci komunikačných a informačných ohrození.

Key words: *informačné a bezpečnostné ohrozenia, analýza a simulácia ohrození*

ÚVOD

Bezpečnosť Slovenskej republiky je neoddeliteľne spätá aj s bezpečnosťou našich susedov a ostatných štátov v euroatlantickom priestore, ktorí sú vystavení podobným hrozbám a výzvam, akým čelíme my. Analýza rizík je nevyhnutným predpokladom k pochopeniu ohrození v čoraz globálnejšom svete. Reakcia „iba" na národnej alebo regionálnej úrovni je nedostatočná.[1] Posledné skúsenosti z vojenských a nevojenských konfliktov poukazujú na kľúčové postavenie informačnej infraštruktúry s dôrazom na bezpečnosť elektronických systémov. Od ich spoľahlivého fungovania dnes závisia vitálne funkcie štátov, väčšina používaných technických systémov, ktorých zlyhanie následne pôsobí na vznik rôznych ohrození.[2] Preto sa ako jediným účinným riešením javí koordinovaný globálny prístup medzinárodného spoločenstva, spojenie úsilia v oblasti analýzy, vyhodnocovania, validácie a simulácie možných informačných a bezpečnostných rizík.[3]

Bezpečnostné trendy vychádzajú z predpokladu dostupných vedeckých a výskumných kapacít v oblasti informačných, komunikačných a simulačných technológií. Realizovaním projektu „Pracovisko analýz a simulácie informačných a bezpečnostných ohrození" (ďalej len „PASIBO") sa v Akadémii ozbrojených síl gen. M. R. Štefánika v Liptovskom Mikuláši (ďalej len „akadémia") vytvorili podmienky pre možnosť interdisciplinárneho riešenia výskumných a vývojových úloh opierajúcich sa o potrebu zabezpečenia informačno-komunikačných technológií napr.: pred kybernetickými útokmi a o technológie zamerané do oblasti modelovania a simulácie napr.: simuláciu krízových javov a ich riešenia.

PASIBO rieši dobudovanie a modernizáciu pracovísk akadémie zameraných na analýzu a vyhodnotenie výstrah pred informačnými ohrozeniami, testovanie odolnosti počítačovej siete voči jednotlivým druhom kybernetických útokov a následnú verifikáciu činností krízových štábov simuláciou navrhovaných riešení. Spája možností špecifikácie budúceho informačného

[1] IVANČÍK, R. - KAZANSKÝ, R.: Kybernetická bezpečnosť. 2015.
[2] IVANČÍK, R. Kybernetická bezpečnosť - neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. 2012.
[3] BUČKA, GONOS: Bezpečnosť priemyselných sietí v prostredí moderných kybernetických hrozieb. 2013.

a bezpečnostného ohrozenia so simuláciou a validáciou jednotlivých krokov smerujúcich k hľadaniu možných riešení existujúcich rizík. Tieto oblasti navzájom úzko vertikálne súvisia, predstavujú kľúčové spôsobilosti pre udržanie bezpečnosti a doposiaľ nie sú ucelene riešené.

PASIBO

Jedným z hlavných cieľov budovania PASIBO bolo vytvoriť syntetické prostredie pre nepretržitú analýzu a hodnotenie možných informačných a bezpečnostných ohrození. Uvedené ohrozenia chápeme ako bezprostredné, deštrukčné, časovo a priestorovo synchronizované pôsobenia na celistvosť a funkčnosť špecifického systému spôsobujúce ohrozenie jeho existencie. Infraštruktúra poskytuje platformu na inovovanie existujúcich postupov a vytvorenie nových možností pre efektívnejšiu analýzu a vyhodnotenie informačných a bezpečnostných ohrození.

PASIBO je tvorené dvoma samostatnými laboratóriami prepojenými s už existujúcou infraštruktúrou akadémie:

- Laboratórium pre analýzu a vyhodnocovanie informačných a bezpečnostných ohrození (ďalej len „LAVIBO“),
- Laboratórium pre verifikáciu a simuláciu informačných a bezpečnostných ohrození (ďalej len „LVSIBO“).

LAVIBO

Platforma LAVIBO slúži na efektívnejšie zabezpečenie zberu dostupných poznatkov o potenciálnych hrozbách a ich cielenom sústredení na jedno miesto tak, aby bolo možné vykonať ich komplexné analytické vyhodnotenie a skoré poskytnutie analyticky spracovaných informácií relevantným príjemcom. V takto vytvorenom unikátnom virtualizovanom prostredí je možné realizovať komplexné scenáre útokov proti kritickým infraštruktúram, analyzovať ich priebeh s využitím analytických metód napr.: časová, prediktívna, štatistická, geografická, transakčná, skúmať ich dopad na odolnosť a prevádzkyschopnosť kritických infraštruktúr a s použitím pokročilých metód modelovania realizovať identifikáciu a vývoj nových bezpečnostných metód. Prostredie zároveň slúži pre overovanie navrhnutých bezpečnostných metód a prípravu podkladov pre ich verifikáciu a simuláciu za účelom transferu získaných poznatkov do aplikačnej praxe.

LAVIBO rozširuje spôsobilosti PASIBO so zameraním na výskum, vývoj a zostavovanie unikátneho prostredia pre analýzu hrozieb orientovaných na bezpečnosť kritických informačných infraštruktúr. V laboratóriu je možné simulovať rozsiahlu počítačovú sieť, jej služby a aplikácie spôsobom, kedy je možné skúmať šírenie kybernetických hrozieb a ich dopady.

Hardvérové (ďalej len „HW“) a softvérové (ďalej len „SW“) prostredie pre informačné a bezpečnostné ohrozenia je rozdelené do dvoch navzájom prepojených modulov simulácií kybernetických útokov - učební, analytickej miestnosti, technologickej miestnosti a miestnosti so systémom konštruktívnej simulácie na platforme OTB v2.5[4]. Technologická miestnosť LAVIBO je vybavená HW pre analýzu informačných a bezpečnostných ohrození a pozostáva z virtualizačného prostredia, dátového úložiska a nevyhnutných aktívnych a pasívnych prvkov sieťovej infraštruktúry. Tieto prvky poskytujú adresárové služby, emailový server, manažment služby, služby DNS[5], hlasové a videokonferenčné služby a prípadne ďalšie služby nevyhnutné pre zabezpečenie štandardnej prevádzky. Komunikačný systém LAVIBO predstavuje neoddeliteľnú a integrálnu súčasť samotného laboratória. Vytvára transparentné komunikačné prostredie pre multiplatformové simulácie kybernetických útokov vrátane mitigácie ich dopadov na proces riešenia informačných a bezpečnostných stavov s plnohodnotným využitím v súčasnosti používaných heterogénnych komunikačných drôtových ale aj bezdrôtových technologických platforiem. Vývojový systém

[4] OTB - One (Semi Automated Forces) Testbed Baseline ver. 2.5. Štandardný nástroj konštruktívnej simulácie plnohodnotne implementovaný vo výcvikovom prostredí od roku 2003.

[5] DNS - Domain Name Servise. Ide o systém, ktorý ukladá prístup k informácii o hostname a názve domény v istej distribuovanej databáze v počítačových sieťach.

poskytuje podporu štatistického testovania súboru náhodných dát, z pohľadu škálovateľnosti a logickej prepojenosti jednotlivých simulácií je platforma schopná obsiahnuť viaceré typy rozhraní.

Z pohľadu architektúry dátového úložiska je manažmentové prostredie realizované na rozdielnych typoch diskových entít takým spôsobom, aby tieto boli schopné reagovať na dynamické zmeny bezpečnostného prostredia. Tým vytvárajú predpoklady na realizáciu výskumných a vývojových úloh s využitím modelovania a simulačných techník. HW a SW komponenty poskytnú dostatočný základ pre sofistikované simulácie v oblasti sociálneho inžinierstva, forenznej, dynamickej a statickej analýzy pre oblasť výskumu, s následným výstupom vo forme štruktúrovaných údajov pre komplexné simulácie ohrození s využitím nástroja OTB v2.5 v tesnom kontexte s využívaním analytických a forenzných SW nástrojov.

Virtualizačné prostredie je logicky rozdelené na dve samostatné prostredia a to na prostredie manažmentu a prostredie simulácií kybernetických útokov. Tie sú umiestnené v dvoch samostatných učebniach vybavených HW prvkami simulácií kybernetických útokov. Prostredie manažmentu je vybavené aplikačným SW testovania bezpečnostných ohrození, systémom bezpečnostného monitoringu siete Security Information and Event Management (ďalej len „SIEM“) a HW komponentmi pre podporu vizualizácie výskumných úloh. Na účely optimalizácie výpočtového výkonu takto realizované prostredie využíva dedikovanú časť centralizovaného výpočtového výkonu a diskového priestoru serverovej infraštruktúry umiestnenej v technologickej miestnosti LAVIBO.

Prostredie manažmentu je vybavené špecifickým HW, ktorý umožňuje realizáciu bezpečnostného monitoringu siete prostredníctvom systému SIEM resp. monitoring zmien v systéme na úrovni aplikácií. Zároveň je možné v reálnom čase simulovať poskytnutie pomoci „napadnutým“ používateľom, resp. simuláciu prvotnej reakcie na incident s využitím HW pre analýzu informačných a bezpečnostných ohrození. Po ukončení simulácie sú zozbierané údaje podrobované hĺbkovej forénznej analýze (reverznému inžinierstvu). Tým sa zabezpečí realizácia procesu budovania znalostnej databázy informácií o formách a spôsoboch kybernetických útokov s využitím SW nástrojov prediktívnych analýz informačných a bezpečnostných ohrození. Takto získané dáta sú zobrazované a prezentované aj pre potreby ďalšieho modelovania a simulácie priebehov informačných a bezpečnostných ohrození s využitím prvkov konštruktívnej simulácie. Zároveň sa tak umožní ohodnotenie rizikových objektov na základe ich prepojení s extrapoláciou na geografické údaje. LAVIBO v rámci PASIBO zabezpečuje:

- jedinečné sofistikované prostredie pre výskum a vývoj metód na ochranu proti útokom na kritickú infraštruktúru,
- jednoduchú realizáciu bezpečnostných experimentov krízového riadenia s maximálnou mierou konfigurovateľnosti topológie siete,
- poskytovanie informácií krízovým štábom zo vstavanej meracej infraštruktúry s predefinovanými meranými veličinami,
- vizualizáciu dejov a udalostí prebiehajúcich v počítačovej sieti,
- konektivitu medzi jednotlivými laboratóriami a ostanými pracoviskami výskumu a vývoja akadémie.

LVSIBO

Platformu LVSIBO definujeme ako výskumné a vývojové laboratórium zabezpečujúce procesy simulácie a modelovania rôznych druhov ohrození v rámci riešenia úloh národnej a medzinárodnej bezpečnosti. Simulácia predstavuje primárny zdroj údajov a informácií pre výskum možností predchádzania následkov alebo ich odstraňovania počas riešenia krízových javov. Variantnosť a zložitosť hľadania najvýhodnejších riešení krízových javov s ich následným vyhodnocovaním nedávajú pri použití klasických nástrojov možnosť výberu optimálneho riešenia. Dobudovaním a modernizáciou používaných simulačných nástrojov sa v akadémii rozšírilo prostredie používanej

konštruktívnej a virtuálnej simulácie. Uvedený simulačný nástroj podporuje simuláciu možností riešenia jednotlivých fáz ohrozenia definovaním príznaku, určením vzniku a trvania krízového javu, návrhom a verifikáciou samotných riešení smerujúcich k obnove a opätovnému stavu pred vznikom ohrozenia.

LVSIBO dopĺňa existujúcu HW a SW základňu a rozširuje ju o možnosti riešenia úloh zameraných na informačné a bezpečnostné ohrozenia. Simulácia využíva stochastické a deterministické procesy (algoritmy) priebehu krízových situácií na syntetickom digitálnom terénnom podklade doplnenom o environmentálne javy, o samostatné moduly a entity charakterizujúce obyvateľstvo, infraštruktúru a dostupné technické prostriedky. V rámci bezpečnostnej komunity je dôraz položený na simuláciu špecializovaných entít výkonného prvku subjektov zabezpečujúcich riešenie krízovej situácie (hasičského a záchranného zboru, policajného zboru a záchrannej zdravotnej služby) špecializovaným SW simulátora výkonného prvku. HW simulátora výkonného prvku poskytuje dostatočný výpočtový a grafický výkon pre SW simulátora výkonného prvku. Procesy prípravy, vykonania a vyhodnotenia simulácie sú manažované špecifickým SW z miesta riadenia a vyhodnotenia. HW miesto riadenia a vyhodnotenia zabezpečuje riadenie a záznam simulácie s požadovaným štatistickým výstupom a funkčným prepojením s HW simulátora výkonného prvku. Výstupy modelovania a simulácie, ukladanie priebehu simulácie pre potreby analýzy a syntézy, diagnostiku chýb a procesov formou grafického zobrazenia v reálnom čase zabezpečuje HW simulátora pre I/O zariadenie.

Inštaláciou a prepojením HW a SW vybavenia LVSIBO s už existujúcimi druhmi simulácie a so zabezpečením interkonektivity s OTB v.2.5 je umožnené simulovať a ovládať skupiny alebo jednotlivcov prislúchajúcich bezpečnostnej komunite. Realizovaná spätná väzba umožňuje reagovať na vzniknutú situáciu na mieste simulovaného krízového javu v reálnom čase, podľa reálneho rozhodnutia a špecifického určenia. Simulovaná entita podľa svojho poslania v reálnom čase reaguje na vonkajšie podnety, na vzniknutý stav v mieste simulovaného ohrozenia. Komunikácia je zabezpečovaná HW komponentmi komunikačného systému simulátora výkonného prvku a to aj s ostatnými súčasťami vytvorenej simulačnej infraštruktúry konštruktívnej a virtuálnej simulácie. Je podporená možnosť vytvárania komplexného záznamu priebehu simulácie s prepojením do jednotnej databázy definovanej DIS protokolom[6] systému OTB v2.5. Systém hlasovej komunikácie simuluje rádiové spojenie a umožňuje simulovať jednotlivé rádiové siete (kanály) formou konferenčných hovorov alebo hovorov Bod - Bod. Vzájomná interkonektivita jednotlivých druhov simulácií realizovaných v LAVIBO a LVSIBO podporuje získanie podkladov potrebných ku komplexnému riešeniu problematiky v oblasti informačných a bezpečnostných ohrození.

Prepojením laboratórií do funkčného celku - PASIBO je zabezpečený komplexný „pohľad“ na postupnosť jednotlivých krokov smerujúcich k riešeniu krízových javov. Interkonektivita podporuje definovanie predpokladaných informačných a bezpečnostných ohrození, skúmanie činnosti, reakcií a správanie sa modulov, validitu vedeckých postupov a argumentov, ich analýzu, vyhodnocovanie a diagnostiku s cieľom hľadania optimálnych metód, postupov a spôsobov. LVSIBO v rámci PASIBO zabezpečuje:

- verifikáciu existujúcich metód a postupov riešenia informačných a bezpečnostných ohrození,
- jedinečné sofistikované prostredie pre výskum a vývoj v oblasti riešenia úloh bezpečnostnej komunity s využitím simulačných technológií,
- vizualizáciu dejov a udalostí prebiehajúcich v simulovanom virtuálnom syntetickom prostredí,

[6] Distibuted Interactive Simulation. Distribuovaná Interaktívna Simulácia je štandardizovaný protokol. Predstavuje platformu pre vedenie wargamingu v reálnom čase cez viac hostiteľských počítačov a je celosvetovo používaná, primárne pre vojenské využitie. Štandard DIS je definovaný v IEEE 1278.

- konektivitu medzi jednotlivými laboratóriami a ostanými pracoviskami výskumu a vývoja akadémie.

ZÁVER

Oblasť bezpečnosti je veľmi dynamická, rýchlo sa rozvíjajúca, preto je pre zabezpečenie efektívnej ochrany potrebné mať vybudovanú infraštruktúru určenú na výskum a vývoj predpokladaných hrozieb, ich analýzu, vyhodnotenie, elimináciu resp. efektívne odstraňovanie následkov v neustále sa meniacom dynamickom prostredí.[7]

Zámerom projektu PASIBO bolo dobudovať, modernizovať a skvalitniť technické a laboratórne vybavenie špecializovaného výskumného a vývojového pracoviska tak, aby sme boli schopní zdieľať vedomosti o ohrozeniach, kvantitatívnych a kvalitatívnych ukazovateľoch zvyšovania odolnosti a možnej obnove aplikovaním navrhnutých riešení. PASIBO je schopné na spoločnom základe, analýzou obsahu, hľadaním skrytých súvislostí a vzájomným prepojením pracoviska s existujúcou infraštruktúrou akadémie poskytnúť podporu pre spracovávanie, analýzu, vyhodnotenie, uchovávanie, verifikáciu a simuláciu rôznych ohrození v oblasti ochrany a bezpečnosti.

Prepojené simulačné nástroje a syntetické prostredia umožňujú budovanie znalostnej a inteligenčnej databázy o správaní sa útočníkov v celom rozsahu kľúčových fáz životného cyklu, vrátane plánovania, zberu a stanovenia priorít podrobnejšieho výskumu.[8] Inteligenčná databáza poskytuje informácie o procesoch so SW možnosťami vyhľadávania a tvorby štruktúrovaných údajov pre podrobnejšie analýzy a identifikácie vzťahom medzi objektmi - osobami, miestami, udalosťami a pod. V rámci simulácie informačných a bezpečnostných ohrození (kybernetických útokov) a následného zberu údajov LAVIBO poskytuje sofistikované metódy pre budovanie pracovných postupov prispôsobených pre konkrétne krízové situácie s výstupom na globálne simulácie riešených ohrození.

PASIBO podporuje prijaté uznesenia vlády Slovenskej republiky č. 499/2007 k návrhu postupu pri implementácii systému reakcie NATO na krízy (NCRS[9]) v podmienkach Slovenskej republiky, č. 161/2008 k návrhu zoznamu opatrení Národného systému reakcie na krízové situácie a zákony č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov, č. 321/2002 Z. z. o ozbrojených silách Slovenskej republiky v znení neskorších predpisov a č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení neskorších predpisov s jeho vykonávacími predpismi.

Táto práca bola podporená výstupmi projektu „Pracovisko analýz a simulácie informačných a bezpečnostných ohrození (PASIBO) - Analysis and Simulation of Information and Security Threats Workplace“, riešeným v rámci OP Výskum a vývoj, Prioritná os 1 Infraštruktúra výskumu a vývoja, Opatrenie 1.1 Obnova a budovanie technickej infraštruktúry výskumu a vývoja, kód výzvy OPVaV-2015/1.1/03-SORO, ITMS kód 26210120044.

ZOZNAM POUŽITEJ LITERATÚRY

BUČKA, P., GONOS, M.: Bezpečnosť priemyselných sietí v prostredí moderných kybernetických hrozieb. In: Acta Scientifica Academiae Ostroviensis [elektronický zdroj]: Sectio A: Nauki humanistyczne, społeczne i techniczne. - ISSN 2300-1739. - č. 1 (2013), online, s. 101-127. Plný text: http://zn.wsbip.edu.pl/wydania/zeszyt2/sekcjaA/zeszyt_a.pdf

CAYIRCI, E., MARINCIC, D.: Computer assisted exercises and training: a reference guide. Hoboken, N.J.: John Wiley, c2009, xvi, ISBN 04-704-1229-1.

[7] CZOSSECK, C., PODINS, K.: Conference on Cyber Conflict. NATO Center of Excellence for Cyber Defence. NATO Review: Nové hrozby - kybernetické dimenzie. 2011.
[8] NEČAS, P., GREGA, M.: Simulation technologies: implications for security management and training. 2013.
[9] NCRS - NATO Crisis Response System.

CLARKE, R.A., KNAKE, K.K.: Cyber war - The next threat to national security and what to do about it. New York, NY: Harper Collins Publishers. 2010. 261 s. ISBN 978-0-06-196223-3.
CZOSSECK, C., PODINS, K.: Conference on Cyber Conflict. NATO CCD COE. Tallinn. ISBN: 978-9949-9040-1-3
IVANČÍK, R.: Kybernetická bezpečnosť - neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie. Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012. s. 173-182. ISBN 978-80-8040-450-5.
IVANČÍK, R. - KAZANSKÝ, R. Kybernetická bezpečnosť. In Bezpečnostné fórum 2015, zborník vedeckých prác z 8. medzinárodnej vedeckej konferencie. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela - Belianum, ISBN 978- 80-557-0849-2.
NATO Center of Excellence for Cyber Defence: http://www.ccdcoe.org/
NATO Review: Nové hrozby - kybernetické dimenzie. 2011. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SK/index.htm
NEČAS, P., GREGA, M.: Simulation technologies: implications for security management and training. In: Security and Defence [elektronický zdroj]: quarterly. ISSN 2300-8741. No. 2 (2013), online. Plný text: http://wydawnictwo.aon.edu.pl/pl/images/Security_2_2013.pdf.
TOLK, A., NABIL R. A., CAYIRCI, E., PICKL, S., SHUMAKER R., SULLIVAN J. A., WAITE, W. F. Defense And Security Applications Of Modeling And Simulation - Grand Challenges And Current Efforts, Proceedings of the 2012 Winter Simulation Conference, Berlín, Nemecko 2012, ISBN 978-1-4673-4781-5.

ADRESA

Ing. Vladimír ANDRASSY, PhD.
Katedra bezpečnosti a obrany
Tel: 00421 960 423 951
vladimir.andrassy@aos.sk

kpt. Ing. Matúš GREGA, PhD.
Simulačné centrum
Tel: 00421 960 422 648
matus.grega@aos.sk

Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 06 Liptovský Mikuláš

IDENTIFIKACE RIZIK INFORMAČNÍ BEZPEČNOSTI

Jiří BARTA, Michaela VAŠKOVÁ, Petra BEŇOVÁ

Univerzita obrany v Brně

Abstrakt: *Článek se zabývá výzkumem v oblasti informační bezpečnosti. Je zaměřen na problematiku vnímání a hodnocení rizika, které vzniká při nakládání s informacemi, využíváním informačním technologiím, zejména v oblasti kybernetické bezpečnosti. Výzkum, který byl prováděn, se zaměřil především na studenty Univerzity obrany z různých ročníků a oborů. Srovnával i rozdílné přístupy civilních studentů a studentů vojenských oborů (vojáků z povolání). Byl navržen dotazník zjišťující vnímání kybernetických hrozeb a na základě jeho vyhodnocení budou realizována opatření ke zvýšení kybernetické bezpečnosti u vybraných skupin.*

Klíčová slova: *informační bezpečnost, zákon o kybernetické bezpečnosti, bezpečnostní hrozby, hodnocení bezpečnosti.*

ÚVOD

V současné době je problematika informační bezpečnosti velmi diskutovaným tématem. Rizika spojená se zabezpečením vlastních dat a systémů se dotýkají nejen velkých firem s cenným know-how, ale prakticky každého běžného uživatele informačních technologií (Hromada et al., 2015). Stále častěji se cílem útočníků stávají obyčejní lidé. Ti nedisponují sofistikovanou bezpečnostní ochranou jako velké firmy a vládní agentury. Cílem útoků bývá především krádež osobních údajů, které mohou být následně zneužita. Jsou to například přihlašovací loginy a hesla do emailů, e-shopů nebo i internetového bankovnictví (Procházková a kol., 2006). Právě internetové bankovnictví se v poslední době stalo velmi lukrativní oblastí pro zločince, kteří se cestou zneužití osobních údajů, snaží získat větší finanční prostředky (Náplavová, 2015).

Prostředí elektronické komunikace a Internetu je pro velké množství uživatelů světem bez jasně daných pravidel a základních záruk. Je to svět, kde je možné existovat pod smyšlenou identitou nebo si vytvořit identitu novou, eventuálně popřít své činy a spoléhat se na anonymitu, nepostižitelnost a nedokazatelnost. Na počátku byl Internet pouze pracovním nástrojem sloužícím ke komunikaci vzdálených skupin a zdrojem informací. V současnosti Internet nabízí nepřeberné množství příležitostí k jeho využívání.

ANALÝZA SOUČASNÉHO STAVU

Informační bezpečnost je nutné chápat jako komplexní pojem, který zahrnuje souhrnné pojetí pro komplexní přístup k ochraně informací. Cílem informační bezpečnosti je zejména ochrana informací a dat před negativními událostmi, jako je jejich ztráta, odcizení, únik, zneužití, zničení, narušení či změny, tedy jakékoliv porušení celistvosti, důvěrnosti nebo dostupnosti, které může mít negativní důsledky (Hromada et al., 2015). Informační bezpečnost představuje ochranu informací ve všech jejich formách, ve fyzické podobě, digitální podobě a dokonce i ochranu informací, které jsou uloženy v mozku jednotlivých uživatelů. V současnosti je zřejmě nejdiskutovanější oblast z informační bezpečnosti ochrana dat v digitální formě, tedy oblast kybernetické bezpečnosti.

Česká republika je jedním z prvních civilizovaných států, který zavedl komplexní právní úpravu národní kybernetické bezpečnosti. Do roku 2014 byla problematika informační bezpečnosti implementována dle jednotlivých oblastí a tím byla roztroušena v různých zákonech. Od roku 2014 je hlavním legislativním pilířem v oblasti kybernetické bezpečnosti je Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). K tomuto zákonu se dále vážou provázející vyhlášky a nařízení vlády (Maisner, 2015). Tím však

otevírá problematika informační bezpečnosti mnoho otázek a nejaktuálnější jsou z oblasti kybernetické bezpečnosti, vlastní vymezení rozsahu a definování hranic kybernetického prostoru.

Kybernetická bezpečnost je pojem 21. století, který úzce souvisí s rozvojem informačních technologií a "internetovým" pojetím společnosti. Dle slovníku kybernetické bezpečnosti (Jirásek & Novák & Požár, 2015) pod pojmem kybernetická bezpečnost chápeme souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru. Kde kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací (Jirásek & Novák & Požár, 2015). Stejné definice a pojetí je uvedeno i v zákoně o kybernetické bezpečnosti (Zákon, 2014).

Kybernetický prostor je možno chápat jako virtuální prostor, který byl vytvořen za pomoci propojení počítačů v síti. V tomto prostoru na sebe vzájemně působí jednotlivé entity bez nutnosti fyzické interakce. Data a informace mohou být sdíleny v určitém čase nebo s případným zpožděním. Uživatelé mohou nakupovat, komunikovat, sdílet mezi sebou informace, bavit se nebo si pouze hrát. V současnosti roste význam sociálních sítí, na kterých mohou lidé spolu komunikovat, ale také se zapojovat do veřejného dění, například uveřejňováním svých politických názorů a tím ovlivňovat politické myšlení ostatních účastníků diskuse či skupiny (Hrůza, 2013).

Internet a celkově kyberprostor má také negativní dopad. Nejenže se to stal místem pro komunikaci i zábavu, ale stal se to také prostředím pro nové druhy kriminality - kybernetické kriminality. Kybernetické útoky jsou vedeny na mezinárodní i národní úrovni, jež mohou vyústit v hrozbu kyberterorismu či vzniku kybernetické války. Cílem těchto útoků se stávají vlády jednotlivých států, vládní orgány či mezinárodní společnosti. Příkladem z České republiky jsou útoky na webové stránky společností či politických stran, na vládní servery s cílem získat informace a potencionální finanční prospěch a v neposlední řadě i útoky na bezpočet privátních firem ať už s cílem finančního zisku nebo získání konkurenční výhody na společném trhu.

Spolu s rozvojem Internetu a nových technologií každoročně stoupá i počet nelegálních aktivit v kyberprostoru. V současnosti již nenalezneme organizaci, která by nedisponovala důležitými informacemi. Tyto informace se stávají stále cennějšími, a proto důležitou činností všech těchto organizací, je zajištění bezpečnosti těchto dat. S neustálým zaváděním nových informačních technologií vzrůstá i naše závislost na nich. Proto se ochrana důležitých informací stále více dostává do popředí.

POUŽITÉ METODY

Při přípravě a řešení výzkumu bylo využito několik vědeckých metod. Nejvíce využívané metody pro zpracování byly metoda analýzy a syntézy. Na základě analýzy současného stavu byl vytvořen teoretický základ pro další řešení problému. Dále byly použita metoda komparace, kterou byly porovnávány metody výuky bezpečného chování v kyberprostoru u zkoumané skupiny obyvatel.

V praktické části výzkumu byl využit deskriptivní výzkum, který zkoumal vztah studentů Univerzity obrany k informační bezpečnosti se zaměřením na aplikaci pravidel bezpečnosti v prostředí Internetu. Cílovými skupinami byli jak studenti vojenského studia, tak studenti civilního studia. Na základě údajů získaných v analýze současného stavu byl výzkum zaměřen především na výzkum rizikového chování při použití mobilních zařízení v prostředí Internetu.

Deskriptivní výzkum proběhl s pomocí dotazníkového šetření. V rámci vyučovaných předmětů z oblasti informační podpory informační bezpečnosti byly studentům v rámci cvičení předloženy dotazníky. Dotazníkové šetření není doposud ukončeno, takže jsou k dispozici pouze průběžné výsledky. Doposud získaná data z provedeného dotazníkového šetření byla hromadně a anonymně zpracována a statisticky vyhodnocena. Na základě statistického vyhodnocení dosavadních výsledků za pomoci indukce byla vytvořena obecná tvrzení o dané problematice.

RIZIKA INTERNETU

Základní cestou pro přístup do kyberprostoru je Internet. Na území České republiky byl Internet oficiálně spuštěn 13. února 1992 na pražské vysoké škole České vysoké učení technické a posléze byly k Internetu připojovány vysoké školy ve všech větších městech. Internet dnes patří k nejvýznamnějším vynálezům moderní doby. Díky Internetu lze překonávat obrovské vzdálenosti a komunikovat. Služeb Internetu využívají orgány veřejné správy a samosprávy, které jeho cestou komunikují mezi sebou a také ulehčují komunikaci veřejné správy s veřejností. Přiblížení veřejné správy občanům se děje v rámci evropských projektů zaměřených na jednotný digitální prostor a v rámci České republiky se tímto zabývají projekty E-governmentu.

Díky Internetu mohou komunikovat i lidé se svými blízkými, sdílet informace či soubory nebo se i jen bavit. Současní žáci a studenti jej využívají ke svému vzdělávání, a proto je Internet nedílnou součástí každé moderní domácnosti. Často jsou přímo na ně cíleny reklamy telekomunikačních společností, které nabízejí sdílené tarify mobilních dat, a doslova jim vnucují mobilní Internet do všech jejich zařízení. A protože je Internet součástí kyberprostoru, tak ani on nezná hranic.

Lidé ke svému životu a práci stále více potřebují moderní technologie. Dnes lze používat k výkonu zaměstnání nejrůznější modely chytrých telefonů, tabletů, netbooků, ultrabooků, chytrých hodinek nebo i chytrých brýlí. Součástí mobilních zařízení je zpravidla možnost bezdrátového připojení ke komunikační síti (Hrůza, 2013). Bohužel je to spojeno i s řadou nevýhod. Díky mobilním zařízením se uživatelé stávají stále dostupnějšími, jejich pohyb může být pomocí softwaru monitorován a tato data uchovávána. Zároveň se i zvětšuje prostor pro kybernetické zločince a jejich útoky.

Velké množství zařízení jsou nechráněna. Existují dva nejčastější důvody, proč jsou mobilní a často i pevná zařízení nechráněna:

- laxní přístup uživatelů - mnoho uživatelů nevěnuje pozornost a úsilí zabezpečit svá zařízení na patřičnou úroveň. Doby, kdy antivirus byl plně dostačující ochranou, jsou již dávno pryč. Často je možno se setkat se zařízeními připojenými k Internetu, která jsou stále v továrním nastavení. Toto nastavení je základní a výchozí pro další zabezpečení. Tím že je uživatel nechá v původním nastavení, ve kterém jsou všechna zařízení daného výrobce, jsou útočníkům známy IP adresy a administrátorská hesla pro ovládnutí těchto zařízení.
- V současnosti je třeba svá zařízení nastavit jak z pohledu administrátorského, tak z pohledu uživatelského, kde šifrovaná komunikace a bezpečné heslo jsou základem.
- softwarová omezení zařízení - některá zařízení, která jsou nyní běžně využívána, nebyla pro přímé napojení do Internetu původně vůbec navržena. Z toho vyplívá, že zařízením mohou chybět i základní prvky pro nastavení bezpečnosti zařízení. Jedná se například o mnoho zařízení, které spadají do pojmu „internet věcí“. Jsou to například na Internet napojené lednice, televizory, kamery, termostaty, zásuvky či žárovky, které je možno ovládat aplikacemi přes wi-fi připojení.
- V září 2016 byl kybernetický útok (DDOS útok) veden na uživatelský účet bezpečnostního experta. Byl to do té doby největší útok, při kterém byly prioritně použity zařízení, které spadají do kategorie internet věcí. Bylo odhadováno, že k tomuto útoku bylo ovládnuto a zneužito přes milion zařízení. A to již je taková síla, že ji většina běžných serverů neodolá, protože provoz v době útoku činil 665Gb/s (COMPUTERWORD, 2016). V říjnu 2016 byl proveden další útok stejným způsobem a byl zaměřen na servery Twittru, Spotify, Netflix, PayPal, SoundCloud a další velké on-line služby.

Takto nezabezpečená zařízení mohou sloužit jako vstupní brána pro kybernetický útok. Uživatelé uchovávají v mobilních zařízeních velmi citlivá data, jakož jsou telefonní kontakty, adresy, e-mailové adresy, která mohou být v mžiku ukradena a zneužita například pro obchodní účely.

Škodlivý software však může proniknout i do plně zabezpečeného mobilního zařízení prostřednictvím stahování aplikací. Proto je nutné vždy zvážit, z jakého zdroje je instalovaná aplikace získána. Někdy nejsou bezpečné ani stránky poskytovatele služeb jako je Google Play či App Stor. Již několikrát se stalo, že škodlivý malware byl součástí oficiální aplikace, která byla provozovatelem prověřena.

Při ochraně mobilních zařízení je třeba kromě instalace ochranných softwarů a nastavení operačního systému, dodržovat bezpečnostní politiku. Je nutné dbát na ochranu osobních údajů, připojovat svá zařízení do zabezpečených sítí a v neposlední řadě nesdělovat nikomu hesla ke svým účtům.

REALIZOVANÉ VZDĚLÁVACÍ AKCE KYBERNETICKÉ BEZPEČNOSTI

Lidé se často registrují na sociálních sítích pro uspokojení touhy komunikovat s ostatními, poznávat nové lidi, bavit se, ale také z touhy být začleněn do kolektivu a nebýt ochuzen o informace. Tento trend se promítá i do škol, kde většina školních zařízení, kroužků či sdružení také využívat sociální sítě, a tím se snaží více přibližovat žákům. Bohužel sociální sítě jsou také místo, ve kterém může uživatelům hrozit velké nebezpečí.

Nebezpečí se ukrývá v neznámých lidech, se kterými dětmi komunikují. Mnoho uživatelů je ochotno sdílet informaci o své osobě, uveřejňovat své fotografie či fotografie rodiny. Nepřipouští si ale fakt, že tyto informace mohou být zneužity.

Právě na Internetu je možno nalézt spoustu informací a rad jak se na Internetu chovat, jak rozpoznat útok a jak se bránit případným útočníkům. Jedním z nich je i televizí vysílaný osvětový projekt sdružení CZ.NIC „Jak na Internet“. Tento projekt formou zábavných, dvouminutových videí, přibližuje širokou problematiku Internetu. Ke každému videu je uveden doprovodný text, který se dané problematice věnuje více do hloubky.

Také Česká pobočky AFCEA již od roku 2004 vyvíjí řadu osvětových, vzdělávacích a odborných aktivit v oblasti kybernetické bezpečnosti. Pravidelně organizuje bezpečnostní semináře pro státní zaměstnance, akademické, zejména vysokoškolské, pracovníky a odborníky z privátní sféry. Pro studenty středních škol organizuje již druhý ročník české celorepublikové soutěže v kybernetické bezpečnosti.

Dále existuje celá řada projektů, které poskytují informace k informační a kybernetické bezpečnosti. Příkladem jsou: Seznam se bezpečně, Bezpečný internet.cz, Safer internet.cz, E-Bezpečí, bezpečně-online.cz a mnoho dalších.

V říjnu 2017 proběhne již pátý ročník celoevropské kampaně s názvem Evropský měsíc kybernetické bezpečnosti (ECSM/European Cyber Security Month). ECSM je celoevropská kampaň, probíhá každoročně v měsíci říjnu a je koordinovaná Evropskou agenturou pro síťovou a informační bezpečnost. ECSM je informační kampaň o kybernetické bezpečnosti zaměřená na občany. Cílem je vyvolat změnu ve vnímání kybernetických hrozeb udílením vyšší pozornosti bezpečnosti dat a informací, vzdělávání a sdílení osvědčených postupů.

Z uvedeného výčtu je zřejmé, že běžným uživatelům je poskytováno velké množství informací, jak se mají na Internetu chovat, jakou mají použít prevenci před kyberútoky, jak kyberútok rozeznat a jak se proti němu chránit. Mnoho uživatelů ale o této možnosti získání informací neví, ne proto, že by je nenašly, ale proto, že je nikdy nehledaly. A dokud se samy nestanou obětmi kybernetického útoku, je velmi malá pravděpodobnost, že by si informace o kybernetické bezpečnosti sami dohledali.

ZÁVĚR

Přetrvávajícím fenoménem Internetu jsou sociální sítě. Bez nich si mladá generace nedokáže představit komunikaci s přáteli či sdílení informací. Stále mladší děti touží po chytrých telefonech a vytvoření profilového účtu na některé ze sociálních sítí, aby mohly být v kontaktu s přáteli a rodinou. Než se tak stane, měli by být seznámeni s možnými riziky Internetu (kyberprostoru) a jak se proti těmto rizikům bránit.

Zásadní otázkou zůstává, kdo je bude před těmito riziky varovat. Vždyť často ani rodiče nevědí, jaká rizika jim při pohybu v Internetu hrozí a jak se proti nim chránit. A při tom první mobilní telefon děti dostávají již na základní škole, ne-li přímo ve školce. Ochrana před kybernetickými útoky by měla probíhat na mezinárodní úrovni, protože kyberprostor nemá hranice. Základní informace a pravidla ohledně kybernetické bezpečnosti by měly děti dostávat již od prvních tříd základní školy, protože tím jak některé základní školy zavedly výuku pomocí tabletů a mobilních zařízení, otevřely přístupovou bránu kyberzločincům do soukromého prostoru vyučovaných dětí.

LITERATURA

COMPUTERWORLD. 2016. Největší DDoS útok v historii, internet věcí útočí. *ComputerWorld: Security World* [online]. [cit. 2017-04-01]. Dostupné z: http://computerworld.cz/securityworld/nejvetsi-ddos-utok-v-historii-internet-veci-utoci-53336

Česko. 2014. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). 2014. In: Sbírka zákonů ČR, ročník 2014, částka 75, číslo 181.

HROMADA, Martin; HRŮZA, Petr; KADERKA, Josef; LUŇÁČEK, Oldřich; NEČAS, Miroslav; PTÁČEK, Bohumil; SKORUŠA, Leopold; SLOŽIL, Richard. 2015. *Kybernetická bezpečnost: teorie a praxe.* Praha: Powerprint s.r.o., 250 s. ISBN 978-80-87994-72-6.

HRŮZA, Petr. 2013. *Kybernetická bezpečnost II.* Vyd. 1. Brno: Univerzita obrany, 100 s. ISBN 978-80-7231-931-2.

HRŮZA, Petr; HROMADA, Martin; KADERKA, Josef; JIRSA, Milan; SLOŽIL, Richard; SKORUŠA, Leopold; PTÁČEK, Bohumil; NEČAS, Miroslav. 2017. *Návrh postupů pro odhalení, monitorování, odražení, vyhodnocování a dokumentaci jednotlivých forem útoků a jejich cílů z hlediska destabilizace kritické informační infrastruktury České republiky.* Metodika.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN isbn978-80-7251-436-6.

JIROVSKÝ, Václav. 2007. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 284 s. ISBN 978-80-247-1561-2.

MAISNER, Martin. 2015. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

NÁPLAVOVÁ, Magdalena. 2014. *Pojetí bezpečnosti v kyberprostoru na základních a středních školách.* Diplomová práce. Brno: Univerzita obrany. 64 s.

PROHÁZKOVÁ, D. a kol. 2006. *Bezpečnost a krizové řízení*. 1. vyd. Praha: Police history. 255 p. ISBN 80-86477-35-5.

ADRESA

Jiří BARTA, Michaela VAŠKOVÁ, Petra BEŇOVÁ
Katedra krizového řízení
Fakulta vojenského leadershipu
Univerzita obrany v Brně
Kounicova 65, 662 10 Brno
jiri.barta@unob.cz

VYBRANÉ TEORETICKÉ A APLIKAČNÉ VÝZVY KREOVANIA VZŤAHU KYBERNETICKEJ BEZPEČNOSTI A KRÍZOVÉHO MANAŽMENTU

SELECTED THEORETICAL AND APPLICATIONAL CHALLENGES OF CREATING A RELATIONSHIP BETWEEN CYBER SECURITY AND CRISIS MANAGEMENT

Miroslav BRVNIŠŤAN

Akadémia Policajného zboru v Bratislave

Abstrakt : *Kybernetická bezpečnosť ako relatívne nový bezpečnostný fenomén vytvára tlak na zmeny v zaužívanom vnímaní bezpečnostného systému a možností systému krízového riadenia. Je zrejmé, že nastáva nová éra, ktorá ovplyvní celkové vnímanie bezpečnosti. Formujúca sa oblasť kybernetickej bezpečnosti nesporne ovplyvní zaužívané mechanizmy, nástroje, metódy a formy krízového manažmentu. Vzájomný vzťah týchto oblastí bude určujúcim aj pre definovanie primeraného vzťahu k súkromnému sektoru, ktorý bude zohrávať nezastupiteľnú rolu.*

Kľúčové slová: *Bezpečnostný systém, krízový manažment, kybernetická bezpečnosť, asymetrické hrozby*

Abstract: *Cyber security as a relatively new security phenomenon puts pressure on changes in the used perception of the security system and the possibilities of the crisis management system. It is clear that a new era is occurring and that affects the overall perception of security. The shaping area of cyber security will undoubtedly influence the mechanisms, tools, methods and forms of crisis management. The interrelationship of these areas will also be crucial for defining a sound relationship with the private sector, which will play an irreplaceable role.*

Keywords: *Security system, crisis management, cyber security, asymmetric threats*

Dynamické zmeny bezpečnostného prostredia, kladú v kontexte zabezpečovania kontinuity základných činností štátu čoraz väčšie nároky na bezpečnosť a bezpečnostný systém štátu. Bezpečnosť štátu tak ako sme ju vnímali v uplynulých desaťročiach sa postupne mení. Vývoj bezpečnostného prostredia je ovplyvňovaný predovšetkým nárastom ekonomickej, sociálnej, technologickej a environmentálnej prepojenosti sveta, ako aj rastúcou komplexnosťou medzinárodnej bezpečnostnej architektúry.

Súčasné krízy, ktorých sme svedkami, majú základy v dynamicky sa meniacej medzinárodnej bezpečnostnej situácii - asymetrické vojny, hybridné ohrozenia, terorizmus, organizovaný zločin, kybernetické útoky, ale aj nárast nacionalistických a náboženských konfliktov, nezamestnanosť, priemyselné havárie, požiare, ekologické katastrofy a povodne. Mení sa spôsob akým štát dokáže reagovať. Relatívne statický bezpečnostný systém je pod tlakom nových faktorov a nie je pripravený primerane reagovať. Oblasť kybernetickej bezpečnosti je dobrým príkladom kedy nové hrozby a riziká vytvárajú dostatočný tlak na realizáciu zmien, no vznikajúce požiadavky na bezpečnostný systém a ich realizácia zaostávajú.

Systém krízového riadenia SR a typické krízové situácie, ktoré boli základom pre jeho konštituovanie, historicky vychádzali zo samozrejmosti materiálnej a fyzickej podstaty bezpečnostného prostredia a relatívne nízkej dynamiky. Nové bezpečnostné hrozby a možné krízové situácie vytvárajú predpoklady na prehodnotenie a re-definovanie charakteristických metód, foriem, prostriedkov a krízových scenárov systému krízového riadenia.

Zatiaľ čo samotná informatizácia spoločnosti, zavádzanie nových, pokročilých technológii znamená zefektívňovanie a zrýchľovanie procesov, ekonomické aspekty týchto procesov a tlak na znižovanie nákladov ovplyvňujú realizáciu primeraných bezpečnostných opatrení. Práve bezpečnosť v kontexte "novej éry" zohráva a bude zohrávať čoraz dôležitejšiu rolu pri formovaní oblasti kybernetickej bezpečnosti. V tomto ohľade je možné kybernetickú bezpečnosť považovať za

dôsledok rozvoja informatizácie spoločnosti. Aké to však má konzekvencie a aký je vlastne vzťah medzi informačnou a kybernetickou bezpečnosťou?

Relatívna neznalosť možných dopadov a väzieb oblasti kybernetickej bezpečnosti na bezpečnostný systém štátu a systém jeho krízového riadenia vytvárajú potrebu komplexnej analýzy. Situáciu zvýrazňuje aj chýbajúci teoretický aparát a metodológia, vrátane vedeckého pohľadu na túto oblasť.

Čo je to vlastne kybernetická bezpečnosť a ako môže ovplyvniť krízový manažment štátu? Odpoveď na takto položené otázky nie je v súčasnosti jednoznačná. Prebiehajúce procesy však naznačujú, že tento vzťah môže byť určujúcim pre budúcnosť budovania bezpečnosti a bezpečnostného systému SR.

Cieľom príspevku je prostredníctvom všeobecnej analýzy vznikajúceho vzťahu krízového manažmentu a formujúcej sa oblasti kybernetickej bezpečnosti poukázať na viaceré okolnosti, ktoré budú určujúce pre ich budúci vývoj.

I. KRÍZOVÝ MANAŽMENT A INFORMAČNÁ BEZPEČNOSŤ

Rozvoj oblasti informačnej bezpečnosti a dôsledky informatizácie spoločnosti sú nesporné. Informačná bezpečnosť je plne integrovaná do bezpečnostného systému štátu, systému riadenia. Existuje celý spektrum predpisov, bezpečnostných politík, pravidiel, štandardov a noriem[1], ktoré definujú požiadavky na bezpečnosť informačných systémov, ktoré zabezpečujú relatívne jednotné a centrálne metodické riadenie informačnej bezpečnosti.

Správa o bezpečnosti SR za rok 2015 poukazuje na niektoré realizované opatrenia v oblasti bezpečnosti štátu, partikulárne aj oblasti krízového riadenia[2]. Na základe hodnotení hrozieb a faktorov ovplyvňujúcich bezpečnosť SR, prijímaných opatrení a v nadväznosti na predpokladané trendy vývoja bezpečnostnej situácie boli v správe hodnotené viaceré opatrenia a úlohy. Tieto poukazujú na systematiku prístupu k otázkam bezpečnosti, respektíve odhaľujú niektoré nedostatky.

Jednou z úloh (úloha č.1 správy) bola úloha pre ústredné orgány štátnej správy vypracovať scenáre možného vývoja bezpečnostných hrozieb s reálnou pravdepodobnosťou ich výskytu a opatrenia na predchádzanie krízovým situáciám a na riešenie vzniknutých krízových situácií formou situačných plánov. V hodnotení plnenia úlohy sa uvádza, že ústredné orgány štátnej správy vychádzali pri plnení opatrenia z analýzy možného vývoja bezpečnostných hrozieb (aj kybernetických?), v rámci ktorej boli identifikované možné scenáre pre jednotlivé hrozby s vyhodnotením ich významnosti. V súlade so všeobecne záväznými právnymi predpismi a v rámci kompetencií jednotlivých rezortov boli vypracované dokumenty, ktorých súčasťou sú situačné plány a plány na zabezpečenie kontinuity činnosti. Z hodnotenia úlohy je zrejmé, že jej plnenie ešte nezohľadňovalo oblasť kybernetickej bezpečnosti, nakoľko táto sa ešte len kreuje. Naopak, dalo by sa očakávať, že v prípade vykonanej serióznej analýzy rizík boli všetky aktuálne riziká pokryté, a teda že tieto zahŕňajú aj riziká, ktoré budú spadať do oblasti kybernetickej bezpečnosti.

Druhá úloha (úloha č.3 správy) bola prijatá za účelom realizovať zhodnotenie systému ochrany prvkov kritickej infraštruktúry v sieťach elektronických komunikácií podľa platných štandardov ISO. Ako je v správe uvedené, opatrenie sa plnilo v spolupráci so všetkými operátormi elektronických komunikačných služieb, ktorí vlastnia prvky kritickej infraštruktúry, pričom sa potvrdilo, že operátori elektronických komunikačných služieb vykonávajú široké spektrum aktivít a investujú do zlepšovania systému riadenia bezpečnosti informácií a zvyšovania úrovne bezpečnosti. Potvrdilo sa, že implementované bezpečnostné procesy a procedúry spĺňajú náročné požiadavky certifikátcie podľa ISO/IEC 27001:2013, čím sa v oblasti zabezpečenia kontinuity

[1] Napr. rada noriem pre oblasť informačnej bezpečnosti ISO/IEC 27000, Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Európskej únii zo 6. júla 2016.
[2] Správa o stave bezpečnosti SR za rok 2015.

riadenia činností potvrdila pripravenosť na zvládanie krízových situácií a zabezpečenia kontinuity poskytovania svojich kľúčových služieb počas krízových situácií.

Z takto vyhodnotenej úlohy je možné logicky konštatovať, že informačná bezpečnosť a systém existujúcich noriem je v zásade postačujúci na ochranu prvkov kritickej infraštruktúry aj pred novými bezpečnostnými hrozbami.

Čo bude teda úlohou formujúcej sa oblasti kybernetickej bezpečnosti nie je možné odvodiť.

Zákon o ochrane kritickej infraštruktúry č. 45/2011 Z.z.[3] určuje pôsobnosť orgánov štátnej správy na úseku ochrany kritickej infraštruktúry, spôsob určovania jej prvkov a povinnosti pri ich ochrane. Pod ochranou sa stanovuje (§2 písm.i) *zabezpečenie funkčnosti, integrity a kontinuity činnosti prvku s cieľom predísť, odvrátiť alebo zmierniť hrozbu jeho narušenia alebo zrušenia.* Obsahuje rámcový postup určenia prvku kritickej infraštruktúry na základe splnenia tzv. sektorových kritérií.

Vznik samotného zákona a jeho štruktúry vychádza zo širších aspektov súvisiacich so zámerom riešenia problematiky kritickej infraštruktúry na pôde EÚ. Iniciátorom bola Európska komisia, ktorá dňa 17. 11. 2005 predložila tzv. „*Zelenú knihu o Európskom programe pre ochranu kritickej infraštruktúry*“. V dôsledku tohto dokumentu boli prijaté viaceré dokumenty a spracovaný postup realizácie ochrany kritickej infraštruktúry v členských krajinách a teda aj v SR. V rámci EÚ je kritická infraštruktúra definovaná v Smernici Rady o určovaní a označovaní európskej kritickej infraštruktúry[4], kde je pre účely tejto smernice kritická infraštruktúra definovaná ako : *„zložka, systém alebo ich časť nachádzajúca sa v členských štátoch, ktorá je nevyhnutná pre zachovanie základných funkcií spoločnosti, zdravia, ochrany, bezpečnosti, kvality života obyvateľov z ekonomického a sociálneho hľadiska, a ktorej narušenie alebo zničenie by malo závažné dôsledky v členskom štáte z dôvodu nemožnosti zachovať tieto funkcie”*.

Z uvedeného procesu (časové hľadisko) vyplýva, že tendencia chrániť kritickú infraštruktúru existovala už dlhodobo, čo sa reaálne prejavilo v postupnom prijímaní riadiacich a strategických dokumentov na úrovni EÚ. Realizačný dokument na úrovni EÚ - Smernica Rady č. 2008/114/EC tento proces začala, na základe čoho bol aj prijatý zákon č. 45/2001 Z.z. Z podstaty procesov EÚ je zrejmé, že SR sa procesu prípravy dokumentov na úrovni EÚ zúčastňovala. Napriek tomu prijatie zákona trvalo takmer 3 roky. Uvedené poukazuje na skutočnosť ako dlho, napriek jednoznačnosti procesov trvalo prijatie v zásade jednoduchej ale kľúčovej právnej normy. Cieľom však nie je kritika, len zovšeobecnené poznanie o zbytočnej časovej zdľhavosti riadiacich procesov v oblasti bezpečnosti.

V tejto súvislosti je potrebné poukázať na niekoľko významných skutočností. Po prvé, zákon č. 45/2001 Z.z. v prílohe definuje tzv. sektory v pôsobnosti ústredných orgánov štátnej správy. V týchto sú zaradené aj elektronické komunikácie - s*atelitná komunikácia a siete a služby pevných a mobilných elektronických komunikácií, vrátane sektora informačných a komunikačných technológii - informačné systémy a siete a internet.* Po druhé, zákon vytvára podmienky na využívanie výstražnej informačnej siete kritickej infraštruktúry - Critical Infrastructure Warning Information Network -CIWIN. Táto sieť by mala umožniť koordináciu a spoluprácu pri výmene informácií týkajúcich sa postupov pri ochrane európskej kritickej infraštruktúry, najmä zaistiť bezpečnú a štruktúrovanú výmenu informácií. Tieto informácie by mali užívateľom CIWIN umožniť aby rýchlo a účinne poznali osvedčené postupy v ostatných ČK a týmto štátom umožniť využívať systém včasného varovania - CIP (Critical Infrastructure Protection). Po tretie, zdieľanie informácií o európskej kritickej infraštruktúre by sa malo uskutočňovať v atmosfére

[3] Zákon NR SR č. 45/2011 Z.z. o kritickej infraštruktúre.

[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

dôvery a istoty. Zdieľanie informácií si vyžaduje vzťah založený na dôvere, aby podniky a organizácie vedeli, že ich citlivé a dôverné údaje sú dostatočne chránené[5].

Uvedené skutočnosti poukazujú na stav, kedy už prostredníctvom zákona o kritickej infraštruktúre boli vytvorené podmienky na komplexnú ochranu informačnej infraštruktúry….

Uvedené logicky znamená, že zámer a reálne nástroje ochrany informačnej a komunikačnej infraštruktúry existujú a sú zavedené v praxi. Proces ochrany a bezpečnosti je v zásade plnohodnotne nastavený, začínajúc analýzou rizík až po havarijné a bezpečnostné plány ochrany, vrátane informačných systémov na výmeny citlivých informácií o ich fungovaní, aktuálnom stave a rizikách. Vzťah krízového manažmentu a informačnej bezpečnosti možno vzhľadom na uvedené informácie charakterizovať ako vyvážený. Znamená to, že krízový manažment a pripravené krízové scenáre počítajú s narušením kritickej informačnej infraštruktúry a teda bezpečnostný systém štátu by mal byť pripravený.

Opätovne sa natíska otázka aká teda bude pridaná hodnota oblasti kybernetickej bezpečnosti v bezpečnostnom systéme?

II. KRÍZOVÝ MANAŽMENT A KYBERNETICKÁ BEZPEČNOSŤ

Krízový manažment je možné považovať za etablovaný a prepracovaný nástroj štátu na riešenie krízových situácií. Typické krízové situácie, ktoré boli základom pre jeho konštituovanie vychádzali z materiálnej a fyzickej podstaty bezpečnostného prostredia.

Moderné bezpečnostné hrozby a krízové situácie vytvárajú nesporne tlak na prehodnotenie a re-definovanie charakteristických metód, foriem a prostriedkov krízového manažmentu. Ako bolo konštatované v predchádzajúcej časti, neberúc v úvahu časové hľadisko, podarilo sa informačnú bezpečnosť a ochranu informačnej infraštruktúry inkorporovať do systému krízového manažmentu. Naďalej je však potrebné sa zaoberať možnými dôsledkami vývoja a jeho potencionálneho vplyvu na možnosti rozvoja krízového manažmentu, vrátane jeho využitia pri riešení principiálne nových krízových situácií - kybernetických.

V zásade však platí, že úroveň krízového manažmentu dosiahla relatívne primeranú úroveň z hľadiska ekonomických možností, poznania a riadenia štandardných krízových situácií. SR je v oblasti krízového manažmentu zapojená do medzinárodných štruktúr krízového manažmentu a spolupracuje v rámci nadnárodných integračných zoskupení. Na rozvoj krízového manažmentu mala vplyv aj integrácia SR do nadnárodných integračných zoskupení ako Európska únia a Severoatlantická aliancia. Ako sa však vysporiada oblasť krízového manažmentu v prípadoch krízových situácií zapríčinených modernými hrozbami[6], za aké je možné považovať napr. kybernetický útok, prípadne iné riziká vyplývajúce z kybernetického prostredia. Kybernetický útok a jeho dôsledky môžu predsa spôsobiť obdobné ale aj oveľa závažnejšie dôsledky s ohľadom na ekonomické, materiálne, finančné alebo ľudské zdroje ako štandardné ozbrojené útoky a z nich vyplývajúce krízové situácie.

Je vôbec možné kybernetický útok považovať za "nový" typ krízovej situácie, alebo "len" za dôvody smerujúce k vzniku "štandardnej" krízovej situácie v oblasti informačnej bezpečnosti?

Aká by mala byť rola systému krízového manažmentu štátu?

Oblasť kybernetickej bezpečnosti ako téma, ktorej sa v súčasnosti venuje čoraz viac pozornosti, rezonuje v bezpečnostných, ako aj v odborných kruhoch relatívne dlho (približne 15 rokov). Zvýšenú pozornosť odzrkadľuje najmä stav, kedy moderná spoločnosť je čoraz viac závislá na informačných a komunikačných technológiách, ktoré ovplyvňujú všetky aspekty jej života. Vo svojej podstate sme svedkami presunu podstatnej časti aktivít ľudstva z materiálneho sveta do sveta

[5] V prípade zdieľania informácii o poškodení alebo napadnutí kritickej infraštruktúry a úniku takýchto informácií by v prípade ich úniku mohlo spôsobiť ekonomické škody alebo poškodenie dobrého mena (napr. banky v prípadoch útokov na jej informačné systémy). Dôvera v bezpečnosť takýchto systémov je dôležitá.

[6] Za takéto je vo všeobecnosti možné považovať napr. všetky formy kybernetickej kriminality, tiež asymetrické hrozby, hybridné hrozby, informačnú vojnu - pozn. autora.

kybernetického. Samozrejmosť fungovania kybernetického sveta sa javí čoraz viac dôležitejšou pre plnenie úloh štátu a spoločnosti. Vzniká závislosť, ktorá zásadným spôsobom ovplyvňuje pohľad na bezpečnosť.

Ako vôbec vznikla téma "kybernetická bezpečnosť? Existuje na to viacero názorov, ktoré sú spravidla založené na poznaní vývoja jednotlivých oblastí bezpečnosti informácií a s nimi spojených typických pojmov. Medzi takéto je možné zaradiť pojmy ako napr. počítačová bezpečnosť, informačná bezpečnosť, bezpečnosť informačných a komunikačných systémov, bezpečnosť internetu a INFOSEC[7]. Nesporne už s týmito pojmami a súvisiacimi oblasťami sa bezpečnostný systém štátu musel vysporiadať. Je takisto zrejmé, že určité komplikácie pri hľadaní súvislosti medzi kybernetickou bezpečnosťou a oblasťou krízového manažmentu môžu nastať už na úrovni pojmov a pokusov dorozumieť sa, vrátane aplikácie týchto pojmov v jednotlivých oblastiach spoločenských vzťahov[8].

Kybernetická bezpečnosť však prinajmenšom vyjadruje niečo nové a najmä umožňuje nový komplexnejší pohľad. Azda najjednoduchšie a najvýstižnejšie ju charakterizuje to, že funguje vo virtuálnej rovine, ktorú nedokážeme vidieť ani uchopiť. Má globálny rozmer, ktorý stiera hranice medzi štátmi a funguje bez ohľadu na politický systém, s mimoriadne širokou paletou aktérov od jednotlivcov, cez rôzne nadnárodné zoskupenia až po štáty. Znamená to, že ak doteraz bola napr. oblasť bezpečnosti informačných a komunikačných systémov chápaná ako oblasť, ktorú bolo možné riešiť na úrovni menších celkov (organizácia, štát) a pravidlá boli jednoducho vynútiteľné, tak s pojmom kybernetická bezpečnosť sú spájané skôr nadnárodné celky a zoskupenia, pričom spôsob vynucovania pravidiel prostredníctvom práva (kreovanie spoločných) je oveľa komplikovanejší. Postavenie jednotlivca a rôznych neštandardných zoskupení osôb sa takisto zásadným spôsobom zmenilo, stávajú sa rovnocennými aktérmi spôsobilými pôsobiť v kybernetickom priestore minimálne rovnako efektívne ako štáty.

Samotná podstata kybernetickej bezpečnosti je založená na prepojenosti informačných a komunikačných systémov, globálnosti a relatívnej rýchlosti toku informácií. Do úvahy je potrebné brať množstvo nových, ešte riadne neidentifikovaných faktorov, ktoré snáď poznáme z materiálneho sveta, no v kybernetickom svete predstavujú úplne nové javy. Hranice štátov, neustály technologický pokrok, masovosť a nové možnosti jednotlivcov ovplyvňovať a škodiť, ale aj pomáhať vytvárajú enormný tlak na tvorbu nových pravidiel a bezpečnostných mechanizmov. Existuje viacero návrhov pojmov pre oblasť kybernetickej bezpečnosti, vyskytujúcich sa v rôznych, spravidla strategických materiáloch NATO a EÚ, ale aj SR. My sa stotožňujeme s pojmom, ktorý je súčasťou slovníka kybernetickej bezpečnosti spracovaného v Českej Republike a využívaného v rámci NATO a EÚ bezpečnostných štruktúr.

Kybernetická bezpečnosť, podľa tohto slovníka, predstavuje *súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu ochrany kybernetického priestoru*[9]. Z takto postavenej definície je zrejmé, že ide o komplex aktivít a krokov, ktoré by mali byť pri zaisťovaní kybernetickej bezpečnosti vykonané, vrátane reakcií štátu na kybernetický útok, resp. jeho dôsledky. Ide o komplexnú výzvu pre bezpečnostný manažment štátu.

Rozvoj oblasti kybernetickej bezpečnosti (obdobie približne 9 rokov!) SR je komplikovaný a možno konštatovať, že napriek viacerým schváleným strategickým dokumentom sa oblasť kybernetickej bezpečnosti nedostala do primeranej pozornosti politikov a kompetentných ústavných činiteľov. Napriek tomu sa niektoré i keď často nesystémové kroky uskutočnili. Hrozby vyplývajúce z informatizácie spoločnosti boli zadefinované už ako súčasť Bezpečnostnej stratégie

[7] Pozri aj OLEJÁR, D.: Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. 164 s. (online). Dostupné na internete: http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s.

[8] Napr. oblasť trestného práva pracuje s pojmami ako počítačová kriminalita, počítačový systém, pozri bližšie zákon č. 300/2005 Z.z trestný zákon.

[9] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti, Policejní Akademie České republiky v Praze, Česká pobočka AFCEA, Praha 2014, s. 57.

SR[10] a Slovenská republika ako prvá členská krajina NATO podpísala v roku 2008 Memorandum o spolupráci medzi Národným bezpečnostným úradom (ďalej len NBÚ) a NATO Cyber Defence Management Authority v oblasti ochrany kybernetického priestoru. V rámci tejto spolupráce boli vytipované viaceré oblasti - napr. pomoc pri vzdelávaní, výmena informácií o zraniteľnosti systémov, technická podpora. V tomto období však ešte nebolo zrejmé, kto (ktorý orgán verejnej moci) a ako bude zodpovedať za oblasť kybernetickej bezpečnosti. Existovali minimálne dva subjekty, a to Ministerstvo financií SR a NBÚ, ktorí deklarovali záujem a vykonali "úvodné" kroky. V rámci Ministerstva financií SR boli pripravené a schválené vládou SR viaceré strategické dokumenty napr. Stratégia pre informačnú bezpečnosť v SR alebo Legislatívny zámer zákona o informačnej bezpečnosti[11]. V tomto čase NBÚ okrem už spomínanej spolupráce s NATO deklaroval záujem o zastrešenie oblasti kybernetickej bezpečnosti. Pri hľadaní riešenia (vzájomné kompetenčné spory) dochádzalo k niektorým absurditám v dôsledku ktorých sa napr. delil virtuálny priestor na kybernetický (v kompetencii NBÚ) a digitálny (v kompetencii MF SR). Výsledkom bol patový stav, ktorý sa podarilo vyriešiť (po 7 rokoch) presunutím kompetencií v oblasti kybernetickej bezpečnosti na NBÚ v roku 2015. Následne boli prijaté boli viaceré dokumenty rámcovo určujúce ďalší rozvoj oblasti kybernetickej bezpečnosti. Koncepcia kybernetickej bezpečnosti SR na roky 2015-2020 a Akčný plán realizácie Koncepcie kybernetickej bezpečnosti SR na roky 2015-2020[12]. V súčasnosti sa pripravuje, ako už bolo uvedené, zákon o kybernetickej bezpečnosti, ktorý mal byť predložený na rokovanie vlády SR začiatkom roka 2017.

Už z uvedeného je možné konštatovať, že v súčasnosti nie je možné predvídať ako sa bude oblasť kybernetickej bezpečnosti rozvíjať, i keď niektoré kroky a už stanovené rámcové úlohy napovedajú, ktorým smerom sa bude oblasť uberať, resp. čoho sa budú zmeny týkať. Za najdôležitejšie bude potrebné doriešiť zosúladenie systémových požiadaviek tak, aby bolo možné zabezpečiť primeranú kompatibilitu v rámci NATO a EÚ. Kľúčovým bude integrovanie funkcionalít systému kybernetickej bezpečnosti do súčasného bezpečnostného systému štátu, vrátane systému krízového riadenia.

To akú rolu bude zohrávať oblasť kybernetickej bezpečnosti napovedá aj Stratégia kybernetickej bezpečnosti EÚ[13]. Úvodné ustanovenia jasne deklarujú čo sa očakáva: *"Počas posledných dvoch desaťročí internet a v širšom meradle kybernetický priestor nesmierne ovplyvnil všetky vrstvy spoločnosti. Náš každodenný život, základné práva, sociálna interakcia a hospodárstvo závisia od bezproblémového fungovania informačných a komunikačných technológií. Otvorený a slobodný kybernetický priestor podporil politické a sociálne začlenenie v celosvetovom meradle; odstránil prekážky medzi krajinami, komunitami a občanmi a umožnil globálnu interakciu a výmenu informácií; poskytol fórum na slobodu prejavu a výkon základných práv a dal ľuďom možnosť dôraznejšie sa dožadovať demokratickej a spravodlivejšej spoločnosti - čo sa najvýraznejšie prejavilo počas Arabskej jari.*

[10] Bod. č. 23 Bezpečnostnej stratégie SR : Miera informatizácie spoločnosti dosiahla vysoký stupeň a stále sa zvyšuje. Výkonnosť techniky, revolučné informačné a komunikačné technológie, nárast rýchlosti prenosu informácií a ich globálnej dostupnosti spôsobujú rýchlu globálnu premenu postindustriálnej spoločnosti na spoločnosť informačnú. Zraniteľnosť informačných a komunikačných systémov, ich preťaženie, neoprávnený prístup k informáciám, šírenie počítačových vírusov a dezinformácií sú rastúcou hrozbou pre SR. Bezpečnostná stratégia SR, schválená NR SR 27.9.2005.

[11] Národná stratégia pre informačnú bezpečnosť, Vláda Slovenskej republiky materiál schválila 27. augusta 2008 uznesením č.570/2008. Stratégia pre informačnú bezpečnosť v Slovenskej republike, schválená uznesením vlády SR č. 270/2008. Legislatívny zámer zákona o informačnej bezpečnosti, schválený uznesením vlády SR č. 136/2010.

[12]Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020, schválená uznesením vlády SR č. 328 zo 17.6.2015 Akčný plán realizácie Koncepcie kybernetickej bezpečnosti na roky 2015 - 2016, schválený uznesením vlády SR č. 93 z 2.3.2016.

[13] SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor, Brusel 7. 2. 2013 JOIN(2013) 1 final.

Aby kybernetický priestor zostal otvorený a slobodný, rovnaké normy, zásady a hodnoty, aké EÚ podporuje mimo internetu, by sa mali uplatňovať aj na internete. V kybernetickom priestore treba chrániť základné práva, demokraciu a zákonnosť. Naša sloboda a prosperita v čoraz väčšej miere závisia od spoľahlivého a inovačného internetu, ktorý sa bude naďalej rozvíjať, ak inovácie súkromného sektora a občianska spoločnosť podporia jeho rast. Ale aj online sloboda vyžaduje bezpečnosť a ochranu. Kybernetický priestor by mal byť chránený pred incidentmi, škodlivými činnosťami a zneužívaním; a vlády plnia významnú úlohu pri zabezpečovaní slobodného a bezpečného kybernetického priestoru".

Vlády majú niekoľko úloh: zabezpečiť prístup a otvorenosť, rešpektovať a chrániť základné práva online a udržiavať spoľahlivosť a interoperabilitu internetu. Významný podiel kybernetického priestoru však vlastní a prevádzkuje súkromný sektor, a preto všetky iniciatívy, ktoré chcú byť v tejto oblasti úspešné, musia uznávať jeho vedúcu úlohu.

Informačné a komunikačné technológie sa stali hlavnou oporou nášho hospodárskeho rastu a rozhodujúcim zdrojom, o ktorý sa opierajú všetky sektory hospodárstva. Sú základom komplexných systémov, ktoré udržiavajú naše hospodárstva v chode v kľúčových sektoroch, ako sú financie, zdravotníctvo, energetika a doprava".

Z uvedenej krátkej analýzy vyplýva viacero zásadných skutočností : Kybernetický priestor je niečo viac ako "len" internet. Ide najmä o prijatie pravidiel, nástrojov a procesov aby tento ostal otvorený a slobodný, aplikovali sa rovnaké normy, zásady a hodnoty, aké EÚ podporuje mimo internetu. Zároveň ide o ochranu základných práv, demokracie a zákonnosti. Dôležitým aspektom je aby vlády uznali vedúcu úlohu súkromného sektora (podľa rôznych zdrojov až 90% informačnej infraštruktúry vlastní súkromný sektor).

Dôležitým pre pochopenie budúceho vzťahu kybernetickej bezpečnosti a krízového manažmentu bude aproximácia smernice EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 2016/1148 zo 6. júla 2016[14] o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

Smernica bude aj základom pripravovaného zákona o kybernetickej bezpečnosti SR. V zásade sa stanovia spoločné minimálne požiadavky na bezpečnosť sietí a informácií na vnútroštátnej úrovni, ktoré by od členských štátov vyžadovali, aby: určili príslušné vnútroštátne orgány pre bezpečnosť sietí a informácií; vytvorili riadne fungujúci tím CERT; a prijali vnútroštátnu stratégiu bezpečnosti sietí a informácií a národný plán spolupráce v oblasti bezpečnosti sietí a informácií. Budovanie kapacít a koordinácia sa týkajú aj inštitúcií EÚ: Tím reakcie na núdzové počítačové situácie zodpovedný za bezpečnosť IT systémov inštitúcií, agentúr a orgánov EÚ („CERT-EU") bol permanentne zriadený v roku 2012. Bude potrebné zaviesť koordinované mechanizmy v rámci prevencie, odhaľovania, zmierňovania a reakcie, čo umožní zdieľanie informácií a vzájomnú pomoc medzi jednotlivými vnútroštátnymi orgánmi príslušnými pre oblasť bezpečnosti sietí a informácií. Od vnútroštátnych orgánov príslušných pre oblasť bezpečnosti sietí a informácií sa bude požadovať, aby zabezpečili vhodnú spoluprácu v rámci celej EÚ, a to najmä na základe plánu spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie, zameraného na reakcie na kybernetické incidenty s cezhraničným rozmerom. Cieľom bude takisto zlepšiť pripravenosť a zapojenie súkromného sektora. Keďže veľká väčšina sietí a informačných systémov je v súkromnom vlastníctve a súkromne prevádzkovaná, je nevyhnutné zlepšiť spoluprácu na podpore kybernetickej bezpečnosti so súkromným sektorom. Súkromný sektor by mal rozvíjať na technickej úrovni svoje vlastné kapacity kybernetickej odolnosti a zdieľať najlepšie postupy v rámci sektorov. Nástroje vytvorené priemyselným odvetvím ako prostriedky reakcie na incidenty, identifikácie príčin a vedenia forenzného vyšetrovania by mali prinášať prospech aj verejnému sektoru.

[14] 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, L 194/1.

Kybernetická bezpečnosť z hľadiska praktickej realizácie bude najmä o vytvorení správy (riadenia) tejto oblasti - pravdepodobne zastrešenej Národným bezpečnostným úradom a realizácie základných bezpečnostných požiadaviek - dostupnosti, integrity a dôvernosti služieb, regulovania prístupu k údajom, službám a oprávneným subjektom, bezpečnej a dôveryhodnej komunikácie oprávnených subjektov, vytvorenie bezpečnej a dôveryhodnej komunikačnej infraštruktúry na komunikáciu medzi jednotlivými entitami, odpojenie entít, ktoré sa stali nedôveryhodnými alebo prestali spĺňať bezpečnostné požiadavky. Ostatné subjekty štátu budú participovať v závislosti od kompetencií a schopností podieľať sa na bezpečnosti kybernetického priestoru. Bude potrebné redefinovať a kreovať pravidlá bezpečnosti tohto prostredia, právne a trestnoprávne nástroje, práva a povinnosti, postavenie a úlohy orgánov činných v trestnom konaní a pod. Strategické riadenie bezpečnosti kybernetického priestoru bude vytvárať tlak na efektívnosť, dynamiku a flexibility všetkých zúčastnených subjektov.

ZÁVER

Možno konštatovať, že v súčasnosti ešte nie je možné predvídať ako sa usporiada vzťah kybernetickej bezpečnosti a krízového riadenia štátu. Nie je ešte úplne zrejmé, čo všetko musí urobiť štát aby bol "kyberneticky bezpečný". Niektoré kroky a už realizované rámcové úlohy však naznačujú možný smer, čoho sa budú prípadné zmeny týkať, vrátane očakávaných komplikácií. Čas bude zohrávať dôležitú rolu. Medzinárodné záväzky a vývoj bezpečnostnej situácie vytvárajú dostatočný tlak aby sa tak urobilo čo najskôr. Minulosť však naznačuje, že procesy a ich časovanie nebudú vôbec jednoduché. Takéto konštatovanie naznačuje, že bezpečnosť štátu je často obetovaná na úkor množstva neštandardných a časovo zdĺhavých aktivít.

Krízový manažment vo vzťahu ku kybernetickej bezpečnosti môže nadobudnúť dve základné polohy: 1. Krízový manažment ako nástroj realizácie kybernetickej bezpečnosti a 2. Kybernetická bezpečnosť ako súčasť krízového manažmentu. Ako sa však oblasť kybernetickej bezpečnosti v súčasnosti vyvíja je skôr pravdepodobný scenár č. 1. Prakticky to znamená, že oblasť krízového manažmentu bude musieť vhodne reagovať na požiadavky vyplývajúce z realizácie opatrení kybernetickej bezpečnosti.

Vznika tu však niekoľko odlišností, ktoré budú zohrávať zásadnú rolu. V prvom rade sa mení rola súkromného sektora, čo nakoniec vyplýva aj zo Stratégie kybernetickej bezpečnosti EÚ. Zatiaľ čo doteraz štát spravidla dokázal jednoducho zabezpečiť relevantné bezpečnostné opatrenia v štandardných podmienkach, tak v prípade kybernetickej bezpečnosti je celkom zjavne odkázaný na úzku spoluprácu so súkromným sektorom. Zatiaľ čo v oblasti ochrany kritickej infraštruktúry štát stanovil jasné pravidlá a súkromný sektor sa v zásade rýchlo prispôsobil, tak v oblasti kybernetickej bezpečnosti bude potrebné budovať nové nástroje a mechanizmy. Štát bude v oblasti kybernetickej bezpečnosti na súkromný sektor odkázaný a táto závislosť sa bude s technickým a technologickým rozvojom prehlbovať. Štát musí budovať nové spôsobilosti a najmä vzájomnú dôveru všetkých zúčastnených subjektov. Bez dôvery nebude možné realizovať systémové opatrenia v oblasti kybernetickej bezpečnosti.

Kybernetická bezpečnosť napriek niektorým podobným funkcionalitám a princípom s oblasťou informačnej bezpečnosti vytvorí samostatnú oblasť, avšak úzko prepojenú na už existujúce spôsobilosti bezpečnostného systému a krízového manažmentu. Vzájomný vzťah týchto oblasti bude jednak závisieť od konečného definovania oblasti kybernetickej bezpečnosti a jednak od možností zmien a flexibility oblasti krízového manažmentu.

Všeobecne možno konštatovať, že kľúčovým bude integrovanie funkcionalít systému kybernetickej bezpečnosti do súčasného bezpečnostného systému štátu, vrátane systému krízového riadenia.

ZOZNAM POUŽITEJ LITERATÚRY

Akčný plán kybernetickej obrany NATO (NATO Cyber Defence Action Plan), www.mosr.sk

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti na roky 2015 - 2016, schválený uznesením vlády SR č. 93 z 2.3.2016,www.nbusr.sk

Bezpečnostná stratégia SR, schválená NR SR 27.9.2005, www.mosr.sk

IVOR, J. a kolektív Trestné právo hmotné. Všeobecná časť. I a II., Druhé doplnené a prepracované vydanie, Bratislava: IURA EDITION, 2010, 625 s., ISBN 978-80-8078-308-2

JIRÁSEK,P.,NOVÁK,L.,POŽÁR,J.: Výkladový slovník kybernetické bezpečnosti, Policejní Akademie České republiky v Praze, Česká pobočka AFCEA, Praha 2014, 200 str., ISBN 978-80-7251-397-0

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020, schválená uznesením vlády SR č. 328 zo 17.6.2015, www.nbusr.sk

Legislatívny zámer zákona o informačnej bezpečnosti, schválený uznesením vlády SR č. 136/2010 z 24. februára 2010

MAISNER, M., VLACHOVÁ, B. Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, a.s., 2015. 232 s. ISBN 978-80-7478-817-8.

Národná stratégia pre informačnú bezpečnosť, schválená uznesením vlády SR č.570/2008 z 27. augusta 2008.

NATO Review: Nové hrozby - kybernetické dimenzie, dostupné na: http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm

OLEJÁR, D. Manažment informačnej bezpečnosti a základy PKI. Bratislava, 2015. 164 s. (online). Dostupné na internete: http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s

Posilnená stratégia kybernetickej obrany NATO (Enhanced NATO Policy on Cyber Defence), 2014, www.mosr.sk

Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Európskej únii zo 6. júla 2016, L194/1.

Správa o bezpečnosti SR za rok 2015, dostupné na https://www.slov-lex.sk/legislativne-procesy, 2017

Stratégia kybernetickej bezpečnosti Európskej únie Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013), www.mosr.sk

Stratégia kybernetickej bezpečnosti Európskej únie. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013), http://www.consilium.europa.eu/sk/policies/cyber-security/.

Stratégia kybernetickej obrany NATO (NATO Policy on Cyber Defence), 2011, www.mosr.sk

Stratégia pre informačnú bezpečnosť v Slovenskej republike, schválená uznesením vlády SR č. 270/2008 z 27. augusta 2008

Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012, www.nato.int/docu/report/2012/Tallin-Manual/index.htm

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

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

Zákon č. 45/2011 Z.z. o kritickej infraštruktúre.

ADRESA

JUDr. Miroslav BRVNIŠŤAN,PhD
Akadémia Policajného zboru v Bratislave
Katedra verejnej správe krízového manažmentu
Sklabinská 1, 835 17 Bratislava

STŘEDOŠKOLSKÁ SOUTĚŽ ČESKÉ REPUBLIKY V KYBERNETICKÉ BEZPEČNOSTI

Petr HRŮZA

Univerzita obrany v Brně

Můj příspěvek je úvodním slovem souhrnné zprávy Středoškolské soutěže ČR v kybernetické bezpečnosti. Autoři této zprávy jsou členové soutěžního výboru soutěže, včetně mě. Předsedou soutěžního výboru a „otcem" celé myšlenky uspořádání této soutěže je Petr Jirásek.

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti. Nicméně se vzrůstající závislostí společnosti na informačních technologiích vzrůstá i riziko zneužívání těchto technologií uživateli (interní útočníci) nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám. V případech, kdy je interní nebo externí útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu. Obecným trendem v celém světě je kvalitní ochrana těchto informačních technologií před zásahy, které mohou ohrozit jejich chod.[1]

To logicky vede k požadavku na vytvoření a přípravu nových odborníků na kybernetickou bezpečnost[2], jakož i prohloubení všeobecné osvěty mezi běžnými uživateli informačních technologií i mezi občany.

Dne 25. května 2015 Česká republika přijala vládní usnesení, které zahrnovalo Národní strategii kybernetické bezpečnosti ČR a Akční plán Národní Strategie kybernetické bezpečnosti ČR na období 2015 - 2020. Tento akční plán mimo jiné zahrnuje celou řadu požadavků na vzdělávání odborníků, všeobecné veřejnosti i studentů na všech vzdělávacích stupních. Vysoké školy již několik let reagují na tuto situaci a postupně (byť nekoordinovaně) nabízejí vzdělávání v oblasti kybernetické bezpečnosti a obrany. Nicméně střední školství se doposud touto problematikou cíleně nezabývalo, což mimo jiné způsobuje malý zájem o studium oborů z oblasti kybernetické bezpečnosti a obrany na vysokých školách absolventy středních škol.

Akční plán Národní strategie kybernetické bezpečnosti ČR mimo jiné obsahuje řadu cílů[3] mířících právě na studenty a pedagogy středních škol, například: (a) navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti u studentů středních škol; (b) přispět k modernizaci vzdělávacích programů na středoškolské úrovni; (c) podporovat přípravu expertů; (d) přispět k přípravě metodických materiálů pro učitele a (e) podporovat u studentů rozvoj talentu v oblasti kybernetické bezpečnosti ve spolupráci s vysokými školami.

Pracovní skupina kybernetické bezpečnosti České pobočky AFCEA (dále jen „Pracovní skupina") již od roku 2004 vyvíjí řadu osvětových, vzdělávacích a odborných aktivit v oblasti kybernetické bezpečnosti a obrany. Pravidelně organizuje bezpečnostní semináře pro státní zaměstnance, akademické, zejména vysokoškolské, pracovníky a odborníky z privátní sféry. Vydala Výkladový slovník kybernetické bezpečnosti, který se stal oficiální publikací a získal celou řadu odborných ocenění. Zorganizovala řadu praktických cvičení, ukázek a výstav moderních

[1] Výňatek z důvodové zprávy k zákonu o kybernetické bezpečnosti České republiky.

[2] Kybernetická bezpečnost je souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru. Přičemž kybernetický prostor je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnující připojení k veřejné síti (internet). [Jirásek, Novák, Požár, Výkladový slovník kybernetické bezpečnosti, Praha, 2013. ISBN 978-80-7251-397-0]

[3] Zejména akční cíle kategorie F.

bezpečnostních trendů a technologií. Spolupracuje s vysokými školami a propojuje znalosti a zkušenosti mezi veřejnou správou, armádou, akademickou sférou a privátním sektorem.

Na konci roku 2015 členové Pracovní skupiny přišli s myšlenkou uspořádat celorepublikovou soutěž v kybernetické bezpečnosti zaměřenou na středoškolské studenty. Na jaře roku 2016 byla Česká republika oslovena evropskou agenturou ENISA[4], aby nominovala národní tým složený ze středoškolských a vysokoškolských studentů k účasti na European Cyber Challenge (dále též „Evropské finále"). Tato skutečnost významně urychlila přípravy prvotního záměru.

Díky rychle získané podpoře ze strany vybraných státních institucí, v čele s Národním bezpečnostním úřadem, Ministerstvem vnitra ČR a Ministerstvem práce a sociálních věcí, partnerských odborných asociací, zejména ICT Unie, ČIMIB, NCBI, a významných akademických institucí v čele s ČVUT, Univerzitou obrany v Brně, Policejní akademií ČR, Masarykovou univerzitou a VUT Brno, bylo v červenci 2016 rozhodnuto uspořádat první ročník Středoškolské soutěže ČR v kybernetické bezpečnosti již ve školním roce 2016/2017.

Soutěžní výbor, který byl sestaven z odborníků na kybernetickou bezpečnost, měl před sebou nelehký úkol. V relativně krátkém čase připravit kvalitní soutěž s cílem oslovit a motivovat mladou generaci k zájmu o kybernetickou bezpečnost. Pomocí soutěže ověřit znalosti středoškoláků v oblasti kybernetické bezpečnosti a vybrat nejlepší kandidáty pro účast na Evropském finále. Oslovit pedagogické pracovníky středních škol, připravit pro ně podpůrné materiály pro výuku kybernetické bezpečnosti a pomoci jim pochopit zákonitosti a záludnosti kybernetického prostoru a digitálního vzdělávání.

Přes drobné technické problémy v počáteční fázi příprav a velmi vysokou časovou náročnost bylo možné v říjnu 2016 prohlásit, že soutěž je připravena ke spuštění. Přispěla k tomu i celá řada odborných partnerů, kteří se do přípravy soutěže zapojily. Velké poděkování zaslouží všichni partneři, přesto je na místě zmínit dva z nich. Společnost Corpus Solutions, a.s. vytvořila pro soutěž zcela nový soutěžní portál s využitím technologie Lime Survey. Portál byl použit pro první a druhé soutěžní kolo a byl připraven čelit vysoké provozní zátěži. Společnost DataSpring a.s. poskytla hosting a technickou podporu soutěžnímu portálu ve svém datovém centru. Obě tyto aktivity přispěli k vysoké bezpečnosti provozu soutěžního portálu a bezpochyby k bezproblémovému průběhu prvního ročníku soutěže.

Nejvýznamnější výzvou prvního ročníku soutěže však byla skutečnost, podaří-li se oslovit studenti k účasti v soutěži a střední školy k zájmu o spolupráci. Soutěžní výbor neponechal nic náhodě a vytvořil celou řadu kampaní mířících jak na studenty samotné, tak na zřizovatele škol, střední školy, středoškolské pedagogy, rodiče a různá sdružení a asociace, která dlouhodobě spolupracují se středními školami.

Výsledkem je účast více než tisíce studentů ze 162 středních škol[5] z celé ČR. Ukázalo se, že největší vliv na přilákání zájmu studentů měla sociální média v čele s Facebookem. Neméně důležitá však byla i přímá komunikace se školami. V průběhu soutěže zástupci Soutěžního výboru rovněž uskutečnili 63 odborných přednášek na středních školách po celé ČR pro téměř 2.500 studentů a přibližně 150 pedagogů. Tato aktivita se setkala s velkým ohlasem a připravila prostor pro další spolupráci i větší zapojení středních škol do dalších ročníků soutěže.

Soutěž byla rozdělena do tří kol, přičemž otázky a úkoly se v jednotlivých kolech lišily svou obtížností a komplexností. První kolo proběhlo na přelomu listopadu a prosince 2016. Do druhého kola se uskutečnilo v březnu 2017. Do druhého kola se kvalifikovalo 565 studentů, z nichž 30 postoupilo do finále. Finálové kolo se uskutečnilo 1. června 2017 v Brně v rámci mezinárodního veletrhu obranných a bezpečnostních technologií IDET 2017, což umožnilo studentům a jejich pedagogickému doprovodu se seznámit s novými trendy a moderními technologii v oblasti bezpečnosti a obrany.

[4] European Union Agency for Network and Information Security.
[5] 162 středních škol je přibližně 12% všech středních škol v ČR.

Z finálového kola rovněž vzešli kandidáti na účast v národním týmu ČR pro Evropské finále. Jejich kvalifikace byla potvrzena na letním soustředění v Kybernetickém polygonu Masarykovy univerzity v Brně v červenci 2017.

Soutěžní výbor jménem všech jeho členů a organizátorů děkuje všem podporovatelům a partnerům prvního ročníku soutěže. Soutěž byla organizována jako nezisková, neztrátová a co nejméně nákladová se zapojením dobrovolníků, kteří na přípravě a průběhu soutěže strávili více než 1.750 hodin bez nároku na odměnu. Bez pomoci partnerů a podporovatelů a zejména bez dobrovolného aktivního zapojení mnoha osob, by nebylo možné soutěž uskutečnit. Organizátoři a Soutěžní výbor se rozhodli uspořádat druhý ročník soutěže ve školním roce 2017/2018 s cílem zvýšit povědomost studentů o kybernetické bezpečnosti, motivovat mladé lidi o moderní technologie a umožnit studentům středních škol poměřit své znalosti se svými vrstevníky.

Do prvního kola druhého ročníku soutěže se již zapojilo přes 2.300 studentů, a to mají studenti ještě tři týdny, aby se mohli so soutěže přihlásit. V druhém ročníku proto očekáváme trojnásobný nárůst soutěžících. Na Soutěžní výbor to bude také trojnásobné množství práce vykonané pro soutěž. Zájem partnerů o podporu soutěže tím také narůstá a hlásí se další zájemci. Aktuální dění okolo soutěže je možné sledovat na facebookových stránkách https://www.facebook.com/kybersoutez/.

ADRESA
pplk. Ing. Petr HRŮZA, Ph.D.
Katedra taktiky
Fakulta vojenského leadershipu
Univerzita obrany v Brně
Kounicova 65, 662 10 Brno, Česká republika
petr.hruza@unob.cz

KYBERNETICKÉ HROZBY KRITICKEJ INFRAŠTRUKTÚRY

Ladislav KITTEL

Akadémia Policajného zboru v Bratislave

Abstrakt: *Článok sa zaoberá problematikou kritickej infraštruktúry, jej právnym vymedzením so zreteľom na kybernetické hrozby, ktoré môžu ohroziť fungovanie informačných systémov s možnými následkami pre spoločnosť v prípade narušenia funkcií kritickej infraštruktúry.*
Kľúčové slová: *kritická infraštruktúra, kybernetický priestor, kybernetické hrozby*

Abstract: *The article deals with critical infrastructure issues, its legal definition with regard to cyber threats that can threaten the functioning of information systems with possible consequences for society in case of disruption of critical infrastructure functions.*

Keywords: *critical infrastructure, cyberspace, cyber threats*

KRITICKÁ INFRAŠTRUKTÚRA

Vychádzajúc z novodobých bezpečnostných rizík vzrástla vo vyspelých štátoch sveta potreba definovania kritickej infraštruktúry, ako oblasti infraštruktúry ktorej znefunkčnenie, alebo zničenie má za následok ohrozenie, alebo narušenie politického alebo hospodárskeho života v krajine, ohrozenie alebo straty na životoch alebo majetku, škody morálneho charakteru a demoralizáciu a dezorganizáciu spoločnosti. Objektívna potreba zabezpečiť ochranu a obranu dôležitých objektov národnej infraštruktúry pred tradičnými hrozbami, akými boli a sú prírodné katastrofy, technologické havárie, nedbalosť, novodobá hrozba teroristických útokov, neoprávnené vniknutie do počítačových systémov, alebo trestná činnosť, sa rozšírila o možnosť kybernetických útokov.

Kritická infraštruktúra predstavuje objekty, ktoré svojou funkciou zabezpečujú dôležité prvky chodu spoločnosti. Sú dôležité pre bezpečnosť štátu, správny chod ekonomiky, plynulý chod verejnej správy a sprístupnenie základných životných potrieb obyvateľom štátu. Zaradené sú sem objekty osobitnej dôležitosti, vybrané informačné a komunikačné prostriedky, zariadenia na zásobovanie vodou, elektrickou energiou, ropou, zemným plynom a ďalšie objekty majetku štátu a právnických osôb, fyzických osôb - podnikateľov a fyzických osôb určené vládou, alebo iným kompetentným orgánom štátnej správy.[1]

Poškodenie alebo prípadné narušenie kritickej infraštruktúry môže byť spôsobené prírodnou katastrofou, alebo môže byť zapríčinené vplyvom ľudského faktoru. Môže ísť o zlyhanie techniky a technologických postupov alebo môže ísť o úmyselné akcie organizovaného zločinu, terorizmu alebo iný spôsob útoku. Preto cieľom ochrany kritickej infraštruktúry musí byť minimalizácia výpadkov činností týchto infraštruktúr tak, aby narušenie činností alebo služieb bolo krátkodobé, zvládnuteľné minimálne provizórnym alebo alternatívnym spôsobom.[2]

Ďalším dôležitým faktorom kritickej infraštruktúry je jej vzájomná závislosť v rôznych sektoroch, ktorých narušenie vytvára domino efekt, čo znamená, že porucha kritickej infraštruktúry v jednom sektore ma vplyv aj na ďalšie sektory. Veľmi dôležitým je energetický sektor, na ktorom je závislých mnoho ostatných sektorov ako napríklad doprava, informačne systémy a ďalšie.

Postup orgánov zodpovedných za kritickú infraštruktúru, stanovenie postupov pri určovaní prvkov kritickej infraštruktúry, sektorových kritérií a tvorení predpokladov na ich účinnú ochranu, sú riešené v zákone NR SR č. 45/2011 Z.z. o kritickej infrastructure (ďalej len „zákon“). Zákon ďalej stanovuje úlohy orgánov štátnej správy, povinnosti právnických osôb, fyzických osôb -

[1] ŠIMÁK, L., HORÁČEK, J., NOVÁK, L., NÉMETH, Ľ., MÍKA, V. 2005. Terminologický slovník krízového riadenia. Žilina: FŠI ŽU, 2005. 44 s. ISBN 80-88829-75-5.
[2] http://www.minv.sk/?Ochrana_kritickej_infrastruktury.

podnikateľov a fyzických osôb pri zabezpečovaní ochrany kritickej infraštruktúry a sankcie za porušenie týchto povinností.[3]

Vychádza hlavne s adaptácie smernice o označení a identifikácií európskych kritických infraštruktúr (2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu) v ktorej sú špecifikované pojmy európska kritická infraštruktúra, analýza rizík, citlivé informácie o ochrane kritickej infraštruktúry a ďalšie pojmy.[4]

Za kybernetický priestor je považované globálne a dynamické prostredie, ktoré je charakteristické kombinovaným použitím fyzických, technologických a digitálnych prostriedkov, ktoré sú určené na tvorenie, ukladanie, modifikovanie, výmenu, zdieľanie, využívanie a elimináciu informácií.

Kybernetický priestor obsahuje :

- Fyzickú infraštruktúru a telekomunikačné zariadenia, ktoré umožňujú prepojenie technologických a komunikačných sietí (napr. smartfóny; počítače; systémy SCADA - „Supervisory Control And Data Acquisition“, teda „dispečerské riadenie a zber dát“ - nejde o plnohodnotný riadiaci systém danej technológie, ale systém zameraný skôr na dispečerský dohľad, monitoring).
- Software systémy, ktoré zabezpečujú základnú prevádzkovú funkčnosť a prepojiteľnosť zariadení.
- Siete medzi počítačovými štruktúrami.
- Prístupové uzly a sprostredkovateľské uzly používateľov.
- Databázy.

Internet je označovaný ako sieť sietí a siete medzi počítačmi sú označované ako intranet. Ďalším charakteristickým znakom kybernetického priestoru je jeho decentralizácia tzn. neexistuje žiadna entita, ktorá by mala kontrolu na celým priestorom, ale skladá sa s mnohých samostatných sietí.

Kybernetická bezpečnosť je jedným z určujúcich prvkov bezpečnostného prostredia pričom na úrovni štátu predstavuje systém sústavného a plánovitého zvyšovania právneho, obranného, bezpečnostného a vzdelanostného povedomia, ktorý zahŕňa aj zvyšovanie účinnosti prijatých a aplikovaných technicko-organizačných opatrení riadenia rizík v kybernetickom priestore za účelom jeho transformácie na dôveryhodné prostredie, ktoré umožňuje bezpečné fungovanie spoločenských, ale aj hospodárskych procesov pri zabezpečení akceptovateľnej úrovne rizík v kybernetickom priestore.[5] Jej zraniteľnosť spočíva vo využití slabého miesta, alebo zneužití nedostatkov v bezpečnostných opatreniach, ktoré môžu byť využité jednotlivými hrozbami. Využitá môže byť zraniteľnosť softwaru, hardwaru, procesná zraniteľnosť, alebo zraniteľnosť spojená s ľudskou chybou.

Problematiku kybernetickej bezpečnosti nie je možné vnímať izolovane, ako problém jedného štátu ani ako izolovaný problém jednej alebo niekoľkých zložiek spoločnosti. Kybernetická bezpečnosť je vzhľadom na svoj všeobecný charakter celospoločenským fenoménom, pričom si vyžaduje intenzívne spoločné využívanie informácií a koordináciu aktivít na národnej, ako aj medzinárodnej úrovni.

KYBERNETICKÉ HROZBY

Kybernetická hrozba je akékoľvek potenciálne nebezpečenstvo, ktoré je často viazané na určitý nedostatok, alebo zraniteľnosť v systému, ktorý môže mat za následok poškodenie dotyčného systému, napríklad zničenie, nepovolený prístup, modifikáciu dát alebo nedostatočnosť služieb.

Kybernetické hrozby sú hlavne charakteristické svojou nesúmernosťou, obmedzenými možnosťami na zistenie ich pôvodu a faktom, že môžu byt vyvolané rôznymi vplyvmi.

[3] http://www.zakonypreludi.sk/zz/2011-45.
[4] https://publications.europa.eu/sk/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10.
[5] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.

Kybernetické hrozby a z nich vyplývajúce kybernetické útoky môžeme vo všeobecnosti považovať za nebezpečné, lebo:

- Nevyžadujú veľké náklady a väčšina metód využívaných na produkovanie určitého útoku môžu byť získané s internetu alebo zakúpené na internete za relatívne nízku cenu.
- Vytvorenie takéhoto útoku nevyžaduje ťažko získateľné znalosti a skúsenosti čo znamená, že útoky pochádzajúce od hocikoho môžu spôsobiť veľké škody.
- Kybernetické útoky sú neprimerané v námahe a úsilí, ktoré je potrebné na ich vyvolanie a v následkoch ktoré môžu spôsobiť. Škody môžu byt dokonca oveľa horšie ako boli očakávané od pôvodcu útoku.
- Hlavným aspektom je anonymita pôvodcu útoku, ktorú im poskytuje komplexná štruktúra internetu a legislatívnych medzier v mnohých štátoch.

Tieto hrozby sú o to nebezpečnejšie a aktuálnejšie, lebo veľká časť kritickej infraštruktúry, zahrnujúca energetiku, vodohospodárstvo, zdravotníctvo, či prepravu je kontrolovaná, monitorovaná a ovládaná pomocou rôznych informačných systémov ako napríklad SCADA. Obvykle sa tento pojem používa pre software, ktorý z centrálneho pracoviska monitoruje priemyslové a iné technické zariadenia a procesy a umožňuje ich ovládanie.

Tieto systémy, ktoré boli v minulosti väčšinou prístupné iba interne (v podnikoch, inštitúciách), sa stávajú stale viac prístupné pomocou internetu. Zvýšená prepojiteľnosť, integrácia, diaľkové ovládanie a používanie štandardov a protokolov otvoreného softwaru, zvyšujú ovládateľnosť kritickej infraštruktúry, zároveň ju robia zraniteľnejšou voči rôznym hrozbám z kybernetického priestoru ako napríklad narušením a ohrozovaním bodov bezdrôtového pripojenia, alebo distribúciou infikovaných USB kľúčov v zariadeniach.

Nebezpečenstvá vyplývajúce z kybernetických útokov rôzneho druhu sú zhoršené faktom že mnoho s týchto informačných systémov (monitorovacie, ovládacie, koordinačné) sú slabo zabezpečené z dôvodu, že boli vyvinuté v čase keď sa nepočítalo so všeobecnou prepojiteľnosťou cez internet, alebo fungujú na základe softwaru, ktorý už dosiahol koniec životnosti (nie sú vytvárané aktualizácie) ako napríklad Windows XP. Zároveň používanie otvoreného softvéru poskytuje možným útočníkom ľahšiu identifikáciu rôznych zraniteľností.

Prevencia pri ochrane kritickej infraštruktúry sa zameriava na zisťovanie kybernetickej bezpečnosti kritickej infraštruktúry tak, aby bola čo najviac odolná voči narušeniu, a aby všetky relevantné subjekty v rámci kritickej infraštruktúry boli schopné a pripravené reagovať na možnosť výskytu kybernetického útoku, respektíve kybernetickým bezpečnostným incidentom. Pri detekcii nových spôsobov útokov je dôležitá schopnosť čo najrýchlejšie identifikovať nové kybernetické hrozby a analyzovať kybernetické bezpečnostné incidenty. Ide hlavne o zdieľanie technických a netechnických informácií o hrozbách zraniteľnosti, útokoch na národnej a medzinárodnej úrovni.

Veľmi dôležite sú informácie od subjektov zodpovedných za kybernetickú kriminalitu - policajne zložky, zo spravodajskej činnosti v kybernetickom priestore - spravodajské zložky a za kybernetickú obranu - vojenské zložky, až po analýze informácií, ku ktorým je často obmedzený prístup je možno zaujať tie najefektívnejšie protiopatrenia. Až následne, ako reakcia sa určujú opatrenia na nápravu príčin narušenia v systéme, respektíve v bezpečnostnom kybernetickom incidente, pričom ide hlavne o poskytnutie technickej podpory a pomoc s riešením následkov narušenia v systéme kritickej infraštruktúry. Veľmi dôležitá je rýchla a efektívna reakcia, pretože dĺžka trvania kybernetického útoku je priamo úmerná škode, ktorá bude s neho vyplývať. Tato fáza zahrňa aj ex post analýzu bezpečnostného incidentu.

ZÁVER

Kybernetické útoky sa stavajú stále väčšinou hrozbou a koordinovaný kybernetický útok na kľúčové štruktúry kritickej infraštruktúry môže spôsobiť nebezpečný domino efekt ohrozujúci národnú bezpečnosť a civilne obyvateľstvo. Zvládanie a minimalizácia narušenia systémov kritickej infraštruktúry cez kybernetický priestor musí byť zakomponovaná do celkového krízového

manažmentu s tým, že subjekt zodpovedný za krízový manažment a kritickú infraštruktúru musí mať vybudovaný potrebný inštitucionálny rámec na plnenie úloh v oblasti kritickej infraštruktúry, vyčlenené finančné zdroje na bezpečnostný výskum a spolupracovať s výkonnými zložkami štátu a obdobnými orgánmi ostatných štátov v spoločnom európskom priestore.

ZOZNAM POUŽITEJ LITERATÚRY

ŠIMÁK, L., HORÁČEK, J., NOVÁK, L., NÉMETH, Ľ., MÍKA, V. *Terminologický slovník krízového riadenia*. Žilina: FŠI ŽU, 2005. 44 s. ISBN 80-88829-75-5.

VIDRIKOVÁ, D., BOC, K. *Ochrana kritickej infraštruktúry - 1. časť*. Žilina: Žilinská univerzita, 2013. ISBN 978-80-554-0654-1.

Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike.

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.

http://www.vlada.gov.sk/medzirezortna-terminologicka-komisia-bezpecnostnej-rady-slovenskej/.

http://www.minv.sk/?Ochrana_kritickej_infrastruktury.

https://secit.sk/content/cerv-stuxnet-ohrozuje-atomovu-elektraren.

http://www.zakonypreludi.sk/zz/2011-45.

http://www.revistaie.ase.ro/content/68/11%20-%20Colesniuc.pdf.

https://link.springer.com/content/pdf/10.1007%2F978-0-387-88523-0.pdf.

https://publications.europa.eu/sk/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10.

ADRESA

Mgr. Ladislav KITTEL
Akadémia Policajného zboru v Bratislave
Katedra verejnej správe krízového manažmentu
Sklabinská 1, 835 17 Bratislava
ladislav.kiitel@minv.sk

POČÁTKY KRIZOVÉHO ŘÍZENÍ V ČESKÉ REPUBLICE

Milan KNÝ

Policejní akademie České republiky v Praze

Abstrakt: *V článku jsou shromážděna fakta a názory na řešení bezpečnostní problematiky a konstituování oboru krizového řízení v ČR po přelomovém roce 1989.*

Klíčová slova: *krizové řízení, krizový management, bezpečnostní management, bezpečnost.*

Abstract: *The facts and views regarding the solution of security problematics and constitution of the crisis management field in the Czech Republic after the breakthrough year 1989 are compiled in the article.*

Key words: *crisis management, security management, safety, security.*

ÚVOD

Na počátku relativně širokého tématu je vhodné „definovat" prostor a čas, objekt zájmu a jeho historické zasazení. Počátek existence rovněž vyžaduje normativní určení, neboť zvláště u společenských procesů a jejich systémového vymezení „zrození" nastává z existence již předchozího a z vůle nutnosti. Kdy „vznikl" krizový management v Čechách?

Své poznatky prezentujeme z intervalu 1990 až 2017 s fuzzy hranicemi na obě strany a se zvláštním zřetelem k relevanci „počátky krizového řízení v České republice", která se stává samostatným českým státem analogicky se Slovenskou republikou na přelomu 21. století.

Cílem příspěvku je vymezit prostor zájmu v souvislosti s okolím, upřesnit pojmový aparát v kontextu vývoje oboru teorie a praxe a krystalizace významného tématu bezpečnostní vědy. Aby nedošlo ke zklamání vnímatele, nutno podotknout, že autorský názor a odraz objektivních explicitních znalostí nebude zdaleka tímto sdělením vyčerpán. Může však z implicitních znalostí a zvláštních dochovaných pramenů posloužit výzkumníkům k inspiraci a opatrnosti využít kupříkladu „jen" současných legislativních úprav k tématu.

OČEKÁVÁNÍ A RIZIKA SPOLEČENSKÝCH ZMĚN

Mezinárodní situace se po ukončení 2. světové války determinovala ve Střední Evropě a tím i v Československu tak, že se stala v bipolárním světě antagonického působení ve sféře zájmu východní velmoci. Ekonomicky součástí Rady vzájemné hospodářské pomoci (RVHP) a vojensky součástí aliance Varšavské smlouvy v dominanci SSSR.

Vnější i vnitřní bezpečnost byla v tomto rámci řešena v těsné a unifikované podobě, působily mocenské a politické elity jako determinanty odlišně, když byla změně vojenská doktrína v souvislosti se zánikem bipolarity. Přírodní a průmyslové hrozby bezpečnosti se prakticky nezměnily a ekologické původně nebyly adekvátně vnímány. (viz koncept PESTEL[1]).

Tradiční pojetí bezpečnostních složek státu se v Československu a později v České republice a ve Slovenské republice prakticky nezměnilo, jen další vývoj legislativní i organizační probíhal samostatně - odděleně. Pro armádní doktrínu zanikla představa „nepřítele" a spojence z východu odchodem „dočasně umístěných sovětských vojsk" a zrušením svazku Varšavské smlouvy. Aliance NATO však zrušena nebyla a stala se hostitelem pro satelitní země bývalého sovětského bloku. Armáda České republiky (AČR) zahájila restrukturalizaci, zrušena byla vojenská základní služba (VZS). „Obrana obyvatelstva" a příslušné složky vojska zůstaly dočasně v resortu Ministerstva

[1] Vnější faktor rozvoje podle konceptu PESTLE apod., jsou symbolizované jako politické, ekonomické, sociální, technologické, ekonomické a legislativní, mnohdy v kombinaci působení.

obrany ČR. Vnější rizika byla podceněna, v každém případě iluze svobody v politice i u občanů působily jako demotivátor pro velení AČR. Z armády odešla řada odborníků do civilních a nearmádních bezpečnostních složek. Změny probíhaly také u Policie České republiky (PČR) a v Hasičském záchranném sboru (HZS), mj. v souvislosti se změnou správního uspořádání republiky.

V oboru, který byl také nazýván „krizové řízen" docházelo k „mírnému pokroku" na některých vysokých školách a v rámci projektů spolupráce se „západem" (MATRA, švýcarský nebo nizozemský projekt či USA/FBI). Vyvíjela se terminologie a instituce ve státní správě s patrným vlivem angličtiny (např. management místo řízení).

Uvědomovaná společenská rizika devadesátých let

V první polovině devadesátých let dvacátého století byla podchycena v akademické sféře škála významných společenských rizik (tzn. nikoliv s ohledem na jednotlivce, podniky a lokální instituce, spíše se zřetelem na kompetenci státu), která se neshodují zcela s vědomím rizik v 21. století. Jeden z dokumentů amerického FBI[2] konfrontoval závažné bezpečnostní hrozby v USA s hrozbami, vyskytujícími se ve Střední Evropě a „u nás". *Až úsměvné bylo si představit, že by se vulkanicky aktivovala Milešovka nebo že pobřeží Labe postihlo tornádo.*

Vážně však byla specifikována rizika:

a) Živelné pohromy
b) Provozní průmyslové havárie
c) Epidemie
d) Ekonomika /obavy z nefunkčnosti trhu
e) Expanze kriminality
f) Občanské nepokoje
g) Válka
h) Migrace

Ad a) Z dlouhodobého hlediska se rizika živelných pohrom v daném prostředí nemění, jen pravděpodobnost ohrožení souvisí s četností v aktuálním časovém intervalu. Ochrana proti povodním, například, byla podceněna do konce devadesátých let minulého a počátku 1. dekády stávajícího století.

Ad b) Průmyslové havárie prolongují svůj charakter ve změnách technologií, jejich příčiny se mohou pohybovat do oblasti softwarového zabezpečení.

Ad c) Epidemie, v současnosti spíše pandemie hrozí v civilizovaném prostředí zřídka, neúmyslně, pohybem obyvatel, novými virovými mutacemi přenosem v globálním prostředí.

Ad d) „Ekonomika /obavy z nefunkčnosti trhu" je pravda, že na počátku návratu k tržní ekonomice obavy pramenily z nejistoty[3], jak se podaří zvládnout transformaci ekonomiky z centrálně plánované ekonomiky převážně netržní[4]. Současná ekonomická rizika jsou zcela jiná, viz např. krize „nemovitostí a úvěrů v USA" s globálním rozšířením.

Ad e) „Expanze kriminality" platila do přelomu tisíciletí, později s otevřením kybernetického prostření „nové hrozby" implikovaly také „nové kriminální skutky" v progresivním průběhu a účinnosti jednotlivých opatření bezpečnosti. Na kriminalitu měly vliv i prezidentské amnestie.

Ad f) „Občanské nepokoje" ve větším rozsahu nenastaly, pořádkové jednotky v podmínkách demokratické společnosti měnily styl zásahu, který se stal běžným způsobem akceptovatelným většinou obyvatelstva. Vztah policista - občan se však vyvíjí pomalu.

[2] Crisis Management FBI Academy 1991.
[3] Známý problém privatizace, kritizovaná forma, tempo implementace v rozporu s legislativním zabezpečením, problém trvá a není dosud vyhodnocen objektivním auditem.
[4] Banc of ...Lehman Brothers, viz investiční krize 2008 se světovým dopedem.

POČÁTKY TEORIE ŘÍZENÍ KRIZOVÝCH SITUACÍ

Zkušenosti z řešení krizových situací a dalších bezpečnostních situací iniciovaly teoretický přístup k řízení tohoto procesu. „Situace“ byla vnímána jako proces dynamický, intervalový. „Řízení“ je pojato šířeji než vlastní proces ohrožení zájmového prostoru, akutnímu průběhu předchází fáze přípravy, analýzy a plánování, podobně jako u projektového řízení. Operativnímu řízení v krizi následuje fáze revitalizace, adaptace, odstranění škod.

Uvědomili jsme si, že řešení krizí a podobných hromadných jevů vyžaduje exploataci teorie, metodologie a procesů z oboru managementu, neboť je v zájmu „člověka“ chránit se a připravovat se podle praktických případů na další možný výskyt podobných rizik. Řídit nelze všechno, proto v definici krize „překáží“ vše, co přímo řídit nelze. Z teorie řízení je zde relevantní spíše pojem regulace, monitoring, kontrola, plánování, predikce apod. Jedním ze zdrojů „teorie“ byla systémová analýza „připravenosti na řešení krizové situace“ (Ministerstvo vnitra ČR, 1993). Je třeba připomenout, že v tu dobu se státní správa samostatného státu po rozpadu federace konsolidovala a těžila ze zastaralých norem co bylo možné ještě z období socializmu. Zkušenosti ze zahraničí se vzájemně neshodovaly. Na vysokých školách patrně po objednávce praxe ke školení specialistů pracovali paralelně na metodice. Z našich pramenů nový bezpečnostní obor zájmu přichází s názvem „Krizový management“ (Institut krizového managementu, jako institucionální složka, Vysoké školy ekonomické v Praze, 1993. [5]

Na začínající (1992) Policejní akademii v Praze byla zpracována studie „Řízení krizových situací - teorie“, 1994. Teprve k pozdějším studijním programům byla zřízena samostatná katedra krizového řízení na fakultě Bezpečnostního managementu. Do té doby byl obor rozvíjen na katedře policejního managementu a informatiky a na katedře tělesné a služební přípravy.

Vývoj terminologie

Je pochopitelné, že po roce 1990 orientace na Západ koreloval s budováním svobodné a demokratické společnosti, pro kterou byla důležitá transformace ekonomiky a práva v zabezpečeném prostředí. Tato změna je doprovázena také kontextem s jinými jazyky. Hledá se ekvivalent. Pro korunu v oblasti měn přestává být ekvivalentem rubl, pro překlad textů a prameny odborných znalostí ruština. Není naší ambicí komentovat, co je správné, z historického a geografického zájmu by byla dlouhodobá kontinuita (např. viz Švýcarsko) a stabilita. V našem prostředí byly používány tyto jazyky a v nich odborná terminologie: *čeština, slovenština, ruština, angličtina, němčina, francouzština*. V *p*ísemném i mluveném slovu většina Čechů dobře rozuměla slovenštině a ruštině. Dominance angličtiny teprve startovala jako generální světový jazyk, také v oblasti bezpečnosti. Němčinu ovládali starší ročníky. Francouzština byla motivující k působení v Evropském společenství společně s angličtinou, která je jazykem velení složek NATO. Z jazykových komunikačních prostředků je patrna perspektiva vytěžování pramenů s ohledem na jazyk anglický a orientací na USA. Za zmínku stojí zejména dva prameny, kterých bylo využito počátkem 90. - tých let:

- Emergency Management - ICMA, 1991
- Crisis Management - FBI Academy, 1991

V souvislosti s bezpečnostními hrozbami 21. století v kybernetickém prostoru uvádíme odvozené atributy, vycházející z odlišnosti substantiv: **bezpečnost a obrana**.

Krize (crisis) má příčinu a následek, který může implikovat **konflikt**. **Válečný konflikt** (Webová definice) - Válka je stav organizovaného násilí mezi dvěma nebo více skupinami lidí. Násilí je ve válce použito válčícími stranami jako mocenský prostředek k prosazení politických, náboženských, ideologických, ekonomických nebo jiných cílů. Válka je opakem míru.

Filosofie představovala „krizi“ od 18. století jako narušení rovnováhy mezi pokrokem a setrvačností zastaralých institucí.“ Nejstarší pramen (Genesis, Starý zákon / interpretace Tomáš

[5]Do řad akademických pracovníků přicházeli jako lektoři bývalí pracovníci armády a dalších bezpečnostních sborů.

Sedláček, 2017): krize je důvod ke smíření. Krize je změna, s možností šance na zlepšení, inovaci. Válečný konflikt souvisí především s mezinárodními vztahy a světovou bezpečností. „Konflikt, krize a intervence“ se vyskytují také v oblasti psychologie a sociologie vztahů mezi lidmi. Tato zmínka není od věci, neboť „vše vychází od člověka a jeho chování“[6]. V managementu je rozhodující lidský činitel v pozitivním i negativním smyslu.

Další pojem, který hodláme zmínit jako příklad je **recese** (z latinského slova recessio = ústup)**.** Ekonomická recese je v makroekonomii definována jako pokles reálného hrubého domácího produktu (HDP) po dvě nebo více následující čtvrtletí v roce (analogicky dvě po sobě jdoucí čtvrtletí s **ekonomickým poklesem**). Tuto fázi zmiňujeme k ilustraci ekonomickým hospodářským cyklem.

Krizím i **konfliktům** lze zabránit, nebo je zmírnit, to je úlohou řízení. Když už k nim dojde, proměnit je v konkurenční výhodu, v subjektivní užitek.

Náročná bezpečnostní (životní) situace (1990+), pojem nemá ustálenu specifikaci a pojmenování. Každá taková situace nemusí mít charakter krize ani konfliktu. Blízkými atributy jsou „emergentní“, „mimořádná“, kritická. Porovnejme dále „kritickou infrastrukturu“ a „kritickou informační infrastrukturu“.

Pro ekonoma je základním hospodářským celkem domácnost, to je rodina i „singl“. Sociologie pracuje se skupinou, se společenským celkem, psychologie s jednotlivcem, v komplexu těla a duše. Ve všech objektech lze rozlišovat „krize“.

Ke krizi lze přistupovat podle KASTOVÉ (2000) tvořivě, také životní krize mají dynamický charakter, který je podporou jiného než postiženého subjektu ovlivňován intervencí např. terapeuta. K hlubinné psychologii mnoho přispěl C. G. JUNG.

„…Když se člověk ocitne v zatěžující nerovnováze mezi subjektivně významně vnímaným problémem a mezi možnostmi jak je zvládnout disponibilními prostředky, je to charakteristické pro krizi“. V krizi cítíme ohrožení své identity, kompetence…jsem ohrožen ztrátou sebevědomí jak formovat další svůj život, jeho smysl, holou existenci. Ochromuje nás úzkost, bezradnost, pocit marnosti snažení. Východiskem z krize je naděje, jako alternativa dynamiky rizika.[7] Objeví-li se nápad, alespoň jak se vrátit k původnímu nebo starou strategii změnit inovací.

Latinské crisis: rozdělení, svár, rozsudek, rozhodování přes (inflexní) bod obratu. (Volně podle KASTOVÉ, 2000).

POJETÍ KRIZE V BEZPEČNOSTNÍM MANAGEMENTU

Pojetí „fází krizí“ (1994), vyžadující řízení

Průběh bezpečnostní krizové situace je dynamický proces, ve kterém jsou zakomponovány manažerské řídící činnosti, které mají působit na vyřešení krize.

Předmětem je:

- Ochrana ústavních, ekonomických a právních základů státu
- Ochrana života, zdraví, majetku a dalších zájmů obyvatelstva

Zdroje tohoto pojetí jsou:

- Civilní obrana /resort MO/,
- ochrana objektů,
- BOZP,[8]
- obrana státu,
- činnost bezpečnostních složek státu.

[6] ...někdo by namítal, že od Boha, přírody, lidské psýché.

[7] Někdy je třeba změnit hodnotovou orientaci, změnit definici daného celku a jeho perspektivy v novém smyslu existence. Radikální řešení musí být subjektem akceptovatelné.

[8] BOZP (bezpečnost a ochrana zdraví při práci / původně P = „pracujících“) je kontinuálním tématem bezpečnosti, bezpečnostního managementu.

Fáze krize

1. *Předkrizová situace*
2. *Varovné cykly*
3. *Krizové události*
4. *Přechodné stavy*
5. *Pokrizová situace*

KDO má povinnost a odpovědnost v řízení jednotlivých fází krize? Klasicky v managementu odpovědnost a pravomoc i určování úkolů, povinností má kompetentní vedoucí, manažer. V oblasti bezpečnosti, např. BOZP, jsou zavázáni povinnostmi a odpovědností „za sebe sama“, také další účastníci situace.

K pojetí krizového managementu 1999

Můžeme posoudit z hlediska dnešních současných poznatků, do jaké míry byly relevantní položené otázky v „tezích“:

Teze 1: Existuje závislost efektivnosti krizového řízení konkrétní situace a bezpečnostní akce na kvalitě managementu?

Teze 2: Kvalita manažerů významně ovlivňuje kvalitu krizového managementu?

Teze 3: Vzdělání, příprava, výcvik a kondice lidí, pověřených řešením potenciálních či reálných krizových situací je důležitou složkou jejich kvalifikace?

Důsledkem naplnění tezí má být podporována:

- Příprava manažerů
- Efektivita krizového řízení
- Kvalita managementu

ZÁVĚR

Transformace centrálně plánované ekonomiky (CPE) a tržní ekonomiku (TE) probíhala v kontextu přechodu na právní stát a demokratickou společnost. Hledání nové podoby Českého státu v návaznosti na dobré přerušené tradice, zároveň vyžadovalo přehodnotit prvky bezpečnostního systému a jeho vazby. Zejména v první polovině devadesátých let dvacátého století „se štěstím“ bez fatálních krizí a katastrof bylo přežito.

Druhá polovina devadesátých let registruje snahu o změny s využitím „dobré praxe“ a některých apolitických bezpečnostních norem. Uvolnění pro jednání subjektů předstihlo logickou souvztažnost s právním zajištěním kritických zdrojů. Svobody podnikání a bytí zneužili a využili (dle sporných názorů) ty síly, které uskutečnily redistribuci hodnot ve svůj prospěch. Je to znakem snížené úrovně bezpečnosti ve všech oblastech pod optimální hladinu. Vrcholový management společnosti (státu i politiky) liknavě prováděl zabezpečení proti ztrátám a ohrožení vývoje. Pomalu, spíše po závažných událostech, představujících hrozby a ohrožení bylo systematičtěji jednáno.

Povodně na Moravě předcházely totální „stoletou“ povodeň v širokém povodí českých řek. Akademická sféra na slabá místa bezpečnosti upozorňovala (mj. semináře v Ostravských univerzitách).

Stáže našich odborníků ve Švýcarsku a Holandsku, SRN -následné kurzy v ČR pomohly při modelování školení bezpečnostních specialistů a jejich využití při tvorbě zákonných a dalších norem.

Konference (T-Soft a HZS „Budoucnost krizového řízení) různých platforem ozbrojených sborů, škol, civilních a soukromých bezpečnostních služeb zvyšovaly bezpečnostní povědomí a potenciál.

Příprava Krizového zákona a dalších norem k integraci a spolupůsobení záchranných a bezpečnostních složek.

Internet a odkrytí informačních systémů do kybernetického prostoru znamenaly a znamenají nejen nepředstavitelné informační a manažerské možnosti, ale také v protikladu zájmů boj a nebezpečí všem.

Výzkum bezpečnostního managementu => 21.století, digitální svět, kybernetický rozměr špatně definovatelné virtuality už nepatří k tématu Počátky krizového řízení.

SEZNAM POUŽITÝCH PRAMENŮ

State of Missouri - Trade Mission. Prague and Bratislava, October - November 3, 2000.

KNÝ Milan. ***Vývojové tendence krizového managementu v ČR***. Sylabus ke školení bezčnostních ředitelů resortů, Praha, 1993.

Zvládání kritických situací a pomoc při pohromách v Holandsku. Ministerstvo obrany, Hlavní úřad civilní ochrany ČR, Praha 1995, studie.

POLMAN J.M.M: a SOURBAG M:B:M. ***Řešení krizí***, Nizozemsko, Praha 1995, studie

HILTERMAN Frank a další. ***Evropa a místní správa.*** Projekt MATRA, kurz pro lektory, Nadace Fond pomoci místní správě ČR, Institut pro místní správu, Asociace holandských municipalit (VNG), holandská konzultační firma Rubicosort.1999 (následně kurz „Krizové řízení“, mj. účast Kný, Stejskal, Brůček, Němec, v Holandsku a v Benešově 1999-2000).

Seminář k problematice krizového managementu ve školách. Rkp. z přednášek Praha SPŠ MV v Praze Ruzyně v kontextu stáže v BRD, Eichstättu, Nadace Hannse Seidela, mj. participace Kný.1999.

HRAZDÍRA Ivo a KNÝ Milan. ***Efektivnost krizového řízení a jeho závislost na kvalitě managementu***. Rkp. skript a slidy ke školení a dalšímu vzdělávání, 2000 - 2002.

Zákon o krizovém řízení, návrh. Připomínky, Kný, 1998 -99, také Víšek.

Institut krizového managementu. Zdeněk Kopecký, VŠE v Praze- Kunratice. ***Poslání Institutu.***

KNÝ M. ***Kriesenmanagement***. Kurz, 1997

On-scene Management for Hazardous Materials Emergrencies. Seminar for Central and Eastern European Nations, Praha, ČR, 1994. Canada/czech Republic - Sponsored, Emergency management Institute, Tederal Emergency Management Agency, Maryland, Colorado, USA. Případová studie.

PAPEŽ Jan. ***Činnost OkÚ a obcí v ochraně před povodněmi***. Podlklad pro přednášku. Institut pro místní správu MV ČR. 2000.

VÍŠEK Jiří st.. ***K pojetí předmětu Teorie řízení krizových situací ve výuce Policejní akademie České republiky***. Ústav bezpečnosní vědy a celoživotního vzdělávání, část z publikace (s. 139-152, patrně BTPx), 1994, z pramenů 1988, …1991-1994.

KASTOVÁ Verena. ***Krize a tvořivý přístup k ní.*** *Typy životních krizí, jejich dynamika a možnosti krizové intervence.* Praha, 2000,Portál, edice SPEKTRUM, 167 s., ISBN 80-7178-365-X, ORIGINÁL Der Schöpferische Sprung, Düsseldorf 1987.

Polizei - Management-Seminar, 6.-19. August 1995, Švýcarsko, Swarzenburg, *kurz pro důstojníky a instruktory Policie České republiky /účast mj. Kný/*

ADRESA

Ing. Milan KNÝ, CSc.
Policejní akademie ČR v Praze
Katedra managementu a informatiky
Lhotecká 559/7, 14301 Praha 4, P.O.BOX 54
Tel.: 974828211, kny@polac.cz

LEGISLATÍVNA ÚPRAVA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ REPUBLIKY
LEGISLATION IN THE FIELD OF CYBER SECURITY OF THE SLOVAK REPUBLIC

Milan MARCINEK

Akadémia Policajného zboru v Bratislave

Abstrakt: *Autor v štúdii popisuje aktuálnu situáciu v oblasti informačnej bezpečnosti na území Slovenskej republiky. Vysvetľuje definíciu pojmu informačnej (kybernetickej) bezpečnosti a kybernetického priestoru. Vzhľadom na skutočnosť, že kybernetická bezpečnosť na Slovensku dlho nemala jasne stanovených tvorcov, Koncepcia kybernetického zabezpečenia SR na roky 2015-2020 bola schválená až v polovici roku 2015. Ďalej autor vo svojej štúdii popisuje návrh zákona o kybernetickej bezpečnosti na území Slovenskej republiky. V kybernetickej bezpečnosti sa uplatňujú normy ISO/IEC 2700x, ktoré autor vo svojej štúdii tiež uvádza.*

Kľúčové slová: *kybernetická bezpečnosť, bezpečnosť, kybernetický priestor, dáta, informácie*

Abstract: *The author describes the current situation in the area of information security in the territory of the Slovak Republic in his study. He explains the definition of information (cyber) security and cyberspace. Due to the fact that cyber security has not been clearly identified for a long time in Slovakia, the Cyber Security Plan of the Slovak Republic for the period of 2015-2020 was approved only in the mid-2015. Furthermore, the author describes the draft bill on cyber security in the territory of the Slovak Republic in his study. In the cyber security the ISO IEC 2700x standards are also applied which the author also mentions in his study.*

Keywords: *cyber security, security, cyberspace, data, information*

ÚVOD

Kybernetický priestor má v súčasnosti vplyv na všetky zložky našej spoločnosti. V súčasnej informačnej spoločnosti slovo „kybernetický“ je synonymum pojmu „elektronicky spracúvaný“. Kybernetický priestor má teda svoju konkrétnu definíciu. Ide o *globálny dynamický otvorený systém, ktorý tvoria elektronické komunikačné siete, informačné systémy, ich programové vybavenie a údaje, ktoré sa pomocou nich spracovávajú, elektronické subsystémy riadiacich, výrobných, bezpečnostných a iných systémov a zariadení, činnosti, ktoré v jednotlivých častiach tohto systému prebiehajú, vzťahy a interakcie medzi časťami, prvkami a subsystémami tohto systému.*

Náš každodenný život závisí na informačných komunikačných technológiách. Otvorený kybernetický priestor sa aktívne presadzuje na celom svete. Aby tento priestor ostal slobodný, je potrebné uplatňovať rovnaké normy, zásady a hodnoty nielen na internete, ale aj mimo neho. Je potrebné zabezpečiť implementáciu vhodných opatrení ako sú procesy, postupy, politiky, softvérové a hardvérové funkcie.[1] Tieto normy sú príručkou pre podniky, ktoré sa snažia zaviesť systém informačnej bezpečnosti.

Informačná bezpečnosť avšak nie je manažérsky proces vytvárajúci zisk, ale v súčasnosti je nevyhnutným nástrojom pre bezproblémový chod procesov, ktoré sa na vytváraní zisku priamo podieľajú. Pod pojmom zisku sa myslí nielen hmotný, ale aj nehmotný majetok spoločnosti.

[1] Pre zavedenie systému manažérstva informačnej bezpečnosti boli vytvorené medzinárodné normy (štandardy) radu ISO/IEC 27000, ktoré špecifikujú požiadavky na riadenie informačnej bezpečnosti pre všetky typy a veľkosti organizácií.

KYBERNETICKÁ BEZPEČNOSŤ

Kybernetická bezpečnosť je pojem 21. storočia. Samotná podstata slova pochádza zo starogréckeho výrazu *kybernétes* = kormidelník. V spisoch starovekých spisovateľov sa uvádza kybernetika ako náuka o správnom riadení provincií. ktorý úzko súvisí s rozvojom informačných technológií.[1] Tento typ bezpečnosti definujeme ako *odvetvie výpočtovej techniky známej ako informačná bezpečnosť, ktoré je uplatňované ako u počítačov tak u sietí.*[2]

Kybernetická bezpečnosť musí byť založená na komplexnom prístupe, čo vyžaduje intenzívne zdieľanie informácií a koordináciu aktivít. Pri budovaní kybernetickej bezpečnosti je potrebné presadzovať spoluprácu medzi civilnými a ozbrojenými zložkami, verejným a privátnym sektorom a medzi národnými a medzinárodnými inštitútmi. Len takýmto spôsobom je možné zaistiť spoľahlivú prevádzku informačných a komunikačných infraštruktúr v kritických sektoroch, rýchle a efektívne reakcie na kybernetické útoky a odpovedajúcu legislatívnu ochranu v digitálnom svete. [3]

Za zakladateľa novodobej kybernetiky je považovaný americký matematik a filozof Norbert Wiener, ktorý v roku 1948 vydal knihu „Kybernetika, alebo riadenie a oznamovanie v živých organizmoch a strojoch“. V tejto knihe prvý raz použil názov kybernetika v novom, modernom slova zmysle. Moderná kybernetika vznikla postupne, čiastočnou fúziou niekoľkých vedných odborov, ako matematická logika, fyzika, evolučná biológia, neurológia a elektrotechnika.

KYBERNETICKÁ BEZPEČNOSŤ V SLOVENSKJE RPEUBLIKE

Kybernetická bezpečnosť veľmi dlho nemala jasne stanovených zodpovedných aktérov. Niektoré činnosti boli dvojité, iné sa podceňovali. Situáciu dobre ilustruje aj to, že doteraz pre túto oblasť chýba jednotná terminológia. Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 už obsahuje jasnú organizačnú štruktúru. [6]. Ku schváleniu došlo 17. júna 2015, vláda Slovenskej republiky schválila uznesením č. 328/2015 Koncepciu kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, ktorej cieľom bolo navrhnúť nový inštitucionálny rámec riadenia kybernetickej bezpečnosti v Slovenskej republike. Reagovala tak na prioritu návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sieťových a informačných systémov v Únii a na určenie vnútroštátneho príslušného orgánu pre bezpečnosť sieťových a informačných systémov.

Cieľom Koncepcie kybernetickej bezpečnosti Slovenskej republiky je dosiahnutie nasledujúcich stavov:

- Ochrana národného kybernetického priestoru je systémom fungujúcim koncepčne, koordinovane, efektívne, účinne a na právnom základe.
- Bezpečnostné vedomie všetkých zložiek spoločnosti sa systematicky zvyšuje.
- Súkromný a akademický sektor, ako aj občianska spoločnosť sa aktívne zúčastňuje na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti.
- Efektívna spolupráca je zabezpečená na národnej, ako aj medzinárodnej úrovni.
- Prijaté opatrenia sú primerané, uznávajú ochranu súkromia a základné ľudské práva a slobody. [7]

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, ktorý vláda Slovenskej republiky schválila dňa 2. marca 2016 uznesením č. 93/2016. Akčný plán obsahuje návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru štátu pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť Slovenskej republike nenahraditeľné škody, a tak by mohla byť narušená dôveryhodnosť štátu, či organizácie. Akčný plán ku Koncepcii je jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík, medzinárodnej spolupráce, zvyšovania povedomia a spôsobilostí, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného

kybernetického priestoru. Jednotlivé úlohy sú zoskupené v ôsmich prioritných oblastiach, s určením zodpovedného riešiteľa a spolupracujúcich subjektov, vrátane časového rámca ich realizácie.

Na Slovensku je kybernetická bezpečnosť zastrešená prostredníctvom CSIRT (*Computer Security Incident Response Team*). Ide o špecializovanú jednotku, ktorá je určená pre riešenie počítačových incidentov. Zabezpečuje služby spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich dôsledkov s následným obnovením činnosti informačných systémov. [7]

BEZPEČNOSŤ

Pojem „bezpečnosť" („*security*") pochádza z latinského *securitas* (sine cura + tutus) a čiastočne z nemeckého pojmu „*Sicherheit*". Tieto výrazy znamenajú bezstarostnosť, bezpečnosť, istotu, pokoj, ochranu a zabezpečenie. Ide o stav, v ktorom je zachovaná bezpečnosť, poriadok alebo je chránený život, zdravie, prostredie či majetok.

Bezpečnosť môže byť dynamická ako proces ľudskej činnosti alebo statická ako určitý momentálny stav. Vo význame vnútornej bezpečnosti ide o súhrn spoločenských vzťahov, ktoré upravuje právo a ktoré chránia práva a oprávnené záujmy fyzických a právnických osôb, záujmy spoločnosti a ústavné zriadenie, faktická úroveň, ako sa tieto vzťahy chránia, kategóriu, v ktorej sa rozumie bezpečnosť ako prípustná miera nebezpečenstva. V dynamickom vnímaní je to proces, ktorý zaisťuje neporušiteľnosť, nedotknuteľnosť (*safe*); ochranu (*protection*) a obranu (*defence*).

ŠTANDARDY KYBERNETICKEJ BEZPEČNOSTI

Dáta sa stávajú informáciami, keď získajú zmysel a hodnotu. Hodnotu informácií určuje vždy ich vlastník, pre ktorého informácie majú význam. Ak sú informácie dáta, ktoré majú vlastníka a hodnotu, potom informačná bezpečnosť znamená bezpečnosť týchto informácií. Platnou definíciou pre informačnú bezpečnosť je manažment hrozieb a rizík, ktoré pôsobia na informačné aktíva alebo manažment hrozieb a rizík, ktoré pôsobia na dáta.

Štandardy kybernetickej bezpečnosti boli vytvorené relatívne nedávno, pretože práve v posledných rokoch pribúda citlivých informácií uložených v počítačoch, ktoré sú pripojené k internetu. Tiež mnoho úloh, ktoré boli pôvodne spracovávané v papierovej forme sa dnes spracovávajú elektronicky. Zvyšuje sa potreba pre informačnú vierohodnosť a bezpečnosť. Dôležitým aspektom kybernetickej bezpečnosti je ochrana pred krádežou identity. [2] Inštitúcie a firmy majú zvýšenú potrebu k zaisteniu informačnej bezpečnosti. Narastá potreba chrániť obchodné tajomstvá, dôverné informácie a osobné údaje o zákazníkoch, zamestnancoch alebo obchodných partneroch. [2]

V rámci kybernetickej bezpečnosti sa aplikujú nasledovné normy, ktoré boli odvodené od štandardov BS 7799 vytvorených Britským štandardizačným inštitútom (BSI). Prvou je norma ISO/IEC 27001, ktorá poskytuje model pre zavedenie efektívneho systému riadenia bezpečnosti informácií (ISMS) v organizácii a dopĺňa tak normu ISO/IEC 27002. [2]

ISO/IEC 27001

Norma ISO/IEC 27001 poskytuje odporúčanie ako aplikovať ISO/IEC 27002 v rámci procesu ustanovenia, prevádzky, údržby a zlepšovania systému riadenia bezpečnosti informácií v organizácii v súlade so systémami riadenia kvality alebo bezpečnosti prostredia. Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je

- zaistenie kontinuity obchodných procesov,
- minimalizácia strát a
- maximalizácia návratnosti investícií.

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo

prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy. Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky

Predmetná norma teda popisuje vhodný systém riadenia, štruktúru a procesy pre riadenie bezpečnosti informácií podľa opatrení definovaných v ISO/IEC 27002. Systém manažérstva informačnej bezpečnosti podľa ISO 27001 je určený k ochrane informácií, čiže k zvládnutiu rizík, ktoré tieto informácie môžu eventuálne ohrozovať. Dôležitou súčasťou uvedenej normy je popis pre vybudovanie prevádzky systému riadenia bezpečnosti informácií. Organizácie musia realizovať analýzu rizík, aby bolo možné určiť špecificky optimálne bezpečnostné ciele a opatrenia, zaviesť ich a použiť podľa vlastných požiadaviek. Po identifikácii bezpečnostných cieľov je potrebné ich zrozumiteľne zdokumentovať pre všetky osoby v organizácii. Tieto podklady musia byť dostupné pre manažérov, zamestnancov a rovnako vybraným nezávislým stranám (interný audítori, certifikačný audítor, atď.).Norma ISO 27001 je takisto ako všetky ISO štandardy medzinárodne platným štandardom. Spoločnosť, ktorá získa certifikát v jednej krajine, nemusí opäť preukazovať splnenie požiadaviek v inej krajine.

ISO/IEC 27002:2013

ISO/IEC 27002:2013 je zbierka najlepších bezpečnostných praktík a môže byť využitá ako kontrolný zoznam všetkého správneho, čo je nutné pre bezpečnosť informácií v organizácii uskutočniť. Dokument je určený vedúcim a riadiacim zamestnancom, špecialistom a odborníkom pracujúcim v oblasti bezpečnosti informačných systémov, ako odborná publikácia, obsahujúca interpretáciu prístupu k zachovaniu dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore. Kybernetický priestor (cyberspace) je definovaný ako komplexné virtuálne prostredie, vyplývajúce z interakcie ľudí, softvéru a služieb na internete vykonávanej pomocou technológií, zariadení a sietí k nemu pripojených, nezávisle od ich fyzickej formy.

Ciele opatrení poskytujú kvalitný základ pre bezpečnostnú politiku. Nie všetky sú aplikovateľné v každej organizácii a môžu sa objaviť požiadavky na ich preformulovanie či prispôsobenie podľa aktuálnych potrieb organizácie. Väčšina z nich je však všeobecne aplikovateľná.[8]

Norma popisuje aj praktiky pre zaistenie bezpečnosti informácií, ktoré by organizácia mala brať do úvahy pre zaistenie kontrolných cieľov. Nová verzia normy obsahuje 113 základných opatrení, ktoré sa ďalej rozdeľujú na stovky špecifických bezpečnostných opatrení. [8] Rozhodnutie, ktoré opatrenia sa majú aplikovať je ponechané na organizácii. Vhodné opatrenia sú vyberané na základe hodnotenia rizík a ich implementácia je závislá na konkrétnej situácii. Cieľom nie je implementovať všetko, čo norma popisuje, ale skôr naplniť všetky aplikovateľné ciele opatrení. [8]

ISO 27032 - kybernetická bezpečnosť

ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity znamená v preklade „Informačné technológie - Bezpečnostné techniky - Návody pre kybernetickú bezpečnosť „

Ako už z názvu vyplýva, dokument je určený vedúcim a riadiacim zamestnancom, špecialistom a odborníkom pracujúcim v oblasti bezpečnosti informačných systémov, ako odborná publikácia, obsahujúca interpretáciu prístupu k zachovaniu dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore. Pričom kybernetický priestor (cyberspace) je definovaný ako komplexné virtuálne prostredie, vyplývajúce z interakcie ľudí, softvéru a služieb na internete

vykonávanej pomocou technológií, zariadení a sietí k nemu pripojených, nezávisle od ich fyzickej formy.

Právne akty, záväzné pre Slovenskú republiku z dôvodu členstva v Európskej únii, Organizácii pre ekonomickú spoluprácu a rozvoj, Organizácii Spojených národov a Organizácii Severoatlantickej zmluvy:

- Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 15), transponovaná do zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
- Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci spoločenstva pre elektronické podpisy (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 24), transponovaná do zákona č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 25), transponovaná do zákona č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Dohovor Rady Európy o počítačovej kriminalite z 23. novembra 2001, transponovaný do zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov; podpísali ho členské štáty Rady Európy a ďalšie účastnícke štáty a Slovenská republika ho podpísala a ratifikovala vo februári 2005,
- Nariadenie Komisie (ES) č. 831/2002 zo 17. mája 2002, ktorým sa vykonáva nariadenie Rady (ES) č. 322/97 o štatistike spoločenstva so zreteľom na prístup k dôverným údajom na výskumné účely (Mimoriadne vydanie Ú. v. EÚ, kap.1/zv.4),
- Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (Smernica o súkromí a elektronických komunikáciách) (Mimoriadne vydanie Ú. v. EÚ, kap.13/zv. 29), transponovaná do zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Dodatkový protokol k Dohovoru o počítačovej kriminalite o kriminalizácii činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov z 28. januára 2003; Slovenská republika ho zatiaľ neratifikovala,
- Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23. 12. 2008),
- Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa (Ú. v. EÚ L 337, 18. 12. 2009); smernica bude v roku 2011 transponovaná do novely zákona č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
- Nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 z 11. marca 2009 o európskej štatistike a o zrušení nariadenia (ES, Euratom) č. 1101/2008 o prenose dôverných

štatistických údajov Štatistickému úradu Európskych spoločenstiev, nariadenia Rady (ES) č. 322/97 o štatistike Spoločenstva a rozhodnutia Rady 89/382/EHS, Euratom o založení Výboru pre štatistické programy Európskych spoločenstiev (Ú. v. EÚ L 87, 31. 3. 2009).

Z informačno-bezpečnostného hľadiska sú príslušné nielen všetky zákonné normy, ktoré upravujú podmienky používania informačných a komunikačných technológií, ale aj tie, ktoré umožňujú spracovanie informácií v elektronickej podobe.

VÝVOJ PRÁVNEJ ÚPRAVY

Informačná bezpečnosť je pojem, ktorý zatiaľ nie je v Slovenskej republike v primeranej miere premietnutý do legislatívy. Napriek tomu má informačná bezpečnosť oporu v legislatíve, ako aj v strategických a koncepčných dokumentoch schválených vládou Slovenskej republiky. Informatizácia spoločnosti a s ňou súvisiaca informačná bezpečnosť verejnej správy je vymedzená zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Ochrana utajovaných skutočností predstavuje klasifikovanú informáciu a systémy pracujúce s klasifikovanou informáciou. Utajované skutočnosti sú klasifikované z hľadiska dôvernosti, pričom bezpečnostné požiadavky na ich ochranu sú komplexné a zohľadňujú najmä potrebu zaistenia integrity a dostupnosti údajov. Ochrana osobných údajov a používanie elektronického podpisu sú upravené osobitnými predpismi a príslušné inštitúcie zabezpečujú dohľad nad ich dodržiavaním. Elektronický obchod upravuje zákon č. 22/2004 Z. z. o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Počítačovú kriminalitu upravuje § 247 zákona č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov, do ktorého sú premietnuté princípy Dohovoru o kybernetickom zločine CETS č. 185/2001, vydanom Radou Európy.

HLAVNÉ DÔVODY NA VYPRACOVANIE ZÁKONA O INFORMAČNEJ BEZPEČNOSTI

Prakticky všetky dôležité oblasti života spoločnosti v súčasnosti podstatne závisia od spoľahlivého fungovania systémov jej digitálneho priestoru, a preto zaistenie primeranej ochrany digitálneho priestoru je prioritným záujmom Slovenskej republiky. Keďže narušenie alebo zlyhanie jednej časti digitálneho priestoru môže ohroziť inú jeho podstatnú časť, alebo aj celý digitálny priestor, zaistenie informačnej bezpečnosti digitálneho priestoru musí byť trvalé a komplexné, a to si vyžaduje systematický, koordinovaný a legislatívne podporený prístup všetkých zainteresovaných subjektov. Štát môže bezprostredne zaisťovať ochranu informačných systémov verejnej správy, z ktorých sú mnohé pre riadenia a chod štátu kľúčové. Množstvo dôležitých informačných a komunikačných technológií digitálneho priestoru Slovenskej republiky je však v súkromnom vlastníctve a štát nemá iné ako právne nástroje na presadenie potrebných bezpečnostných opatrení na ochranu týchto systémov. Súčasný právny poriadok Slovenskej republiky síce obsahuje viacero právnych noriem, ktoré riešia čiastkové problémy, a tak pokrývajú špecifické oblasti informačnej bezpečnosti, ale jednotný, všeobecný právny predpis pre informačnú bezpečnosť digitálneho priestoru v slovenskej legislatíve chýba. Absencia takého zákona sa prejavuje napríklad v nekonzistentnosti terminológie, nedostatočnom používaní bezpečnostných štandardov, v prekrývajúcich sa kompetenciách štátnych orgánov a v neúplnosti pokrytia informačnej bezpečnosti právnymi predpismi a kompetenciami. Ďalším dôsledkom neúplného a nekonzistentného právneho rámca informačnej bezpečnosti je to, že sa ochrana informačných a komunikačných systémov v Slovenskej republike riadi rôznymi právnymi predpismi alebo je celkom ponechaná na uváženie ich vlastníkov a správcov. Výsledkom toho je rôznorodá, nekompatibilná a často nedostatočná úroveň ochrany informačných a komunikačných technológií, čo okrem vlastného ohrozenia a ohrozenia digitálneho priestoru znižuje možnosť ich bezpečnej kooperácie a efektívnejšieho využívania existujúcich informačných zdrojov a výpočtových kapacít.

Na druhej strane absencia alebo nejednoznačnosť právnych predpisov môže viesť k uplatňovaniu ekonomicky náročných ale pritom neadekvátnych bezpečnostných riešení. Preto je potrebné vytvoriť klasifikačnú schému informačných a komunikačných technológií a ustanoviť minimálne požiadavky na ochranu ich jednotlivých kategórií. Digitálny priestor Slovenskej republiky je súčasťou globálneho, celosvetového digitálneho priestoru. Vďaka vzájomnej previazanosti informačných a komunikačných technológií je nevyhnutná aj medzinárodná koordinácia ochrany globálneho digitálneho priestoru. Na riešenie bezpečnostných problémov digitálneho priestoru bola zriadená uznesením vlády č. 479/2009 jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike. Aby si táto jednotka pre riešenie počítačových incidentov mohla plniť stanovené úlohy v domácom aj medzinárodnom meradle, je potrebné legislatívne vymedziť jej kompetencie a vzťahy k ostatným štátnym orgánom Slovenskej republiky. S postupujúcou informatizáciou spoločnosti narastá počet informačných a komunikačných technológií a používateľov služieb informačnej spoločnosti. Potrebnú úroveň ochrany digitálneho priestoru nie je možné dosiahnuť bez dostatočného bezpečnostného povedomia používateľov a udržiavania primeraných znalostí tých, ktorí informačné a komunikačné technológie spravujú a rovnako aj tých, ktorí zodpovedajú za ich ochranu. Je potrebné stanoviť minimálne kvalifikačné požiadavky z informačnej bezpečnosti na informatikov a bezpečnostných špecialistov. Rozvoj a nasadzovanie informačných a komunikačných technológií otvára neustále nové bezpečnostné otázky, ktoré je potrebné analyzovať a prijímať primerané riešenia ešte pred tým, ako nedostatky týchto technológií spôsobia bezpečnostné problémy pri ich používaní. Zákon by mal ustanoviť, kto bude zbierať a spracovávať informácie o nedostatkoch informačných a komunikačných technológií, komu, v akom rozsahu a akým spôsobom sa tieto informácie budú poskytovať. Úlohy spojené s ochranou digitálneho priestoru Slovenskej republiky plnia rôzne štátne aj neštátne inštitúcie a s prehlbujúcou sa informatizáciou spoločnosti budú pribúdať ďalšie úlohy. Súčinnosť inštitúcií podieľajúcich sa na ochrane digitálneho priestoru bude potrebné koordinovať. Zo zodpovednosti za informatizáciu spoločnosti vyplýva pre Ministerstvo financií Slovenskej republiky

Národný bezpečnostný úrad, ako ústredný organ štátnej správy pre kybernetickú bezpečnosť, pripravil na základe schváleného programového vyhlásenia vlády Slovenskej republiky na roky 2016-2020 a v súlade so schválenou Koncepciou kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a Akčným plánom realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“), ktorým do národného právneho poriadku transponuje 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 (ďalej len „smernica NIS“).

Siete a informačné systémy hrajú zásadnú úlohu pri slobodnom pohybe a často sú prepojované a spájané internetom, ako globálnym nástrojom. Narušenie siete a informačných systémov v jednom členskom štáte sa preto dotýka ďalších členských štátov a celej Európskej únie. Odolnosť sietí a stabilita informačného systému je preto základným predpokladom hladkého a nerušeného fungovania vnútorného trhu Európskej únie a predpokladom dôveryhodnej medzinárodnej spolupráce.

Smernica NIS predstavuje prvú celoeurópsku legislatívnu úpravu v oblasti kybernetickej bezpečnosti, ktorá sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov, zvyšuje ich vzájomnú koordináciu a predstavuje bezpečnostné podmienky pre kľúčové sektory.

Cieľom smernice NIS je zaručiť spoločnú bezpečnosť sietí a informačných systém v rámci Európskej únie, prostredníctvom zvýšenia bezpečnosti internetu a súkromných sietí a informačných systémov, na ktorých je do značnej miery postavené fungovanie hospodárskych a spoločenských záujmov.

Významným subjektom na poli kybernetickej bezpečnosti v Európskej únii je Európska agentúra pre bezpečnosť sietí a informácií (ENISA), ktorá prispieva k zabezpečovaniu vysokého

stupňa bezpečnosti a v spolupráci s európskymi krajinami vytvára spoločnú kultúru bezpečností sietí a informačných systémov v Európskej únii.

Povinnosti členských štátov vyplývajúce zo smernice NIS sú nastavené na najnižšej prijateľnej úrovni nevyhnutnej k dosiahnutiu požadovanej pripravenosti a k zabezpečeniu medzištátnej spolupráce založenej na dôvere. Členské štáty môžu v rámci prijatých opatrení zohľadňovať svoje vnútroštátne špecifiká a každý členský štát v tomto smere transponuje smernicu NIS s ohľadom na reálne, skutočné riziká vyskytujúce sa v spoločnosti.

Smernica NIS najmä:

- zavádza bezpečnostné požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb (ďalej len „PZS“) a pre poskytovateľa digitálnych služieb (ďalej len „PDS“),
- 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, s cieľom podporovať strategickú spoluprácu a výmenu informácii medzi členskými štátmi a budovať vzájomnú dôveru,
- stanovuje sieť jednotiek CSIRT, ktorej účelom je prispievať k budovaniu dôvery medzi členskými štátmi a podporovať účinnú spoluprácu.

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI

Základným cieľom Zákona o kybernetickej bezpečnosti je zvýšiť bezpečnosť kybernetického priestoru a predovšetkým sa snažiť ochrániť tú časť infraštruktúry, ktorá je pre fungovanie štátu dôležitá a ktorej narušenie by viedlo k poškodeniu alebo ohrozeniu záujmov štátu. [4]

Hlavným legislatívnym východiskom návrhu zákona je Stratégia pre informačnú bezpečnosť v Slovenskej republike (Uznesenie vlády SR č. 270/2008), Legislatívny zámer zákona o informačnej bezpečnosti (Uznesenie vlády SR č. 136/2010) a Uznesenie vlády SR č. 328/2015 ku Koncepcii kybernetickej bezpečnosti.

V nadväznosti na Legislatívny zámer návrhu zákona o informačnej bezpečnosti, v ktorom boli stanovené okrem čiastkových cieľov dva základné okruhy problémov, a to zaistenie ochrany pre informačné systémy verejnej správy a vytvorenie všeobecného právneho rámca pre ochranu celého digitálneho priestoru Slovenskej republiky, je aj v súlade s naplnenými cieľmi smernice NIS možné konštatovať, že návrh zákona o kybernetickej bezpečnosti komplexne a vyčerpávajúcim spôsobom rieši všetky relevantné otázky.

Príprave návrhu zákona predchádzala široká odborná diskusia. Národný bezpečnostný úrad v rámci príprav organizoval workshopy na tému transpozície smernice NIS do národného právneho poriadku, prebiehali konzultácie s akademickou obcou aj odbornou verejnosťou, boli zriadené príslušné pracovné skupiny. Zákon bol teda vypracovaný aj na základe podnetov a po konzultáciách s orgánmi verejnej moci, ktoré sa k navrhovaným zmenám a oblastiam úprav vyjadrili, ako aj na základe podnetov a diskusií so zástupcami odbornej verejnosti.

Cieľom návrhu zákona je vytvoriť funkčný legislatívny rámec nevyhnutný pre efektívnu realizáciu kľúčových opatrení pre bezpečnosť národného kybernetického priestoru, ktorý transponuje priority a požiadavky, ktoré boli vytvorené na európskej úrovni a prijaté všeobecným konsenzom prostredníctvom smernice NIS.

Medzi hlavné oblasti úpravy návrhu zákona v nadväznosti na smernicu NIS patrí oblasť

- organizácie a pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- národnej stratégie kybernetickej bezpečnosti,
- jednotného informačného systému kybernetickej bezpečnosti,
- postavenia a povinnosti PZS a PDS,

- organizáciu a pôsobnosť jednotiek CSIRT a ich akreditáciu,
- systému zabezpečenia kybernetickej bezpečnosti a minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti,
- kontroly a auditu.

Okrem uvedených okruhov návrh zákona rieši aj niektoré ďalšie požiadavky smernice NIS, ako je napríklad vymedzenie medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti, plnenie notifikačných povinností, nahlasovanie kybernetických bezpečnostných incidentov ako aj dobrovoľné nahlasovanie kybernetických bezpečnostných incidentov, podporuje výskum a vzdelávanie ako aj zvyšovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

Návrh zákona v jednotlivých článkoch novelizuje právne predpisy, ktorých zmena je z dôvodu dostatočnej transpozície nevyhnutná. Ide najmä o zákon č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov, zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov, zákon č. 45/2011 Z. z. o kritickej infraštruktúre, zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov a zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Návrh zákona ďalej komplexným spôsobom rieši odmeňovanie zamestnancov na strane štátu tak, aby bol štát schopný zamestnať odborníkov v oblasti kybernetickej bezpečnosti a tým konkurovať súkromným zamestnávateľom. V súvislosti so zavedením nového správneho poplatku rovnako dochádza k doplneniu zákona č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov.

Vzhľadom na predpokladanú dĺžku legislatívneho procesu a berúc do úvahy potrebnú legis vakanciu sa navrhuje, aby zákon nadobudol účinnosť 1. marca 2018. Ustanovenia, ktoré zakladajú povinnosti, vyžadujúce si prípravu a implementáciu sa navrhujú ustanoviť s odloženou účinnosťou.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, nálezmi Ústavného súdu Slovenskej republiky, so zákonmi, ako aj s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná a s predpismi Európskej únie.

Prijatie navrhovaného zákona nemá sociálne vplyvy, ani vplyvy na životné prostredie ani na služby verejnej správy pre občana, bude mať pozitívne vplyvy na informatizáciu spoločnosti, avšak bude mať negatívne vplyvy na podnikateľské prostredie a na rozpočet verejnej správy.

Cieľom tohto zákona nie je riešiť všetky riziká v kyberpriestore, napr. porušovanie autorských práv, podvodné aktivity, úniky elektronických dát či šírenie chybného elektronického obsahu a pod. [4] Zákon je postavený na dvoch základných zásadách, a to na zásade minimalizácie zásahov do práv súkromnoprávnych subjektov a na zásade individuálnej zodpovednosti za bezpečnosť informačných systémov. [5]

Štát ako taký je povinný zaisťovať primeranú ochranu informačných a komunikačných technológií, ktoré sú v pôsobnosti štátnych orgánov a orgánov samosprávy. Cieľom zákona je vytvoriť ucelený, koordinovaný a efektívny systém ochrany informačných systémov Slovenskej republiky. Keďže informačné systémy sú súčasťou širšieho digitálneho priestoru, ktorého značná časť je v súkromných rukách, zákon vytvára podmienky na zvyšovanie úrovne informačnej bezpečnosti v celom digitálnom priestore Slovenskej republiky prostredníctvom štandardizácie informačnej bezpečnosti.

ZÁVER

Kybernetická bezpečnosť je jednou zo špecifických oblastí informačnej bezpečnosti. Odborná disciplína informačná bezpečnosť sa zaoberá otázkou zaručenia dôvernosti, integrity, dostupnosti a sledovateľnosti informačných aktív všeobecne, zatiaľ čo kybernetická bezpečnosť sa venuje bezpečnosti iba určitej časti informačných aktív, ktoré sú spracúvané vo virtuálnom priestore, kybernetickom priestore. Siete a informačné systémy hrajú významnú úlohu pri slobodnom pohybe a často sú spájané internetom ako svetovým nástrojom. Narušenie siete a informačných systémov v jednom členskom štáte sa dotýka ďalších členských štátov a celej Európskej únie. Odolnosť sietí

a stabilita informačného systému je základným predpokladom hladkého a nerušeného fungovania vnútorného trhu Európskej únie a predpokladom dôveryhodnej medzinárodnej spolupráce.

Investovanie do kybernetickej bezpečnosti znamená investície do budúcnosti a ekonomického rastu štátu. Úroveň kybernetickej bezpečnosti je súhrnom všetkých národných a medzinárodných opatrení, ktoré boli prijaté k ochrane dostupnosti informácií komunikačných technológií a integrity, autenticity a dôvernosti dát v kybernetickom priestore.

V súčasnosti neexistuje taká činnosť vo svete, ktorá by nemohla byť ovplyvnená prostredníctvom aktivít v kybernetickom priestore. Oblasť informačných technológií prenikla do všetkých oblastí života - do národnej obrany, páchanej kriminálnej činnosti, do kritickej infraštruktúry, do služieb ochrany života a zdravia občanov a pod. Je potrebné však uviesť, že technická normalizácia v informačnej bezpečnosti sa nezaoberá niektorými špecifickými odvetviami - najmä kriminalistikou a národnou obranou. Vzhľadom na vysokú úroveň špecializácie uvedených odvetví, tieto činnosti sú prirodzene ponechané na rozvoj vlastných samostatných odvetví. Stále sú to však odvetvia odvodené z informačnej bezpečnosti, pretože objektom ochrany je zaručenie bezpečnosti informácií, ktoré tieto odvetvia spracúvajú.

POUŽITÁ LITERATÚRA

[1] Linuxservices. Kybernetická bezpečnost [online]. 2016 [cit. 2016-02-09]. Dostupné z: https://www.linuxservices.cz/kyberneticka-bezpecnost.

[2] Cybersecurity. Cyber Security (Kybernetická bezpečnost) [online]. 2010 [cit. 2016-02-09]. Dostupné z: http://www.cybersecurity.cz/basic.html

[3] Národní centrum kybernetické bezpečnosti. Strategie pro oblast kybernetické bezpečnosti Ř na období 2012 - 2015 [online]. 2011 [cit. 2016-02-09]. Dostupné z: https://www.govcert.cz/download/nodeid-727/

[4] T-soft. Zákon o kybernetické bezpečnosti [online]. 2014 [cit. 2016-02-09]. Dostupné z: http://www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/

[5] Epravo. Zákon o kybernetickej bezpečnosti [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.epravo.sk/top/clanky/zakon-o-kybernetickej-bezpecnosti758.html

[6] Kybernetická bezpečnosť na Slovensku a v Európe. EurActiv [online]. 2003 [cit. 2016-02-09]. Dostupné z: http://euractiv.sk/veda-a-inovacie/kybernetickabezpecnost-na-slovensku-a-v-europe-000338/

[7] Rokovania. Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020 [online]. 2010 [cit. 2016-02-09]. Dostupné z: http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum187874?prefixFile=m_

[8] RiskAnalysisConsultants. ISO/IEC 27002:2013 [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27002

[9] Iso27001security. ISO/IEC 27001:2013 Information technology [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.iso27001security.com/html/27001.html

[10] Kiwiki. Systém manažérstva informačnej bezpečnosti [online]. 2011 [cit. 2016-02-09]. Dostupné z: http://www.kiwiki.info/index.php/Syst%C3%A9m_mana%C5%BE%C3%A9rstva_informa%C4%8Dnej_bezpe%C4%8Dnosti

[11] ISO Auditor. Systém manažérstva informačnej bezpečnosti [online]. 2016 [cit. 2016-02-09]. Dostupné z: http://www.isoauditor.sk/iso-iec-27001

[12]MARCINEK, M. MARKOVÁ, I. Working Effectiveness of Hydraulic Rescue Equipments for Firefighters In: Advanced Materials Research. - ISSN 1022-6680. - Vol. 1001 (2014), pp. 517-525. Plnýtext:<Spôsobprístupu:http://www.scopus.com/record/=Working+effectiveness+of+hydraulic+rescue+equipments+for+firefighters&sid=5AE8CD94DF72E1297BF6E9BA302CACDA.kq

[13]MARCINEK, M. - DWORZECKI, J. Technical Aspects of use of Selected Specialist Equipment Intended for Road-Side Rescuing, 1. edition. - New York: Iglobal Writer Inc., Pro Pomerania Foundation Poland, 2015. - 175 s. - ISBN 978-83-63680-77-0.

[14]MARCINEK, M. Linka tiesňového volania eCall v podmienkach Slovenskej republiky/The emergency line eCall in the Slovak Republic. In: Bezpečnostné fórum 2015. I. zväzok : zborník vedeckých prác. - Banská Bystrica : Belianum. Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, 2015. - ISBN 978-80-557-0849-2. - S. 161-165.

[15]MARCINEK, M. Analýza zodpovednosti pri preprave nebezpečných látok cestnou nákladnou dopravou podľa Dohody ADR a Dohovoru CMR = Responsibility Analysis in the Transport of Dangerous Substances by Road under the ADR Agreement and CMR Convention In: Ochrana obyvatelstva - Nebezpečné látky 2017 [elektronický zdroj] : sborník přednášek XVI. ročníku mezinárodní konference : [1. - 2. únor 2017, Ostrava]. - ISSN 1803-7372. - č. 1 (2017), CD-ROM, s. 90-97.

[16]MARCINEK, M The Current Situation in Vehicle Safety System In: "Dani Arčibalda Rajsa" = "Archibald Reiss Days" : tematski zbornik radova medunarodnog značaja = Thematic Conference Proceedings of International Significance : Tom II = Volume II : Beograd, 10 - 11. mart 2016 = Belgrade, 10 - 11 March 2016. - Beograd = Belgrade : Kriminalističko-policijska akademija = Academy of Criminalistic and Police Studies, 2016. - ISBN 978-86-7020-357-0. - pp. 462-472.

ADRESA

mjr. Ing. Milan MARCINEK, PhD.
Akadémia Policajného zboru v Bratislave
Katedra verejnej správe krízového manažmentu
Sklabinská 1, 835 17 Bratislava
e-mail: mílan.marcinek@minv.sk

RIADENIE KYBERNETICKEJ BEZPEČNOSTI VO VEREJNEJ SPRÁVE

Igor PAVLOVIČ

Akadémia Policajného zboru v Bratislave

Abstrakt: *Narastajúce nároky a zvyšujúci sa počet kybernetických útokov núti spoločnosti využívajúce informačné technológie, aby sa vopred pripravili na prípadné incidenty počítačovej bezpečnosti ohľadne únikov, prípade zmeny alebo dokonca straty údajov. Vhodná stratégia zverejňovania incidentov môže výrazne zlepšiť včasnosť a účinnosť činností súvisiacich s reakciou na incidenty a tým obnoviť dôveru zainteresovaných strán spoločnosti. V tomto článku sú uvedené štyri faktory, ktoré určujú organizačné preferencie týkajúce sa informácií o incidentoch. Spolu vytvárajú súbor apelov pre spoločnosť pri rozhodovaní o tom, kto a kedy k akým informáciám pristupuje, čo a ako spracováva o incidentoch počítačovej bezpečnosti. Ďalej je popísaný rámec na podporu rozhodovania, ktorý poskytuje organizáciám a spoločnostiam postup, kde sa krok za krokom hovorí o riešení týchto problémov a vypracuje vhodnú stratégiu zverejňovania incidentov..*

Kľúčové slová: *informačný systém, Bezpečnostný incident, verejná správa, krízový manažment.*

ÚVOD

Zvyčajne každou činnosťou, ktorá je vykonávaná v organizácií vzniká potreba o tejto činnosti zapisovať údaje. Tieto údaje sú následne uchovávané a spracovávané. Spracovávaním a uchovávaním týchto údajov sa zaoberá tím ľudí vo vnútri spoločnosti, niekedy aj mimo nej. Potreba spracovávania týchto údajov je nutná z dôvodu bezpečnosti a ochrany organizácie. Väčšina údajov je spracovávaná v informačných systémoch organizácie. Informačný systém musí byť organizovaný celok získavania, prenášania, spracovania, ukladania a poskytovania skutočností i myšlienok v predpísanej podobe tak, aby bolo možné nevyhnutné informácie uchovávať, prenášať a spracovávať ku uspokojovaniu zamestnancov pre dosiahnutie určitého cieľa.[1] Útoky a poškodzovanie týchto údajov sú vyhodnotené ako bezpečnostný incident, ktorý môže ohroziť obmedziť chod organizácie. V závislosti od typu organizácie a využívania informačných systémov. Zverejňovanie informácií o incidentoch je z toho dôvodu nevyhnutnou súčasťou krízovej komunikácie, ktorá môže zmierniť a obmedziť škody spôsobené v organizácií, poskytnúť konkrétne informácie zainteresovaným subjektom, umožní uskutočniť opravy a obnovu zabezpečenia organizácie, resp. jej informačného systému.

V niektorých prípadoch je snaha organizácií nezverejniť vznik incidentu. Tieto organizácie sa vystavujú riziku odhalenia tretími stranami. V týchto prípadoch môžu byť škody omnoho väčšie, ako zverejnenie rizika. Vo svete sa organizácie už desiatky rokov pripravujú a riadia príslušnými internými a národnými smernicami. Na Slovensku platí od marca 2014 výnos Ministerstva Financií Slovenskej Republiky o štandardoch pre informačné systémy verejnej správy. Tento výnos definuje nielen štandardy používania dátových formátov, ale definuje aj postupy v oblasti dátovej bezpečnosti, takzvané bezpečnostné štandardy. Nedostatočné postupy na zabezpečenie včasnej a dôslednej komunikácie so zainteresovanými stranami môžu viesť k škodlivým až likvidačným následkom. Zlá komunikácie môže prispieť k celkovému zmätku, vyvolaniu nedôveryhodnej povesti, v prípade komerčných organizácií

môže viesť k predaju akcií, v prípade štátnych inštitúcií k nedôvere voči zodpovedným funkcionárom. Napriek tomu včasná komunikácia a odhalenie môže pomôcť a aktivovať interné a externé zainteresované strany, odhalený incident analyzovať a uskutočniť rázne a správne

[1] SUJA, M. Súčasný stav a perspektívy rozvoja informačného systému Hasičského. In Perspektívy rozvoja verejnej správy v krajinách Európskej únie : zborník z celoštátneho vedeckého seminára s medzinárodnou účasťou konaného dňa 10.04.2012 na Akadémii Policajného zboru v Bratislave. Bratislava 2012. ISBN 978-80-8054-535-2, s. 29-34.

rozhodnutia. Takýmto postupom sa zvýši dôveryhodnosť a celková transparentnosť organizácie. Plán zverejnenia bezpečnostných incidentov zaručí výhody a obmedzí šancu na ďalšiu eskaláciu incidentov. Článok je zameraný na zadefinovanie algoritmu na podporu rozhodovania, ktorý poskytne organizáciám jasné usmernenie pri tvorbe primeranej stratégie zverejňovania incidentov. Z tohto dôvodu sa identifikuje, označí súbor faktorov, ktoré ovplyvňujú organizačné preferencie týkajúce sa zverejňovania informácií o incidentoch. V časti 3 sú skombinované so štyrmi rôznymi strategickými otázkami za účelom vytvorenia prehľadu výziev týkajúcich sa zverejňovania informácií. V poslednej časti bude pridaný časový rozmer, ktorý nakoniec vyústi do rámca uverejneného incidentu.

ČINITELE VPLÝVAJÚCE NA ZVEREJNENIE INCIDENTU

Spoločnosti zverejňujú, resp. nezverejňujú informácie o bezpečnostných incidentoch kybernetickej bezpečnosti z rôznych dôvodov. Ako bolo spomenuté, pri bankách, prípadne poisťovniach a iných finančných inštitúciách môže strata dôvery odlákať klientov a spôsobiť bankrot spoločnosti, pri štátnych inštitúciách nedôveru občanov v štát. V poslednej dobe vznikajú spoločnosti zaoberajúce sa bezpečnosťou informačných systémov a súčasne sú zavádzané interné normy organizácie týkajúce sa počítačovej a kybernetickej bezpečnosti. Zaoberanie sa problematikou bezpečnostných incidentov je odôvodnené a determinované tromi hlavnými faktormi. Regulačnými, ekonomickými a reputačnými. Napriek tomu samotný proces reakcie na incident môže slúžiť ako motivácia na zverejnenie informácií o bezpečnostných incidentoch. Stále viac dokumentov o bezpečnostných incidentoch zdôrazňuje, že zdieľanie informácií je kľúčovým prvkom úspešného zmiernenia škôd spôsobených bezpečnostnými incidentmi a tiež znižovania pravdepodobnosti ich výskytu v budúcnosti. V čase, keď spoločnosti chýbajú skúsení zamestnanci, ktorí dokážu riešiť celý rozsah možných bezpečnostných incidentov, môže sa zdieľanie informácií o bezpečnostných incidentoch medzi napádanými spoločnosťami a štátnymi inštitúciami stať úspešným prvkom obrany voči týmto útokom. V dôsledku toho, okrem troch faktorov, ktoré už boli spomenuté, zmierňovanie škôd a prevencia môžu slúžiť aj ako rozhodujúce faktory stratégie zverejňovania incidentov spoločnosti v oblasti kybernetickej bezpečnosti. Z toho dôvodu je zrejmé, že stratégia zverejňovania informácií môže byť ovplyvnená štyrmi faktormi: Zmierňovanie škôd a prevencia, súlad s predpismi, ekonomická nákladovosť a efektívnosť a povesť.

PROBLÉMY PRI OZNAMOVANÍ POČÍTAČOVÝCH INCIDENTOV

Štyri uvedené faktory popísané v predchádzajúcej kapitole by mali brať do úvahy zodpovední pracovníci organizácie alebo inštitúcie, keď dôjde k incidentu počítačovej bezpečnosti s možným vysokým vplyvom na organizáciu. Zodpovedné osoby by mali adekvátne k incidentu reagovať a vyvolať primeranú reakciu. Okrem iného musia čo najskôr posúdiť situáciu a vykonať súbor adekvátnych rozhodnutí s cieľom zmierniť možný vplyv tohto incidentu. Druhý spomenutý faktor zahŕňa implementáciu vhodného prístupu k zverejňovaniu informácií. Pokiaľ ide o zverejňovanie informácií, organizácia, v ktorej došlo k incidentu,

začína čeliť problémom s rozhodovaním o publikovaní - oznámení a načasovaní oznámení, o obsahu oznámenia a o spôsobe zverejnenia informácií. Relevantné otázky môžu byť zoskupené do nasledujúcich kategórií: Kategória "Kto" sa vzťahuje na informovanie o incidentoch . Môžu to byť rôzne subjekty, ako sú zákazníci, dodávatelia a partneri spoločnosti; prípadne organizácie verejnej správy, Ďalej to môžu byť subjekty, ktoré pomáhajú spoločnosti reagovať na počítačový útok; vládne a štátne spoločnosti a agentúry, média a širokej verejnosť. Kategória "Kedy" označuje časové rozvrhy, keď sa zverejňujú informácie o bezpečnostných incidentoch. Zahŕňa spúšťače oznámení, rýchlosť zverejňovania informácií a frekvenciu aktualizácií informácií. Kategória "Čo" opisuje obsah toho, čo sa zverejňuje - množstvo informácií, ktoré sa majú uverejniť, ako aj presná správa. Kategória "Ako" odkazuje na metódy, pomocou ktorých sú zverejnené informácie o bezpečnostných incidentoch.

ČASOVÁ OS OZNÁMENIA GENERICKÉHO INCIDENTU

Vytvorenie časovej osi procesu zverejňovania incidentov je východiskovým bodom pri navrhovaní algoritmu na podporu rozhodovania. Časová línia umožňuje v čo najväčšej možnej miere vymedziť spoločné kroky procesu zverejňovania incidentu a použiť ich ako základný postup. Časová os znázorňuje hlavné činnosti oznamovania incidentov, interné aj externé s ohľadom na vyvíjajúci sa životný cyklus incidentu. Každá udalosť je jedinečná a riadená iným spôsobom. Existujú však určité kroky, ktoré zostávajú relatívne nemenné pri každom počítačovom bezpečnostnom incidente.

Krok 1.: Posúdenie vplyvu havárie a vytvorenie reakčného tímu na incident s cieľom iniciovať proces nápravy a zmieriť následky škôd.

Krok 2.: Ďalšie hodnotenie o podrobnostiach týkajúcich sa mimoriadnych udalostí, ako aj o organizačných prioritách týkajúcich sa reakcií na incidenty.

Krok 3.: Vývoj a realizácia stratégie zverejňovania incidentov na základe prechádzajúceho hodnotenia.

Krok 4.: Poučenie sa z incidentu po zverejnení.

Tieto kroky spoločne tvoria základ pre návrh postupu opísaný v ďalšej kapitole.

ALGORITMUS PODPORY ROZHODOVANIA

Keď dôjde k skutočnej udalosti, incidentu, spoločnosť postupuje podľa vopred definovanej časovej línie tak, aby čo najefektívnejšie odstránila škody spôsobené incidentom podľa postupov navrhnutých v rámci rozhodovacieho procesu. V nasledujúcich častiach je opísaný každý krok rozhodovacieho procesu, kde bude vysvetlené, ako funguje každý proces.

a.) potvrdenie bezpečnostného incidentu

V prvej fáze sa incident potvrdzuje buď interným skúmaním, alebo oznámením od externých subjektov.

b.) posúdenie straty dôvery, integrity a dostupnosti

Každá organizácia, spoločnosť môže mať zadefinované rôzne mať zadefinované rôzne postupy pri posudzovaní vplyvu incidentu na jej chod. Závisí to od druhu spoločnosti a jej predmetu činnosti. Všeobecne je dopad incidentu zachytený pomocou posúdenia vplyvu dôvernosti, integrity a dostupnosti, ktoré odrážajú vplyv straty dôvery, integrity a dostupnosti informačných systémov spoločnosti. Pre efektívnu a správnu tvorbu postupov môže spoločnosť vypracovať hodnotenie vplyvu, ktoré zohľadňuje dôvernosť, integritu a dostupnosť dôležitých serverov alebo systémov, ktoré v prípade incidentu okamžite zvýšia úroveň dopadu na maximálnu hodnotu. Zoznam všetkých serverov a systémov s ich úrovňou dôležitosti by mal byť vypracovaný vopred v rámci bezpečnostného projektu pre neskoršie použitie. Zloženie IRT (tím reakcie na incidenty).

c.) tím zamestnancov reagujúci na incidenty

Organizácie by mali mať vopred definovaný zoznam zamestnancov, ktorí sa podieľajú, reagujú na incidenty v závislosti od ich typu a úrovne vplyvu. V prípade pokročilých incidentov v oblasti kybernetického zabezpečenia by mal byť tím tvorený z viacerých oblastí spolupracovať s koordinátormi od menežmentu incidentov, oddelenia ochrany osobných údajov, komunikačného oddelenia spoločnosti, vrcholového menežmentu a právneho zastúpenia spoločnosti.

d.) dotazník o špecifických incidentoch

Po vytvorení počiatočného tímu reagujúceho na incidenty je potrebné vyriešiť, či sa na jeho riešenie vyžadujú interní špecialisti a či je potrebné externé zverejnenie. Odpovede na špecifické otázky závisia od konkrétneho incidentu a preto je potrebné proces vopred definovať tak, aby zahŕňal všetky kľúčové detaily incidentu, ktoré ovplyvňujú rozhodnutie o poskytnutí informácií.

e.) prioritné odozvy na incident

Každý bezpečnostný incident vyvoláva vopred špecifické požiadavky týkajúce sa zverejnenia informácií o tomto incidente. Tieto požiadavky sú objasnené zhromažďovaním informácií o incidente pomocou dotazníka o špecifických incidentoch. Organizácie a spoločnosti si sami určia

preferencie a priority o tom, ako a ktoré informácie o incidentoch zverejniť. Už vyššie bolo spomenuté, že existujú štyri faktory, ktoré vytvárajú tieto preferencie. Stratégia zverejňovania nemôže vychádzať len z toho, čo sa vyžaduje zákonom. Zverejnenie by malo priniesť pridanú hodnotu organizácie a pomôcť zmierniť škodu spôsobenú bezpečnostným incidentom. Z toho vyplýva, že okrem samotnej informácie o incidente je tiež dôležité vedieť, aké priority má organizácia v súvislosti s konkrétnou udalosťou.

f.) databáza znalostí

Obsah znalostnej databázy o incidentoch sa líši v závislosti od spoločnosti. Avšak existuje niekoľko databáz znalostí, ktoré musia byť implementované s cieľom zaručiť dodržiavanie pravidiel. Spoločnosť musí pravidelne obnovovať a dodržiavať databázu platných

právnych predpisov, čo umožní rýchlo určiť, či sa vyžadujú externé oznámenia, komu a ako rýchlo s akým obsahom sú pri danom incidente zverejňované. Takáto databáza umožní vylúčiť spoločnosti potrebu neustáleho kontaktu s externými subjektmi so žiadosťou o právnu radu. Bez rozsiahlych poznatkov o zúčastnených stranách, ktoré môžu ľubovoľným spôsobom pomôcť pri reakcií na incident, alebo by mohli byť predmetom prípadných incidentov, spoločnosť nebude môcť určiť cieľovú skupinu na zverejňovanie informácií v prípade incidentu, z toho dôvodu aj šanca účinne znížiť škodu po incidente sa výrazne zníži. Spoločnosť skráti čas na odstránenie incidentu, ak si vopred zadefinuje databázu na odhaľovanie incidentov s informáciami ako šablóny oznamovania incidentov, dostupné komunikačné kanály v závislosti od miesta, minulé incidenty a spôsob ich zverejnenia atp. Vo všeobecnosti môže databáza zverejňovania incidentov uchovávať akékoľvek taktické informácie, ktoré organizácia považuje za vhodné pre prípadné incidentové scenáre. Niektoré spoločnosti už využívajú riešenia správy incidentov, ktoré poskytujú vopred nainštalované možnosti úložiska. Taktiež je možné vytvoriť webovú stránku, ktorá je pripojená na server organizácie.

g.) plánovanie stratégie zverejňovania

S odvolaním sa na databázu poznatkov má tím dosť dostupných informácií na vyriešenie rozpoznaného incidentu a rozhodne o optimálnej stratégie zverejňovania incidentu. Je vhodné postupovať podľa vhodného algoritmu zo zoznamu možných scenárov incidentov počítačovej bezpečnosti s cieľom definovať, ktoré informácie sú vhodné pre zverejnenie. Je vhodné určiť rozsah minimálne požadovaných informácií, kam zvyčajne patria zákonné požiadavky, prípadne možnosť zverejnenia ďalších informácií s ohľadom zvýšenia dôvery v informačný systém organizácie a tím aj samotnej organizácie.

h.) aktualizácia stavu incidentu

Je dôležité poznamenať, že v čase, keď tím na rozhodovanie o incidente rozhoduje o stratégií zverejňovania, informácie o incidente sa môžu meniť v závislosti na čase. Postupom času vychádzajú najavo rôzne skutočnosti, takže v priebehu hodnotenia dopadov incidentu je potrebné aktualizovať dotazník o incidentoch a na základe nového skutkového stavu upraviť stratégiu zverejňovania.

ZÁVER

V článku je stručne identifikovaný základný súbor faktorov, ktoré ovplyvňujú organizačné preferencie týkajúce sa zverejňovania informácií o incidentoch. Sú zadefinované štyri rôzne základné strategické otázky, na základe ktorých bol vytvorený prehľad výziev týkajúci sa zverejňovania incidentov z oblasti počítačovej bezpečnosti. Informácie ohľadne incidentov a odstraňovania ich následkov pomôžu vytvorenému tímu vytvoriť špeciálny prístup odhaľovania incidentov a efektívneho odstraňovania ich následkov. Zavedenie rámcových nástrojov, ako sú dotazníky a postupy môžu urýchliť proces vypracovania stratégie zverejňovania incidentov s ohľadom na kvalitu konečných riešení. Postup nemusí byť špecifický pre konkrétne organizácie, ale definuje východiskový bod, podľa ktorého si môže každá organizácia jednoduchým spôsobom vytvoriť rámec postupov, či už v rámci zákona, alebo naviac s ohľadom na svoje obchodné a iné

potreby. Postup pri odhaľovaní incidentov

môže posunúť organizácie k podrobnejšiemu organizovaniu úloh a zodpovedností v rámci tímov zaoberajúcimi sa incidentmi počítačovej bezpečnosti.

ZOZNAM POUŽITEJ LITERATÚRY

CSIRT.sk.

Infoweb.minv.sk.

Nariadenie Ministerstva vnútra Slovenskej republiky o bezpečnostnej politike Ministerstva vnútra Slovenskej republiky pre oblasť informačných systémov.

SUJA, M. Súčasný stav a perspektívy rozvoja informačného systému Hasičského. In Perspektívy rozvoja verejnej správy v krajinách Európskej únie : zborník z celoštátneho vedeckého seminára s medzinárodnou účasťou konaného dňa 10.04.2012 na Akadémii Policajného zboru vBratislave. Bratislava 2012. ISBN 978-80-8054-535-2, s. 29-34.

Výnos č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy.

Wikipedia.com.

www.Informatizácia.sk.

ADRESA

Ing. Igor PAVLOVIČ
Akadémia Policajného zboru v Bratislave
Oddelenia informačných technológií
Sklabinská 1, 835 17 Bratislava
Tel.: 09610 57 343, igor.pavlovic@minv.sk

AKTUÁLNÍ TRENDY V OBLASTI KRIZOVÉHO ŘÍZENÍ A JEJICH VAZBA INFORMAČNÍ BEZPEČNOST

Josef POŽÁR, Oldřich KRULÍK, Radek HAVLÍČEK

Policejní akademie České republiky v Praze

Anotace: *Příspěvek si klade za cíl čtenáře seznámit s aktuálními nástroji, které lze zahrnout pod moderní využívání informačních systémů v bezpečnostní oblasti v České republice. Řeč bude jak o celém integrovaném záchranném systému České republiky, tak o specifických funkcionalitách v rámci Policie České republiky a zdravotnického sektoru.*

Klíčová slova: *Informační technologie, informační systémy, vývoj, inovace, bezpečnostní systém, Česká republika.*

Summary: *The paper aims to familiarize readers with the latest tools that can be understand as modern use of information systems in the security area of the Czech Republic. We are talking first about the Integrated Rescue System of the Czech Republic as well as specific functionalities within the framework of the Police of the Czech Republic and the emergency rescue system.*

Keywords: *Information technology, information systems, development, innovation, security system, Czech Republic.*

ÚVOD

Tento příspěvek si klade za cíl čtenáře seznámit s aktuálními nástroji, které lze zahrnout pod moderní využívání informačních systémů v bezpečnostní oblasti v České republice. Řeč bude jak o celém integrovaném záchranném systému České republiky, tak o specifických funkcionalitách v rámci Policie České republiky a zdravotnického sektoru.

INFORMAČNÍ SYSTÉM INTEGROVANÉHO ZÁCHRANNÉHO SYSTÉMU ČESKÉ REPUBLIKY

Informační systém integrovaného záchranného systému České republiky je jednou z funkcionalit, navazujících na někdejší daleko ambicióznější projekt celostátního „Informačního systému krizového řízení“, ISKŘ, o kterém byla řeč přinejmenším již roku 1998. V průběhu času byly zrealizovány jen dílčí funkce původního projektu, a to často za významného kofinancování z unijních zdrojů.

Výsledný informační a komunikační systém s názvem Informační systém integrovaného záchranného systému (IS IZS) byl do ostrého provozu uveden v prosinci 2015 a za první rok svého působení přenesl více než 100 miliónů datových vět. Nyní byl Monitorovacímu výboru Integrovaného operačního programu prezentován jako tzv. „úspěšný“, což znamená že, byl úspěšně realizován s podporou z Integrovaného operačního programu.1

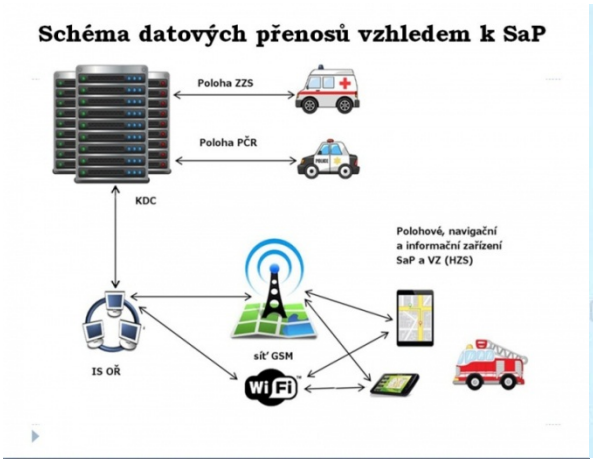
Z pohledu základních složek integrovaného záchranného systému spočívá hlavní přínos projektu především v možnosti efektivní výměny a sdílení dat a informací, možnosti lepší koordinace.

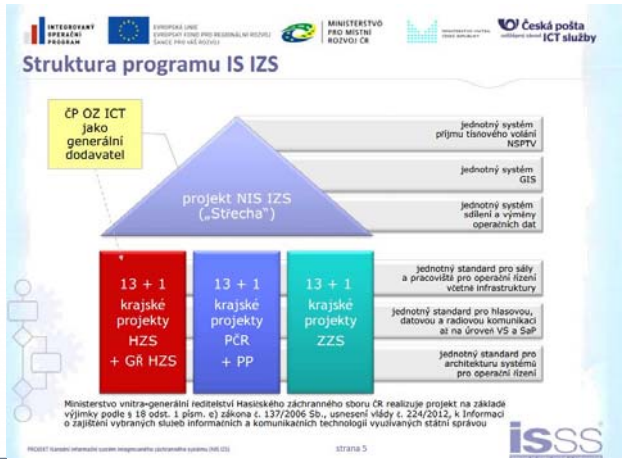
Z pohledu veřejnosti je stěžejním přínosem projektu snížení následků mimořádných událostí v případě společných akcí více složek integrovaného záchranného systému díky rychlejším a provázanějším zásahům. To umožňuje plně dostupné tísňové volání, přesnější určení místa

[1] Informační systém integrovaného záchranného systému. *Hasičský* záchranný sbor České republiky. http://is-izs.izscr.cz/ Národní informační systém integrovaného záchranného systému. *Youtube*. https://www.youtube.com/watch?v=txZLYJ2fN-Q

mimořádné události, okamžité zahájení činnosti potřebných složek a jejich rychlejší přeprava na místo zásahu.

Ilustrace: Příklady vizualizací, vztahujících se k Informačnímu systému integrovaného záchranného systému.[2]





MAPY KRIMINALITY

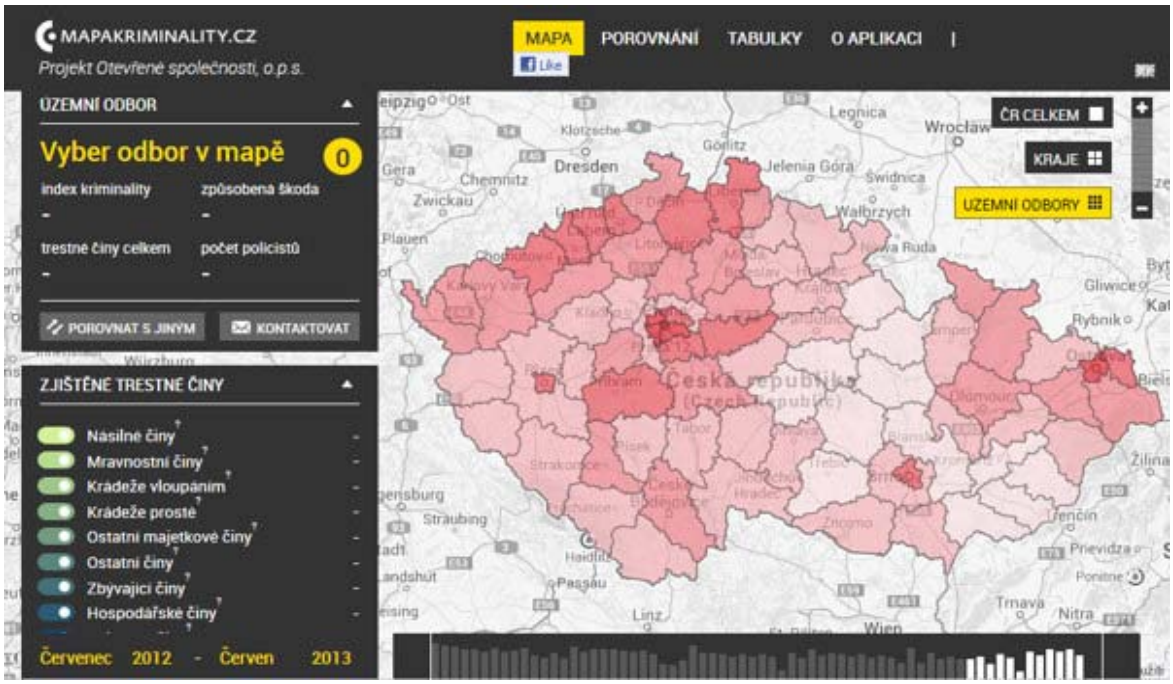
Vedle přehledů, týkajících se současného respektive minulého stavu zjištěné míry kriminality na území České republiky, existuje i projekt, koncipovaný „do budoucnosti" (a nazývaný ostatně pro odlišení právě „Mapy budoucnosti").

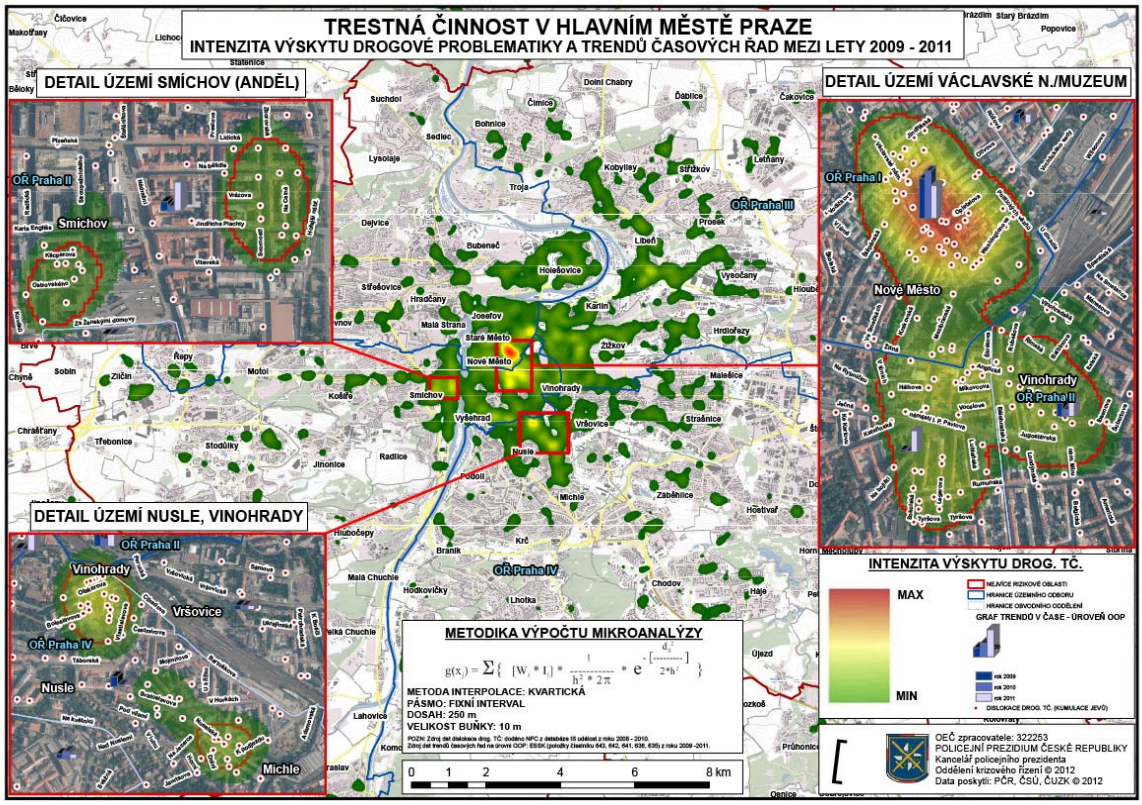
Co se týče „minulosti" respektive „současnosti", na úrovni obvodních oddělení jsou v rámci České republiky k dispozici údaje o zjištěné kriminalitě, její struktuře, stejně jako počty policistů v „terénu". Cílem projektu je usnadnit veřejnosti orientaci v datech o trestné činnosti, která pravidelně publikuje Policie České republiky. Policejní statistiky převádíme do jednoduchých tabulkových a mapových náhledů. Pro ty, kdo chtějí data hlouběji analyzovat, jsou k dispozici ke stažení v počítačově zpracovatelné podobě.[3]

[2] Národní informační systém integrovaného záchranného systému byl prezentován jako úspěšný projekt integrovaného operačního programu. *Hasičský záchranný sbor České republiky*. http://www.hzscr.cz/clanek/ narodni-informacni-system-integrovaneho-zachranneho-systemu-byl-prezentovan-jako-uspesny-projekt-integrovaneho-operacniho-programu.aspx.
ŠTRAUCHOVÁ, Zdenka. Přes nový informační systém integrovaného záchranného systému již prošlo 100 milionů datových vět. *Naše Jablonecko*. 10. VIII. 2016. http://www.nasejablonecko.cz/jablonecko-aktualne/pres-novy-informacni-system-izs-jiz-proslo-100-milionu-datovych-vet/?aktualitaId=44104.

[3] CIBULKA, Jan. Mapy zločinu a česká realita. *Hospodářské noviny*. 19. XI. 2013. http://tech.ihned.cz/c1-61260990-mapy-zlocinu-a-ceska-realita.

Ilustrace: Mapa kriminality v České republice a vizualizace (odhad) drogové kriminality v rámci hlavního města Prahy.[4]



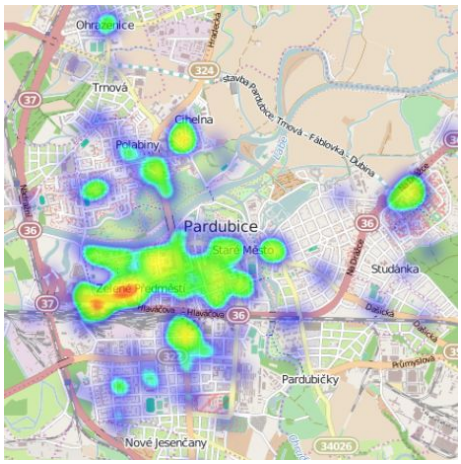


[4] Mapa kriminality. *Otevřená společnost*. http://www.mapakriminality.cz/
Statistické přehledy kriminality. *Policie České republiky*. 2012. http://www.policie.cz/statistiky-kriminalita.aspx.

Co se týče orientace „do budoucnosti“, na začátku aktivit odboru prevence kriminality Ministerstva vnitra (nyní odbor bezpečnostní politiky a prevence kriminality) v oblasti mapování, analýz a predikce kriminality stála inspirace ze zahraničí, která připomínala sci-fi filmy typu Minority Report.

Za využití platformy ACCENDO - Centrum pro vědu a výzkum, byly zmapovány zahraniční zkušenosti, přenositelné do prostředí České republiky.[5] Policisté na začátku své směny dostanou od velitelů mapy s vyznačenými územími, obvykle červenými obdélníky, ve kterých je třeba více hlídkovat. Policisté obvykle zjistí, že na základě takto organizované práce v jejich území působnosti významně klesá kriminalita. I v terénu jsou pomocí mobilních přístrojů neustále ve spojení s operačním střediskem, které on-line sleduje a analyzuje vývoj situace. Hlídka přitom průběžně dostává nové aktualizované pokyny. Paralelní snahou projektu je snaha vštípit veřejnosti informaci, že policisté jsou na místech, kde je to potřeba a v čase, kdy je to potřeba. V ideálním případě pak kriminalita klesá, objasněnost roste, důvěra veřejnosti v policejní síly se zvyšuje.

Ilustrace: Mapa kriminality a pohled do policejní služebny v obci Říčany, která patří mezi průkopníky tohoto řešení.[6]



FUNKCE „ZÁCHRANKA“ PRO POTŘEBY ZDRAVOTNÍKŮ V ČESKÉ REPUBLICE

Aplikace „Záchranka“ představuje řešení, díky němuž může veřejnost přivolat zdravotní záchrannou službu. Záchranářům výrazně pomůže tím, že odešle i přesnou polohu volajícího. V březnu 2016 bylo na systém napojeno 12 ze 14 krajů a později se připojily i Středočeský a Jihočeský kraj. Aplikace jedním stisknutím tlačítka umožní jak vytočit linku 155, tak odeslat informaci o přesné poloze. Pokud člověk trpí nějakými onemocněními, může si předem do aplikace zadat informace o svém zdravotním stavu.[7]

---

[5] HRUŠKA, Lubor a kolektiv. Mapy budoucnosti. Vědecko-výzkumný ústav ACCENDO - Centrum pro vědu a výzkum. Ostrava 2015. ISBN 978-80-87955-06-2. http://www.prevencekriminality.cz/evt_file.php?file=1271
Mapy budoucnosti. *Youtube*; *Ministerstvo vnitra České republiky*. 29. VI. 2015. https://www.youtube.com/playlist?list=pl1cp5donb3zsnfhmz4oqatqu5adfdwzlm
Mapy budoucnosti. *Prevence kriminality v České republice*: *Ministerstvo vnitra České republiky*. http://www.prevencekriminality.cz/projekty/mapy-budoucnosti/

[6] AMBROŽOVÁ, Adéla. Mapy budoucnosti pomůžou Městské policii v Říčanech předpovídat místo zločinu. *Říčany*. 5. III. 2015. http://info.ricany.cz/mesto/mapy-budoucnosti-pomuzou-mestske-policie-v-ricanech-predpovidat-misto-zlocinu.

[7] Aplikace Záchranka začíná: Přivolá sanitku, odešle vaši přesnou polohu i zdravotní stav. *Aktuálně.cz*. 9. III. 2016. https://zpravy.aktualne.cz/regiony/jihomoravsky/aplikace-na-vsechno-zavola-vam-zachranku-odesle-presnou-polo/r~c5377ea2e60011e593630025900fea04/?redirected=1491809903
Mobilní aplikace „Záchranka“. *Youtube*. https://www.youtube.com/channel/UC2xv40spfj7yp2tj2-y6_XA

Ilustrace: Vizualizace, vztahující se k tématu aplikace.[8]

ZÁVĚR

Dynamický vývoj v řadě ohledů, související s konkrétními součástmi bezpečnostního systému České republiky, je nepřehlédnutelný. Snahou Policejní akademie České republiky v Praze je propagovat tento vývoj a dle možností ho aktivně spoluvytvářet. Ačkoli zde existuje značná konkurence ze strany (nejen) „technických" škol, studenti naší školy formou referátů a dalších tématických vystoupení seznamují spolužáky s technickým vývojem v rámci své profese. Podle možností jsou rovněž prováděny exkurze do prostředí, kde jsou nové nástroje nasazeny v ostrém provozu.

ZOZNAM POUŽITEJ LITERATÚRY

AMBROŽOVÁ, Adéla. Mapy budoucnosti pomůžou Městské policii v Říčanech předpovídat místo zločinu. *Říčany*. 5. III. 2015. http://info.ricany.cz/mesto/mapy-budoucnosti-pomuzou-mestske-policie-v-ricanech-predpovidat-misto-zlocinu.

Aplikace Záchranka začíná: Přivolá sanitku, odešle vaši přesnou polohu i zdravotní stav. *Aktuálně.cz*. 9. III. 2016. https://zpravy.aktualne.cz/regiony/jihomoravsky/aplikace-na-vsechno-zavola-vam-zachranku-odesle-presnou-polo/r~c5377ea2e60011e593630025900fea04/?redirected=1491809903.

CIBULKA, Jan. Mapy zločinu a česká realita. *Hospodářské noviny*. 19. XI. 2013. http://tech.ihned.cz/c1-61260990-mapy-zlocinu-a-ceska-realita.

HRUŠKA, Lubor a kolektiv. Mapy budoucnosti. Vědecko-výzkumný ústav ACCENDO - Centrum pro vědu a výzkum. Ostrava 2015. ISBN 978-80-87955-06-2. http://www.prevencekriminality.cz/evt_file.php?file=1271.

Informační systém integrovaného záchranného systému. *Hasičský záchranný sbor České republiky*. http://is-izs.izscr.cz/.

Mapa kriminality. *Otevřená společnost*. http://www.mapakriminality.cz/.

Mapy budoucnosti. *Prevence kriminality v České republice*: *Ministerstvo vnitra České republiky*. http://www.prevencekriminality.cz/projekty/mapy-budoucnosti/.

Mapy budoucnosti. *Youtube*; *Ministerstvo vnitra České republiky*. 29. VI. 2015. https://www.youtube.com/playlist?list=pl1cp5donb3zsnfhmz4oqatqu5adfdwzlm.

Mobilní aplikace „Záchranka". *Youtube*. https://www.youtube.com/channel/UC2xv40spfj7yp2tj2-y6_XA.

Národní informační systém integrovaného záchranného systému byl prezentován jako úspěšný projekt integrovaného operačního programu. *Hasičský záchranný sbor České republiky*. http://www.hzscr.cz/clanek/narodni-informacni-system-integrovaneho-zachranneho-systemu-byl-prezentovan-jako-uspesny-projekt-integrovaneho-operacniho-programu.aspx.

Národní informační systém integrovaného záchranného systému. *Youtube*. https://www.youtube.com/watch?v=txZLYJ2fN-Q.

[8] „Záchranka", Mobilní aplikace Zdravotnické záchranné služby. http://www.zachrankaapp.cz/
Stáhněte si mobilní aplikaci Záchranka. *Výzbrojna.cz*. 18. III. 2016. http://www.vyzbrojna.cz/cz/news/stahnete-si-mobilni-aplikaci-zachranka 426.html

Stáhněte si mobilní aplikaci Záchranka. *Výzbrojna.cz*. 18. III. 2016. http://www.vyzbrojna.cz/cz/news/stahnete-si-mobilni-aplikaci-zachranka 426.html
Statistické přehledy kriminality. *Policie České republiky*. 2012. http://www.policie.cz/statistiky-kriminalita.aspx.
ŠTRAUCHOVÁ, Zdenka. Přes nový informační systém integrovaného záchranného systému již prošlo 100 milionů datových vět. *Naše Jablonecko*. 10. VIII. 2016. http://www.nasejablonecko.cz/jablonecko-aktualne/pres-novy-informacni-system-izs-jiz-proslo-100-milionu-datovych-vet/?aktualitaId=44104.
„Záchranka“, Mobilní aplikace Zdravotnické záchranné služby. http://www.zachrankaapp.cz/.

ADRESA

doc. RNDr. Josef POŽÁR, CSc.
Mgr. Oldřich KRULÍK, Ph.D.
Mgr. Radek HAVLÍČEK
Policejní akademie České republiky v Praze
Lhotecká 559/7, P.O.BOX 54, 143 01 Praha 4

KYBERNETICKÉ HROZBY V REGIONÁLNÍ BEZPEČNOSTI A MOŽNOSTI JEJICH PRÁVNÍHO POSTIHU

CYBER THREATS IN REGIONAL SECURITY AND THE POSSIBILITIES FOR THEIR LEGAL REMEDY

Ivo SVOBODA

Vysoká škola regionální rozvoje

Abstakt: *Ochrana před kybernetickými hrozbami by měla být signifikantním v zájmu státu. Prostřednictvím kybernetických útoků dochází jak ke vzniku škod na majetku, ke škodám nemajetkovým, ale zejména může docházet k ohrožení vnitřní bezpečnosti státu. Může docházek k napadání jak ze strany jiných států, tak ze strany zájmových skupin tvořených jak bázi extremismu, tak ze strany jednotlivců bez ideové pohnutky. Jelikož kyberprostor nezná hranice, je na místě se v boji s tímto fenoménem řídit nejen právním rámcem jednotlivých zemí, ale vnímat i právní klima v zemích celého, globalizovaného, světa.*

Klíčová slova: *Bezpečnostní management, Kybernetická hrozba, Kybernetické bezpečnost, Právní postih, Kriminalita, Regionální bezpečnost*

Abstract: *Protection against cyber threats should be significant in the interest of the state. Through cyber-attacks, both property damage and non-property damage occur, but, in particular, the state's internal security can be endangered. It may be attacked both by other states, by the groups of both extremist and non-ideological individuals. Since cyberspace knows no boundaries, it is important to combat this phenomenon not only in the legal framework of the individual countries, but also in the legal climate in the countries of the globalized world.*

Keywords: *Security management, Cyber threat, Cyber security, Legal punishment, Criminality, Regional security*

ÚVOD

S přijetím zákona o kybernetické bezpečnosti na konci roku 2014, se otázka kybernetických hrozeb a otázka ochrany informačních systémů před jejich dopady v rámci České republiky stala velmi aktuální. Přijetím tohoto zákona č. 181/2014 Sb., O kybernetické bezpečnosti došlo k naplnění mezinárodních dohod a tento zákon je další pojistkou k dosažení vyšší míry kybernetické bezpečnosti. Jedná se o další krok, jelikož již trestní zákoník č. 40/2009 Sb., ve znění pozdějších předpisů ukotvuje několik speciálně konstruovaných trestných činů, které reagují na možné kybernetické ohrožení. Zejména se jedná o trestné činy uvedené v §§ 230-232 Trestního zákoníku (§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací, § 231- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a § 232 - Poškození záznamu v počítačovém systému a nosiči informací na záznamovém systému). Jelikož se ale výpočetní technika dostává do stále širších oblastí lidských i právních vztahů, mohou být kybernetickým ohrožením dotčeny i jiné lidské aktivity a práva, tedy i skutkové podstaty trestných činů. Například v oblasti hospodářských trestných činů, trestných činů proti majetku, či v oblasti osobnostních práv. Typicky se může například jednat o Ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla dle § 291, Ohrožení utajované informace dle § 317, nebo Šíření poplašné zprávy dle § 357 atd atd.

Přestože na většinu subjektů provozujících uvedené systémy se zákon o kybernetické bezpečnosti nevztahuje, měly by se samy v zájmu zajištění bezpečnosti svých informačních systémů seznámeny alespoň rámcově s existujícími hrozbami na tomto poli a možnostmi omezení případných dopadů jejich realizací. Jedním z uvedených subjektů nespadajících do uvedeného zákona jsou dle vyjádření Národního bezpečnostního úřadu také obce, v jejichž případě lze popsané

seznámení s kybernetickými hrozbami považovat za zcela nezbytné, a to v zájmu zajištění bezpečnosti na regionální úrovni. Zde by selhání kybernetické infrastruktury mohlo způsobit citelné škody na kritické infrastruktuře. Předložený článek se pokouší uvedené seznámení zprostředkovat - popisuje možné typy kybernetických hrozeb, popisuje možné trestně právní postihy těchto narušení (a to v komparaci se Slovenskem) a na příkladech demonstruje jejich realizaci a dopady v podmínkách reálného světa a současně nabízí jednoduchá obranná opatření proti nim.

1 VYMEZENÍ POJMU KYBERKRIMINALITA

Za kyberkriminalitu považujeme takové činnosti, při nichž počítače, telefony, mobilní zařízení, a další technologická zařízení fungují jako nástroje k páchání nelegálních aktivit agresorů (např. finanční podvody, prodej nelegálního zboží, zcizení tajných informací, kyberstalking aj.) Kyberkriminalita je většinou namířena proti osobám, případně majetku, organizacím (vláda, firmy), anebo obecně celé společnosti.[1] Kyberkriminalita nabízí agresorům, oproti klasické kriminalitě, řadu výhod:

- Zatímco u běžné kriminality bývá agresor na místě, kde se nelegální čin odehrál, fyzicky přítomen, u kyberkriminality tomu tak není, neboť nelegální čin se odehrává v kyberprostoru. Kyberagresor tudíž může pocházet i z jiné země, čímž se odhalení a dopadení pachatele ztěžuje.
- Prostřednictvím internetu může být ve stejný čas napadeno mnohonásobně větší množství obětí než u tradiční kriminality.
- Kyberprostor poskytuje útočníkům anonymitu.

Anonymita útočníka je nejdůležitějším faktorem, v rámci specifické kybernetické hrozby. Virtualita prostředí, absence kontaktu útočníka s obětí útoku a sofistikované virtuální nástroje zabezpečují téměř stoprocentní anonymitu, která je velice těžce zamezitelná anebo odhalitelná.[2]

2 PODOBY KYBERKRIMINALITY

Ty mohou být velmi různorodé. Informační a komunikační technologie mohou sloužit jako nástroj k páchání nelegálních aktivit a také mohou být jejich cílem.[3]

Informační a komunikační technologie jako nástroj k páchání nelegálních aktivit

- Phising - rozesílání klamavých mailových zpráv uživatelům, za účelem získání jejich citlivých údajů. Oběti jsou lákány na webové stránky, které jsou k nerozeznání od běžných finančních institucí. Pod záminkou aktualizace osobních údajů uživatelů, zadá nic netušící osoba na falešné webové stránce své přihlašovací jméno a heslo, tímto způsobem prozradí své citlivé údaje útočníkům, kteří jsou poté schopni jí z účtu peníze odcizit.
- Vishing - druh phisingu (tzv. hlasový phising = voice phising), kdy jsou využívány hlasové služby, hlasové schránky a VoIP komunikace. Bývá kombinován s phisingem.
- Phaxing - funguje podobně jak už bylo popsáno výše. Jedná se rovněž o druh phisingu, v tomto případě jde o tzv. faxový phising (fax phising). Uživatel obdrží od falešné banky zprávu, aby zaslal své údaje o platební kartě prostřednictvím faxu.
- Pharming - obdoba phisingu, nicméně daleko zákeřnější a hůře rozpoznatelná technika. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu.

[1] GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.
[2] ŠIŠULÁK, S., KURILOVSKÁ, L. *Sociálne siete ako kybernetická hrozba.* Banská Bystrica: Bezpečnostné fórum, 2015. ISBN 978-80-557-0849-2.
[3] MACHÁČKOVÁ, Pavla. Kyberšikana: ubližování bez hranic. *Psychologie dnes*, 2007, roč. 13, č. 9, s. 50-53. ISSN 1212-9607.

- Phreaking - napojení se na telefonní linku oběti. Pachatel tímto způsobem může volat zadarmo na účet oběti do kterékoliv části světa, neomezeně surfovat po internetu či odposlouchávat cizí hovory.
- Defacement - nahrazení původních webových stránek jiným obsahem. Většinou se jedná o reakci na politickou situaci v regionu či ve světě, případně může posloužit k propagaci extrémistických a teroristických skupin a jejich ideologií. Přednostně jsou vybírány známé webové stránky, které jsou hojně navštěvovány.
- Finanční podvody - praní špinavých peněz, podvody s kreditními kartami aj.
- Prodávání ilegálního zboží a výrobků - obchodování se zbraněmi, léky, narkotiky apod.
- Online gambling - hraní hazardních her na internetu. Patří sem např. online sázky (sportovní, politické, společenské události), stolní hry (např. ruleta), karetní hry (např. poker, blackjack), výherní automaty aj. Oproti klasickému gamblingu poskytuje online gambling uživatelům řadu výhod. Patří sem snadná dostupnost (uživatel se může připojit kdykoliv, v kteroukoliv hodinu a v kterýkoliv den), větší možnost výběru z online sázkových kanceláří či kasín a v neposlední řadě časově neomezené sázení v průběhu zápasu.
- Kyber pornografie - využití kyberprostoru k šíření a publikování pornografického materiálu.
- Kyberstalking - virtuální pronásledování, obtěžování a zastrašování obětí přes internet.
- Kyber squotting - registrace či obchodování s doménovými jmény, obsahujícími registrovanou obchodní značku jiného subjektu, než který doménu registruje.
- Kyberterorismus - lze ho považovat za určitý typ kyberkriminality. Cílem teroristů je vyřadit z provozu životně důležité řídící systémy - logistika, doprava, vojenská sféra, zdravotnictví, elektrárny, vodárny, plynovody, ropovody, bankovní sektor aj. Zatím takové případy zaznamenány nebyly. Zkolabování systému bylo vždy způsobené náhodnou chybou v systému, nicméně podceňování situace není do budoucna na místě.
- Kybernetická válka - lze ji chápat jako válku o informace; hlavní zbraní jsou právě získané informace. Jedná se o aktivity zaměřené na získání informační převahy nebo napadení technologické infrastruktury. V této válce není důležitá nejmodernější vojenská vybavenost či početní převaha protivníka, to na čem nejvíce záleží, je zůstat v anonymitě, aby protivník nezjistil, odkud jsou útoky vedeny. V současné době má zbraně použitelné v kybernetické válce k dispozici především těchto pět států - USA, Rusko, Francie, Izrael a Čína. Napadení systémů pro řízení kritické infrastruktury nemusí být tak obtížné, jak se na první pohled zdá. Většina těchto systémů není pravidelně aktualizována, neboť by musely být dočasně vyřazeny z provozu, stejně tak i hesla většinou zůstávají stejná a neobměňují se. Tato skutečnost tak může nahrát i případným islámským teroristům.[4]
- Kyberšikana - obdoba klasické šikany, nicméně agresoři ubližují svým obětem prostřednictvím moderních informačních a komunikačních technologií. Přestože se jedná převážně o psychické ubližování, následky mohou být stejně tragické jako u tradiční šikany.
- Whaling - příjemcem zpráv je pouze jediná osoba (v rámci cílové organizace zpravidla vysoce postavená) a záměrem útočníka bývá získání specifických dat - velmi často například přihlašovacích údajů k informačním systémům organizace.

Informační a komunikační technologie jako cíl nelegálních aktivit

- Neautorizovaný přístup do počítačového systému či sítě - krádeže dat a tajných informací. Pachateli se mohou stát například bývalí zaměstnanci, kteří byli z firmy či dané instituce propuštěni.

[4] HODNÝ, Jiří. Islamisté online. *Vojenské rozhledy*, 2009, roč. 18, č. 2, s. 70-78. ISSN 1210-3292. a dále i HODNÝ, Jiří. Virtuální univerzita jihádu: výcvik a vzdělávání islámských teroristů v kyberprostoru. *Vojenské rozhledy*, 2009, roč. 18, č. 1, s. 115–120. ISSN 1210-3292.

- E-mail bombing - tzv. e-mailové bombardování se projevuje tím, že daným osobám je rozesíláno velké množství e-mailů, čímž dojde k přeplnění jejich poštovní schránky.
- Spam - nevyžádané hromadně rozesílané zprávy různého obsahu.
- Hoax - nevyžádaná mailová zpráva (tzv. řetězový mail), která uživatele varuje před nějakým falešným nebezpečím, snaží se ho pobavit, hraje na city uživatele tím, že zveřejní nějaký srdceryvný příběh, upozorňuje na nějaký vir…. Uživatel je pokaždé žádán, aby si zaslané sdělení nenechal pro sebe a poslal je dál svým známým a přátelům. Tímto způsobem dochází k masovému šíření rozsáhlého seznamu e-mailových adres mezi předem neurčité množství cizích lidí, čímž vznikají ideální podmínky pro šíření spamu a počítačových virů.
- Malware - počítačový program určený ke vniknutí nebo poškození počítačového systému. Za malware jsou označovány počítačové viry, trojské koně, adware a spyware.
- Hacking - jedná se o proniknutí do cizích počítačových systémů za účelem získávání informací o systému a přístupu ke všem informacím na systému.
- Cracking - prolomení softwarové ochrany počítače. Napadený software je modifikován a šířen dále prostřednictvím internetu.
- Botnet - program, který funguje obdobně jako robot. Bývá tajně nainstalován na uživatelském počítači. Obsahuje komunikační a řídící modul, čímž umožňuje neautorizovanému uživateli vzdáleně tento počítač ovládat a využít pro plnění různých příkazů. Botnet je nejčastěji používán pro hromadné šíření spamu.

4 MOŽNOSTI PRÁVNÍHO POSTIHU KYBERNETICKÉ KRIMINALITY

Jak již bylo uvedeno výše, vzhledem k tomu, že výpočetní technika se dostává do stále širších oblastí lidských i právních vztahů, mohou být kybernetickým ohrožením dotčeny různorodé lidské aktivity a práva, a tomu by tedy měly být uzpůsobeny skutkové podstaty konkrétních trestných činů. Jedná se o celou oblast hospodářských trestných činů, trestných činů proti majetku, či v oblasti osobnostních práv. Velmi závažná poškození práv a oprávněných zájmů však nutno spatřovat v oblasti bezpečnostní, kdy kybernetické útoky a kybernetické kriminalita může mít za následek ohrožení bezpečnosti kritické infrastruktury v municipalitách, může dojít i k ohrožení

vnitřní bezpečnosti státu, a ostatně může být tímto způsobem vedena válka mezi jednotlivými státy, názorovými klany či náboženskými skupinami v globálním měřítku.

Pokud budeme konkrétní, možnosti trestního postihu v České republice dle zák. 40/2009 Sb., Trestního zákoníku ve znění pozdějších předpisů jsou konstruovány např. v ust. §§ 230-233 a dále v ust. § 270 (§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací, § 231- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému, § 232 - Poškození záznamu v počítačovém systému a nosiči informací na záznamovém systému a § 270 - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi). Na Slovensku hovoří zák. č. č. 300/2005 Zz. Trestný zákoník obdobně v ust. §§ 196, 247 a § 283 (§ 196 - Porušovanie tajomstva prepravovaných správ, ust. § 247 Poškodenie a zneužitie záznamu na nosiči informácií a § 283 Porušovanie autorského práva.[5]

Tato ustanovení však jsou typicky zaměřena na kyberkriminalitu, ale i jiná ustanovení mohou postihovat projevy kybernetického zločinu, namátkou můžeme vybrat třeba typicky např. skutkové podstaty trestných činů Ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla dle § 291, Ohrožení utajované informace dle § 317, nebo Šíření poplašné zprávy dle § 357 atd atd.[6]

ZÁVĚR

V tomto článku byla popsána kyberkriminalita a její možné formy a metody. Současně byly popsány informační a komunikační technologie jako nástroj i cíl páchání nelegálních aktivit a v konečném důsledku trestné činnosti, které může mít za následek nejen rozsáhlé majetkové škody, ale může být závažným faktorem při ohrožení bezpečnosti kritické infrastruktury v regionálním, celostátním i globálním měřítku. Závěrem článku bylo poukázáno a skutečnost, že např. v České republice i na Slovensku jsou možnosti trestního postihu podobné, ale současně bylo zkonstatováno, že rezervy jsou stále ještě v oblasti prevence, a to nejen při tvorbě technických opatření, ale zejména při prevenci nejslabšího článku - tedy lidského faktoru. Zde je zřetelné akční pole pro bezpečnostní management a jeho roli při koordinaci, školení a kontrole lidského faktoru v rámci řízení lidských zdrojů.

SEZNAM POUŽITÉ LITERATURY

CÓLON, Marcos. *Phishing attack leads to breach at government agency* [online]. 2012 [cit. 2015-04-06]. Dostupné z: http://www.scmagazine.com/phishing-attack-leads-to-breach-at-government-agency/article/247283/

CYBER CONFLICT STUDIES ASSOCIATION. *The History of Stuxnet: Key Takeaways for Cyber Decision Makers* [online]. 2012, 30 s. [cit. 2015-04-06]. Dostupné z: http://www.afcea.org/committees/cyber/documents/TheHistoryofStuxnet.pdf,

ERBSCHLOE, Michael. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Boston: Elsevier Butterworth Heinemann, c2005, xix, 212 p. ISBN 07-506-7848-8. a dále i ESET *Threat Encyclopedia* [online]. 2008, 2015 [cit. 2015-04-06]. Dostupné z: http://www.eset.com/us/threat-center/encyclopedia/threats/

F-SECURE. *Virus and threat descriptions* [online]. 2015 [cit. 2015-04-06]. Dostupné z: http://www.f-secure.com/en/web/labs_global/threats/descriptions a dále i WIKIA, INC. *Virus Information* [online]. 2007, 2015 [cit. 2015-04-06]. Dostupné z: virus.wikia.com/wiki/

GAUSS: *Abnormal Distribution* [online]. Kaspersky Lab Global Research and Analysis Team, 2012 [cit. 2015-04-06]. Dostupné z: http://www.securelist.com/en/downloads/vlpdfs./kaspersky-lab-gauss.pdf,

GOSTEV, Alexander. *Kaspersky Security Bulletin 2012*: Cyber Weapons. In: Securelist [online]. 2012 [cit. 2015-04-06]. Dostupné z: http://securelist.com/analysis/kaspersky-security-bulletin/36762/kaspersky-security-bulletin-2012-cyber-weapons/

GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

HODNÝ, Jiří. Islamisté online. *Vojenské rozhledy*, 2009, roč. 18, č. 2, s. 70-78. ISSN 1210-3292.

HODNÝ, Jiří. Virtuální univerzita jihádu: výcvik a vzdělávání islámských teroristů v kyberprostoru. *Vojenské rozhledy*, 2009, roč. 18, č. 1, s. 115–120. ISSN 1210-3292.

[5] Zák. č. 300/2005 Zz. Trestný zákoník
[6] Zák. č. 40/2009 Sb., trestní zákoník

HONG, Jason. The state of phishing attacks. *Communications of the ACM* [online]. 2012, vol. 55, issue 1 [cit. 2015-04-06]. DOI: 10.1145/2063176.2063197
KOPŘIVA, Jan. Kybernetické hrozby pro regionální bezpečnost a obranná opatření proti nim. *In. Bezpečnostní management*. Praha, 2/2016. ISSN ISSN 2464-6903.
LABORATORY OF CRYPTOGRAPHY AND SYSTEM SECURITY (CRYSYS LAB). SKyWIper (a.k.a. Flame a.k.a. Flamer): *A complex malware for targeted attacks* [online]. 2012, 64 s. [cit. 2015-04-06]. Dostupné z: http://www.crysys.hu/skywiper/skywiper.pdf
LANGNER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon. *Security & Privacy*, IEEE. 2011, roč. 9, č. 3, s.
MACHÁČKOVÁ, Pavla. Kyberšikana: ubližování bez hranic. *Psychologie dnes*, 2007, roč. 13, č. 9, s. 50-53. ISSN 1212-9607.
NÝVLT, Václav a Jan KRUŽNÍK. *Anonymous napadli servery OSA*, web české vlády i Evropského parlamentu [online]. 2012 [cit. 2015-04-06]. Dostupné z: http://technet. idnes.cz/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu-1mp-/sw_internet.aspx?c=A120126_134112_sw_internet_nyv
RAUI, Costin a Igor SOUMENKOV. KASPERSKY LAB. *The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor* [online]. 2013, 20 s. [cit. 2015-04-06]. Dostupné z: http://www.securelist.com/en/downloads/vlpdfs/themysteryofthepdf0-dayassemblermicrobackdoor.pdf
"Red October" Diplomatic Cyber Attacks Investigation. In: *Securelist* [online]. 2013 [cit. 2015-04-06]. Dostupné z: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation
SOUMENKOV, Igor. *Kaspersky Lab Identifies Operation "Red October," an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide*. In: Kaspersky Lab [online]. 2013 [cit. 2015-04-06]. Dostupné z: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide
SZOR, Peter. *The art of computer virus research and defense*. Boston: Addison-Wesley, c2005, xxvii, 713 s. ISBN 03-213-0454-3.
ŠIŠULÁK, S., KURILOVSKÁ, L. Sociálne siete ako kybernetická hrozba. Banská Bystrica: Bezpečnostné fórum, 2015. ISBN 978-80-557-0849-2.
Zák. č. 300/2005 Zz. Trestný zákoník
Zák. č. 40/2009 Sb., Trestní zákoník

ADRESA

doc. JUDr. PhDr. Ivo SVOBODA, Ph.D.
Vysoká škola regionální rozvoje
Žalanského 68/54, 163 00 Praha

SYSTÉMOVÉ INŽENÝRSTVÍ A MOŽNOSTI VYMEZENÍ VHODNÝCH MODELŮ VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI NA PA ČR V PRAZE

SYSTEMIC ENGINEERING AND THE POSSIBILITY OF DEFINITION OF APPROPRIATE MODELS OF CYBERNETIC AND INFORMATION SECURITY EDUCATION IN THE PA CR IN PRAGUE

Vladimír ŠULC, Václav HNÍK

Policejní akademie ČR v Praze

***Anotace**: Předkládaný příspěvek je rozdělen na tři hlavní části:*

1. *Diskusi systémového vymezení vědního oboru Kybernetika a odpovídající oblasti Kybernetická bezpečnost (včetně souvislostí uvedených pojmů s exaktní teorií informace a dalšími obory, zvláště s teorií systémů. Byl zmíněn zákon o kybernetické bezpečnosti a rovněž nařízení vlády č. 275/2016 Sb. o oblastech vzdělávání ve vysokém školství pro bezpečnostní obory.*
2. *Informaci o hledání nejvhodnější spolupráce při řešení vědeckovýzkumné práce v této oblasti, které vyústilo v uzavření smlouvy mezi PA ČR v Praze a Univerzitou Tomáše Bati ve Zlíně, fakultou logistiky a krizového řízení v Uherském Hradišti. V této části jsou rovněž uvedeny hlavní důvody této spolupráce a k čemu především by tato spolupráce měla sloužit.*
3. *Návrh laboratoře aplikované kybernetické bezpečnosti pro výuku předmětů kybernetické bezpečnosti, schéma prvního návrhu uvedené laboratoře a stručný popis technických, programových a organizačních prostředků, které jsou potřebí k realizaci tohoto návrhu.*

***Klíčová slova:** Systémové inženýrství, kybernetika, kybernetická bezpečnost*

***Annotation:** The present contribution is divided into three main parts:*

1. *Discussion of the systemic definition of the field of science Cybernetics and related areas Cybernetic safety (including the context of the above terms with the exact theory of information and other fields, especially with the theory of systems). The cyber security law, as well as Government Order No. 275/2016 Coll. Education in higher education for security was mentioned as well.*
2. *Information on finding the most suitable co-operation in solving the scientific research work in this field, which resulted in a contract between PA CR in Prague and Tomas Bata University in Zlín, Faculty of Logistics and Crisis Management in Uherské Hradiště. This section also mentions the main reasons for this cooperation and what is the main purpose of this cooperation.*
3. *Design of an Applied Cyber Security Laboratory for cyber security training, a first design of the laboratory, and a brief description of the technical, program and organizational tools needed to implement this proposal.*

***Keywords:** System engineering, cybernetics, cyber security*

ÚVOD

Současný stav odborné problematiky v oblasti informatiky a ve vědním oboru kybernetika lze i na základě jen zběžného rozboru dostupných informačních zdrojů charakterizovat jako velmi proměnlivý, rozsáhlý a svými novými výsledky (zejména v aplikacích) ovlivňující téměř všechny oblasti lidského života.

Kybernetika jako věda, která se zabývá obecnými principy řízení a přenosu informace ve strojích a živých organismech, tvoří důležitou součást oborů lékařských, vojenských, ekonomických, sociologických a dalších. Za zakladatele je považován Norbert Wiener, který vydal v roce 1948 knihu Kybernetika aneb Řízení a sdělování u organismů a strojů. Od této doby se kybernetika jako vědní obor nesmírně rozvinula. Pozoruhodné však je, že se rozšířil i význam slov „kybernetika“, „kybernetický“. Slovní spojení „kybernetický prostor“, „kybernetická bezpečnost“,

„kybernetická kriminalita“ „kybernetický útok“ získaly svůj svébytný význam. Nejinak tomu je i v případě slovního spojení „kybernetický zákon“.

V souladu se současnými poznatky o obsahu a důsledcích „Kybernetického zákona“ v ČR je nyní na PA ČR v Praze realizována i plánována řada vzdělávacích a vědecko-výzkumných aktivit v oblastech uvedených níže.

SYSTÉMOVÉ VYMEZENÍ VĚDNÍHO OBORU KYBERNETIKA A ODPOVÍDAJÍCÍ OBLASTI „KYBERNETICKÁ BEZPEČNOST“

Princip zpětné vazby byl znám již dříve v regulační technice a používal se při návrhu zpětnovazebních systémů pro účely sdělovací techniky. Zakladatelé kybernetiky ale rozpoznali, že jde o velmi obecný princip. Je především zásluhou rozvoje kybernetiky jako vědy, že se stal obecně známým a umožnil vysvětlit řadu dějů odehrávajících se v nejrůznějších dynamických systémech a popisovaných v dalších vědních oborech.

Exaktní teorie informace byla jako odnož teorie pravděpodobnosti zkoumána a rozvíjena v matematice. Informace doplnila fyzikální obraz světa v tom smyslu, že jde o stejně důležitou entitu, jako je hmota či energie. Informace je zřejmě dnes nejfrekventovanějším pojmem, který kybernetika přinesla. Zpracování informace se stává stále důležitějším, a pomalu ale jistě mění charakter našeho současného života a stává se tak základem nové „technologické revoluce“ v současném světě.

Systematické studium společných znaků různých systémů a obecných vlastností systémů jako systémů (tj. teorie systémů) vedlo k poznatku, že systémy různé fyzikální podstaty mohou mít velmi podobné chování a že chování jednoho systému můžeme zkoumat prostřednictvím chování jiného, snadněji popsatelného či realizovatelného systému jako vhodného modelu ve zcela jiných časových či prostorových měřítkách (viz teorie modelů a modelování). Ukázalo se, že mnohé systémy mechanické, hydraulické, pneumatické, tepelné atd. jsou popsány formálně stejnými (například diferenciálními) rovnicemi. To vedlo ke vzniku analogových, hybridních a číslicových počítačů (informačních a komunikačních technologii - ICT jako komunikačního prostředí kybernetiky v současném digitálním světě).

Kybernetika se nyní opět stává samostatným vědním oborem (po oddělení od informatiky) tedy vědou (se součástmi teoretické, technické a aplikační kybernetiky) o systémech řízení procesů v živých i neživých objektech, organismech, strojích, moderních robotech apod. Pojem „kybernetika“ ~~je~~ původně odvozený od řeckého slova kybernetes, tj. kormidelník, se tak stává velmi perspektivním a dynamickým jednotícím prvkem pro výstavbu systémů řízení a studiem procesů v automatech, ICT, živých organismech i ve společenských systémech. Vytváří jednotné hledisko na živé i neživé systémy tak, že soustřeďuje poznatky různých oborů, jako biologie, fyziologie, psychiatrie, psychologie, logiky, matematiky, strojového zpracování dat, automatizační a regulační techniky, teorie řízení apod. V tomto kontextu civilizovaný svět přijímá také nové normy bezpečnosti, v nichž jsou nyní odděleny pojmy informační a kybernetické bezpečnosti.

Z legislativních norem, které se této oblasti týkají, je nejdůležitější „Zákon o kybernetické bezpečnosti“. Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. V tomto zákoně se rozumí: kybernetickým prostorem digitální prostředí (umožňující vznik, zpracování a výměnu informací) tvořené informačními systémy a službami a sítěmi zatím elektronických komunikací (v budoucnu optoelektronických a bionických systémů), kritickou informační infrastrukturou systémy kritické infrastruktury v odvětví komunikační a informačních systémů tedy v oblasti kybernetické bezpečnosti. Dále zákon vymezuje orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti. Upřesňuje se také pojem znalostní pracovník moderních „učících se podniků a organizací“. Z pohledu robototechniky se také již nyní objevují diskuze o novém pojetí „elektronická osoba“ (vedle „fyzické a právnické osoby“).

Dalším významným podkladem pro zkoumání v této oblasti je Nařízení vlády č. 275/2016 Sb. „*Nařízení vlády o oblastech vzdělávání ve vysokém školství*“ pro BEZPEČNOSTNÍ OBORY - Základní tematické okruhy: Bezpečnostní politika státu, Metodologie posuzování rizik, Hospodářská opatření pro krizové stavy, Bezpečnostní hrozby vojenského a nevojenského charakteru, Vedení operací vojenského a nevojenského charakteru, Řízení bezpečnosti ve veřejném a soukromém sektoru, Krizové řízení, Právní systém České republiky v oblasti bezpečnosti, Ochrana kritické infrastruktury, Ochrana obyvatelstva, Kybernetická bezpečnost, Aplikovaná informatika pro bezpečnostní sbory, Informační a komunikační systémy pro podporu krizového řízení, Ochrana ekonomiky, Vnitřní bezpečnost a veřejný pořádek, Civilní nouzová připravenost EU a NATO, Prevence závažných havárií, Integrovaný záchranný systém, Požární ochrana, atd.

HLEDÁNÍ NEJVHODNĚJŠÍ SPOLUPRÁCE PŘI ŘEŠENÍ VĚDECKOVÝZKUMNÉ PRÁCE V TÉTO OBLASTI JAKO NEJLEPŠÍHO ZPŮSOBU ŘEŠENÍ DANÉHO PROBLÉMU V DANÉM ČASE.

Aktuálnost těchto nových projektů v oblastech kybernetické a informační bezpečnosti vychází především z časoprostorového vnímání rozvíjených vědních oborů a využití systémového chápání kulturních a civilizačních procesů v oblasti „technologické revoluce“. Tyto procesy jsou vyvolány zejména rychlým vývojem moderní informatiky (informačních a komunikačních technologií), kybernetiky (kybernetických strojů jako jsou numericky řízené stroje, roboty a robotické linky, roboty s umělou inteligencí, učící se systémy a „učící se organizace a podniky“ apod.), moderní fyziky, moderní matematiky a procesního inženýrství. Důležité jsou teoretické a praktické nástroje vhodné pro tvorbu modelů systémově vymezených procesů a modelování a simulace složitých dynamických systémů.

Z toho vyplývá potřeba využívání moderních inteligentních laboratoří a simulátorů různých procesů v kybernetickém prostoru. Jedná se zejména o simulaci moderních kybernetických útoků a proti nim zaměřené obrany systémů, a dále o simulaci již probíhající kybernetické války ve světě a jí odpovídajících reakcí obranných.

Nové pojetí kybernetického prostoru a z něho vyrůstající nová „učící se organizace“ dává také nový pohled na chápání bezpečných procesů v řízení definovaných reálných systémů (organizací). Ukazuje se nutnost systémově vymezit vhodné oblasti vzdělávání pro teorii a praxi odpovídající novým modelům kybernetické bezpečnosti a hledat možnosti nových způsobů využití informačních a komunikačních technologií při výuce.[1, 2] Rovněž je třeba hledat nová pravidla bezpečného provozování různých aktivit v kybernetickém prostoru globalizovaného světa, a tím alespoň trochu omezit některé projevy kyberterorismu, kyberšpionáže, kyberšikany apod.

Výše uvedeným potřebám a pojetím odpovídá zaměření uzavřené smlouvy mezi PA ČR v Praze a Univerzitou Tomáše Bati ve Zlíně, fakultou logistiky a krizového řízení v Uherském Hradišti. Smlouva má především dát základ pro výměnu potřebných informací a odborných podnětů pro vědeckou a výzkumnou činnost. Dále má směrovat získané poznatky do pedagogické práce učitelů i u jiných programů a také dát odpovídající podněty na inovace laboratoří kybernetické bezpečnosti pro studenty bakalářských studijních oborů a aplikované kybernetické bezpečnosti pro magisterské studium. Vše by mělo být systémově pojaté jako nové pracoviště, soustřeďující studium praktického generování kybernetických útoků a adekvátní kybernetickou obranu na virtuálních modelech podniků a organizací. Cílem pracoviště je také a soustředit studující a pedagogy na studium metodik zajišťování kybernetické bezpečnosti a vytváření odpovídající báze znalostí

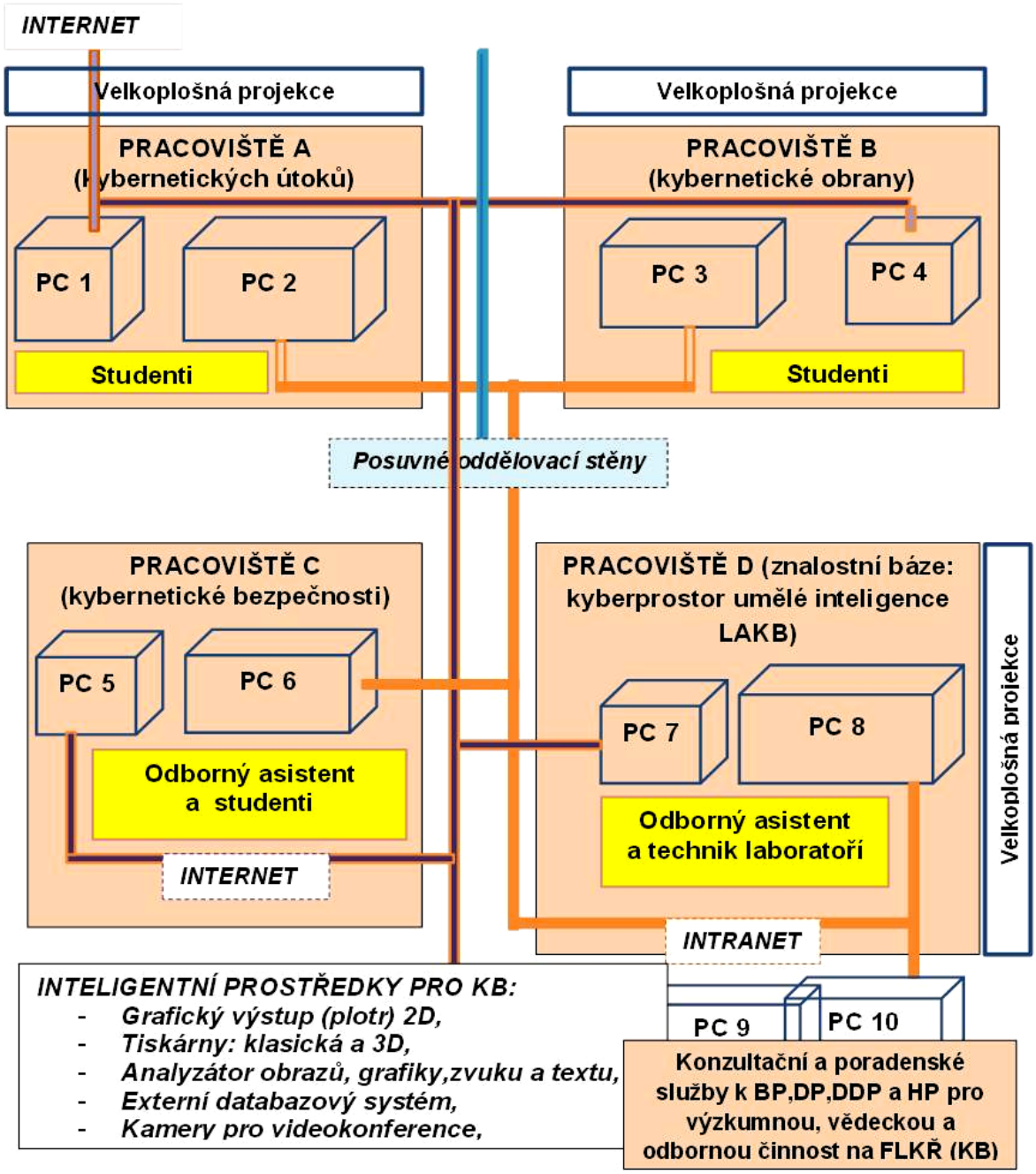
[1] JANKOVÁ, M. a J. DVOŘÁK. Možnosti IT vzdělávání na virtuálních univerzitách. In: *Information Technology for Practice* 2013. Frýdek-Místek: Tiskárna Kleinwachter, 2013. ISBN: 978-80-248-3223-4. s. 123–130.

[2] CARMENADO, I., J. PUENTE a F. GAJARDO. Behavior competence development through e-learning: experience at the undergraduate level in the context of Aula a Distancia Abierta (ADA) Madrid, Spain. In: *Procedia Social and Behavioral Sciences, 3rd World Conference on Educational Sciences - 2011*. Istanbul: Elsevier, 2011. Volume 15, str. 111–119.

v souvislosti s kybernetickou bezpečností jako vědomostní základny budoucích nových studentů - doktorandů a případně i habilitantů.

Výstupy řešení naší spolupráce na vědeckovýzkumném úkolu budou také zaměřeny na:

- ochranu informačních a komunikačních aktiv z pohledu kybernetické bezpečnosti a procesního inženýrství,
- definování kybernetického prostoru pro možné rozpoznávání zranitelných míst a identifikování bezpečnostních hrozeb,
- vyjádření bezpečnostního incidentu jako stavu informačních aktiv a popisu bezpečnostní události ve stavovém prostoru modelu kybernetického systému.



Obr. 1 Návrh laboratoře aplikované kybernetické bezpečnosti (LAKB) pro výuku předmětů kybernetické bezpečnosti s vybavením i pro CAD.

Technické prostředky

a) Internet
   Síť počítačů PC1, PC4, PC5, PC7 k rychlému připojení k internetu s možností online práce s prostředky pro kybernetickou bezpečnost (s odpovídající šířkou pásma periferních jednotek (grafických vstupů a výstupů) pro a práci s komunikačními prostředky, videem apod. v reálném čase).
b) Intranet
   Lokální síť počítačů PC2, PC3, PC6, PC8 (PC9, PC10 ve specializovaném pracovišti) bezpečnostně oddělených od internetu a vybavených:
   - dostatečně výkonnými počítači,
   - dvěma monitory u každého počítače v této lokální síti počítačů s odpovídajícími technickými prostředky komunikace (myš 2D a 3D, a vybranými inteligentními komunikačními prostředky: kamera a mikrofon…).
c) Velkoplošná projekce
   U každého pracoviště vytvořit odpovídající velkoplošnou projekci (TV nebo dataprojektory) řešených úloh a zadaných úkolů s cílem sledování následujících činností:
   - z pracoviště A provádění kybernetických útoků na modelu právě řešeném,
   - z pracoviště B provádění online opatření proti útokům ve formě kybernetické obrany na modelu právě řešeném,
   - z pracoviště C sledování a řízení prováděných kybernetických útoků na pracovišti A a kybernetické obrany na pracovišti B,
   - z pracoviště D sledování a ovlivňování činností pracovišť A, B a C a zkoumání těchto činností v adaptabilním prostředí s cílem vytvářet metodiku a modely pro zajištění kybernetické bezpečnosti v řešené oblasti.

Programové prostředky

a) Na počítačích připojených k internetu
   - Prostředky SW pro komunikaci po internetu s vnějším a vnitřním prostředím.
b) Na počítačích připojených k intranetu
   - Programy typu CAD s některými moduly (stavebnictví - modely budov, elektroinstalace, vodoinstalace apod., strojírenství, elektrotechnika a případně další), zvláště s těmi, které obsahují modely bezpečnosti (například statiky budov, energetické náročnosti výroby v nových technologiích apod.).

Organizační prostředky

a) Na každém pracovišti (A, B, C) zabezpečit vhodné pracovní prostředí pro 4 účastníky modelování tj. 4 (osoby) x 3 (pracoviště) = 12 vhodných pracovišť pro osoby u PC.
b) Na pracovišti C vytvořit serverové řízení celé laboratoře odborný asistent KB pro modelování), na pracovišti D vytvořit perspektivně místo pro jednoho odborného pracovníka v oblasti umělé inteligence pro modely KB, a dále pracoviště pro trvalý dozor jednoho technika nad provozuschopností pracoviště (pro bezpečnou a kvalitní činnost HW, SW a OW na všech pracovištích a osobní odpovědnost za provozuschopnost uvedených prostředků).
c) Na pracovišti PC9 a PC10 vytvořit v rámci konzultační a poradenské služby k BP, DP, DDP a HP pro výzkumnou, vědeckou a odbornou činnost odpovídající zázemí pro tuto integrační činnost procesů KB.

ZÁVĚR

Předchozí text je rozdělen na tři hlavní části:

1. diskusi systémového vymezení vědního oboru Kybernetika a odpovídající oblasti Kybernetická bezpečnost,

2. informaci o hledání nejvhodnější spolupráce při řešení vědecko-výzkumné práce v této oblasti,
3. návrh laboratoře aplikované kybernetické bezpečnosti pro výuku předmětů kybernetické bezpečnosti.

Část 1. zahrnuje také stručnou diskusi o souvislosti uvedených pojmů s exaktní teorií informace a dalšími obory, zvláště s teorií systémů. Bylo nutné zmínit zákon o kybernetické bezpečnosti a rovněž nařízení vlády č. 275/2016 Sb. o oblastech vzdělávání ve vysokém školství pro bezpečnostní obory.

Část 2. stručně popisuje důvody, které vedly k uzavření smlouvy mezi PA ČR v Praze a Univerzitou Tomáše Bati ve Zlíně, fakultou logistiky a krizového řízení v Uherském Hradišti. Jako hlavní důvody uvádíme potřebu využívání moderních inteligentních laboratoří k modelování a simulaci složitých dynamických procesů a systémů v kybernetickém prostoru. Rovněž uvádíme, k čemu především by tato spolupráce měla sloužit.

Část 3. uvádí schéma prvního návrhu uvedené laboratoře a stručný popis technických, programových a organizačních prostředků, které jsou k realizaci tohoto návrhu potřebí.

ZOZNAM POUŽITEJ LITERATÚRY

CARMENADO, I., J., PUENTE a F. GAJARDO. Behavior competence development through e-learning: experience at the undergraduate level in the context of Aula a Distancia Abierta (ADA) Madrid, Spain. In: *Procedia Social and Behavioral Sciences*, 3rd World Conference on Educational Sciences - 2011. Istanbul: Elsevier, 2011. Volume 15, s. 111–119.

JANKOVÁ, M. a J. DVOŘÁK. Možnosti IT vzdělávání na virtuálních univerzitách. In: *Information Technology for Practice* 2013. Frýdek-Místek: Tiskárna Kleinwachter, 2013. s. 123–130. ISBN: 978-80-248-3223-4.

Příspěvek je výstupem řešení projektu specifického výzkumného úkolu č. 2 FBM „Kybernetická bezpečnost a ochrana kritické informační infrastruktury“ Policejní akademie ČR v Praze.

ADRESA

Ing. Vladimír ŠULC, Ph.D., RNDr. Václav HNÍK, CSc.
Policejní akademie ČR v Praze
Katedra managementu a informatiky
sulc@polac.cz, hnik@polac.cz

INTERNET JAKO NÁSTROJ RADIKALIZACE OSAMĚLÝCH VLKŮ

Tomáš ZEMAN, Jan BŘEŇ, Rudolf URBAN

Univerzita obrany v Brně

Abstrakt: *tPříspěvek je literární rešerší problematiky využití internetu ze strany osamělých vlků. Jedná se o radikálně orientovanou osobu, která připravuje teroristické útoky samostatně, bez přímé podpory ze strany teroristické organizace. Počet teroristických útoků osamělých vlků přitom v posledních dvou desetiletých významně vzrůstá jak na území Spojených států (USA) tak v rámci Evropské unie (EU). Internet je pro osamělé vlky jednak zdrojem informací, jednak výhodným prostředkem pro komunikaci s dalšími radikály. Na druhou stranu, využívání internetu osamělými vlky pro tyto účely, dává protiteroristickým jednotkám prostor pro jejich včasnou identifikaci. Metody identifikace radikálních autorů na internetu jsou ovšem zatím stále ve stádiu vývoje a pro jejich efektivní použití bude ještě nutné překonat některé metodické problémy.*

Klíčová slova: *terorismus, osamělý vlk, internet, radikalizace, identifikace.*

ÚVOD

V odborných publikacích lze nalézt několik definic charakterizujících pojem „osamělý vlk“, popř. „osamělý aktér“ v oblasti terorismu. Všechny definice se nicméně shodují v tom, že se jedná o radikálně orientovanou osobu, která není v přímém kontaktu s jakoukoliv teroristickou skupinou a jejími aktivitami. Vyznačuje se negativními protispolečenskými tendencemi končícími realizaci násilných činů. Teroristické útoky připravují tito aktéři samostatně a je proto velmi složité předem identifikovat jejich cíle, záměry a způsoby provedení útoku. V případě osamělých vlků se nelze infiltrovat do žádných struktur, nebo se s nimi cíleně sbližovat. Takovéto postupy u této kategorie útočníku nelze uplatit. Jedná se o sólové hráče, kteří plánují a připravují své teroristické akce sami a zpravidla nekooperují s ostatními.

Ne vždy se však jedná o sociálně vyloučené osoby. Dostupná data naopak naznačují, že téměř polovina osamělých vlků své extrémistické postoje dává nějakým způsobem najevo dříve, než spáchají teroristický útok (Ellis et al. 2016). Své úmysly obvykle naznačují blízkým přátelům nebo rodinným příslušníkům, stejný význam má však v současnosti také sdělování názorů na internetu, přičemž lze předpokládat, že význam internetu bude v tomto směru nadále vzrůstat. Např. Semenov et al. (2013) zjistila, že většina tzv. „školních střelců“ oznámila své úmysly předem na internetových diskuzních fórech. Internet však není pro osamělé vlky pouze nástrojem pro prezentaci vlastních postojů, ale velmi často také zdrojem jejich radikalizace. Hamm & Spaaij (2015) upozornili na změny v mechanismu radikalizace „osamělých vlků“ v USA. Uvádějí, že před 11. září 2001 byla jejich radikalizace spojena nejčastěji s předchozím členstvím v extremistické skupině, zatímco od 11. září 2001 byl tento zdroj radikalizace postupně nahrazen internetem.

VÝVOJ POČTU TERORISTICKÝCH ÚTOKŮ SPÁCHANÝCH OSAMĚLÝMI VLKY

O vývoji počtu teroristických útoků, které byly spáchány „osamělými vlky“, nebyly až donedávna k dispozici prakticky žádné relevantní údaje. V současnosti již existuje několik specializovaných databází zaměřených na evidenci tohoto typu teroristických útoků, např. databáze CLAT (Ellis et al. 2016). Pro účely tohoto článku byly použity údaje ze dvou databází, u kterých byly publikovány meziroční statistiky počtu teroristických útoků, resp. případů „osamělých vlků“.

Prvním zdrojem informací je americká databáze „osamělých vlků“, kterou shromáždili a publikovali Hamm & Spaaij (2015). Databáze zahrnuje celkem 98 případů „osamělých vlků“, kteří vykonali teroristické útoky ve Spojených státech (USA) mezi lety 1940 a 2013. Autoři

uvádějí, že jednotlivé osoby byly zařazeny do databáze jen tehdy, pokud byly splněny následující 4 podmínky:

- 1) Jednalo se o politické násilí spáchané jednotlivci, kteří jednali na vlastní pěst
- 2) Tito jednotlivci nepatřili do žádné organizované teroristické skupiny nebo sítě
- 3) Jednali nezávisle na vůdci nebo hierarchii
- 4) Jejich taktika a metody byly zvoleny těmito jednotlivci bez přímého rozkazu nebo instrukcí z okolí

Druhým zdrojem informací je evropská databáze CLAT (Countering Lone-Actor Terrorism database), která zahrnuje 98 připravovaných teroristických útoků „osamělých vlků", z nichž 72 bylo skutečně provedeno (Ellis et al. 2016). Jedná se o teroristické útoky připravované nebo uskutečněné ve 28 zemích Evropské unie (EU), Norsku nebo Švýcarsku mezi lety 2000 a 2014. Do databáze byly zařazeny pouze ty teroristické útoky, které splnily následujících 6 kritérií:

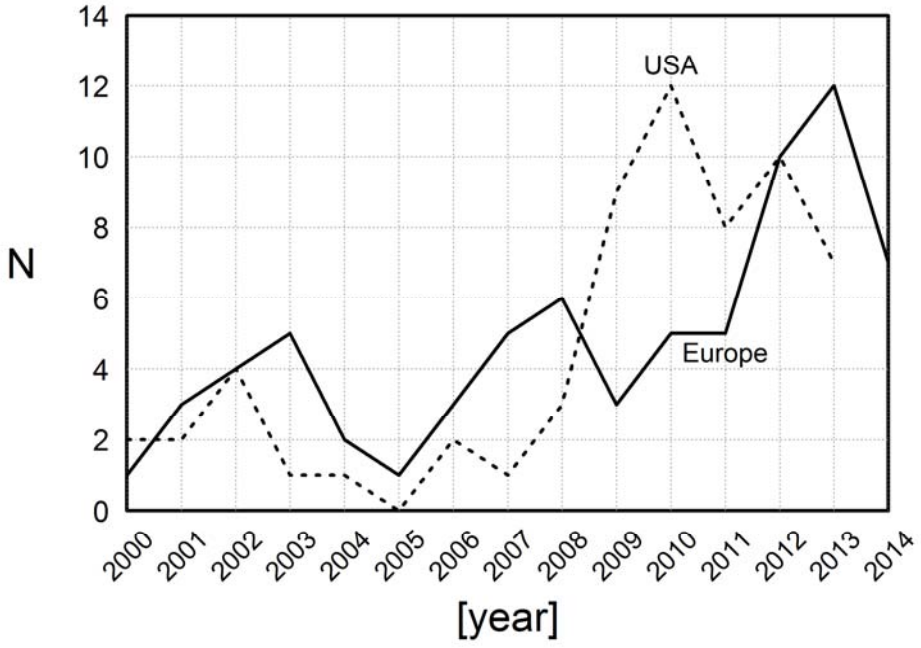
- 1) Násilí, nebo hrozba násilí byly buď naplánovány, nebo uskutečněny
- 2) Jednalo se o jednotlivce, dvojice nebo trojice útočníků
- 3) Útočník jednal bez jakékoliv přímé podpory na úrovni plánování, přípravy a provedení útoku
- 4) Útočníkovo rozhodnutí jednat nebylo přímo ovlivňováno žádnou skupinou ani jinými osobami
- 5) Motivací nebyl pouze osobní materiální zisk
- 6) Cíl útoku přesahuje osoby, které byly útokem přímo zasaženy

Jak upozorňují Ellis et al. (2016), u databáze CLAT nelze vyloučit určitou míru zkreslení, neboť informace o jednotlivých teroristických činech pocházejí pouze z veřejně dostupných zdrojů. V těchto zdrojích nemusejí být uvedeny všechny podstatné informace o teroristickém útoku, včetně informací, které jsou klíčové pro rozhodnutí o zařazení útoku do databáze. V různých zemích se navíc objevují odchylky v klasifikaci jednotlivých činů a i v mediálním zájmu o tyto činy, což bezprostředně ovlivňuje dostupnost informací ve veřejných zdrojích. Autoři proto předpokládají, že databáze nezahrnuje všechny útoky „osamělých vlků", ke kterým ve sledovaném období skutečně došlo. Připouštějí, že některé teroristické činy „osamělých vlků" mohly z výše uvedených důvodů uniknout jejich pozornosti.

Kritéria pro zařazení do obou databází jsou mírně odlišná, což do jisté míry relativizuje výsledky jejich srovnání. Problematická je zejména skutečnost, že zatímco evropská databáze CLAT (Ellis et al. 2016) je databází teroristických útoků, americká databáze (Hamm & Spaaij 2015) zahrnuje záznamy o samotných „osamělých vlcích". Někteří z nich nicméně mohli v daném roce spáchat více teroristických útoků, což by u evropské databáze CLAT vedlo k více záznamům, zatímco u americké databáze by zůstal záznam jen jeden. Rozdílná jsou u obou databází také kritéria pro zařazení činů, resp. osob do databáze. Nejzásadnější odlišností je v tomto směru skutečnost, že zatímco do evropské databáze CLAT byly zahrnuty také teroristické činy spáchané dvojicemi, či trojicemi pachatelů, americká databáze je omezena striktně na jednotlivce. Domníváme se nicméně, že rozdíly v počtu zařazených teroristických činů způsobené odlišnou metodikou sběru dat budou relativně malé.

Na Obr. 1 je znázorněn vývoj počtu případů osamělých vlků v USA a počtu teroristických útoků spáchaných osamělými vlky v evropských zemích (EU, Norsko, Švýcarsko) od roku 2000 do roku 2014. U obou datových souborů (Hamm & Spaaij 2015; Ellis et al. 2016) je evidentní rostoucí trend v počtu těchto teroristických útoků v průběhu sledovaného období. V USA dosáhl tento trend vrcholu v roce 2010. Do roku 2013 pak roční počet útoků, které byly spáchány „osamělými vlky" mírně klesl. Na rozdíl od USA, byl v Evropě zaznamenán nejvyšší počet teroristických útoků „osamělých vlků" až v roce 2013, což může souviset s počínající migrační vlnou, která následně vyústila v evropskou migrační krizi, nebo souběžnou expanzí Islámského státu. V roce 2014 sice počet útoků mírně poklesl, novější data však nejsou k dispozici, takže nelze soudit, zda se rostoucí

trend ve vývoji počtu útoků skutečně zastavil, nebo jde jen o náhodnou odchylku. Ellis et al. (2016) upozorňují na skutečnost, že část pozorovaného nárůstu počtu teroristických činů lze pravděpodobně přisoudit rozšiřování digitálních archivů, což zvyšuje mediální dosah novějších teroristických činů. Toto vysvětlení však může objasnit nanejvýš menší část popsaného trendu, kdy se počet teroristických útoků „osamělých vlků“ během jednoho desetiletí přibližně ztrojnásobil.



Obr. 1 Vývoj počtu případů osamělých vlků ve Spojených státech (USA) a počtu teroristických útoků spáchaných osamělými vlky v Evropské unii, Norsku a Švýcarsku (Europe) v rozmezí let 2000 až 2014 (zdroj dat: Hamm & Spaaij 2015; Ellis et al. 2016)

INTERNET A OSAMĚLÍ VLCI

Internet je mnohými autory (např. Rudner 2017) považován efektivní komunikační nástroj pro teroristy. Je zdrojem obrovského množství informací, k nimž se lze dostat relativně anonymně a s minimálním vynaložením nákladů ve srovnání s ostatními způsoby komunikaci (např. telefonické spojení, pošta, ústní sdělení). Na druhou stranu, Mueller & Stewart (2015) význam internetu při přípravě a organizaci teroristických útoků zpochybňují s tím, že informace volně dostupné na internetu jsou v drtivé většině případů nekvalitní, nedostatečné a často zavádějící. Úspěšné využití takových informací pro přípravu teroristického útoku (např. domácí výroba bomby) bez předchozích praktických zkušeností a vědomostí považuje za nepravděpodobné. Mueller & Stewart (2015) analyzovaly ve své studii 61 případů útoků osamělých vlků na objekty nebo občany USA od 11. září 2001. Zjistili přitom, že přestože se mnoho z nich pokusilo s využitím návodů z internetu vytvořit podomácku vyrobenou bombu, pouze v jednom případě skončil tento pokus úspěchem (bombový útok na bostonský maraton z 15. dubna 2013).

Jakkoliv je význam internetu coby zdroje informací praktické povahy, které by mohly být efektivně využity při přípravě teroristických útoků osamělých vlků, omezený, jeho význam při šíření teoretických, resp. ideologických informací je daleko zásadnější. Základním nástrojem pro distribuci tohoto typu informací na internetu jsou:

- A) webové stránky teroristických organizací (pro další informace viz Tsfati & Weimann 2011)
- B) internetová fóra
- C) sociální sítě

Podle Brandona (2008) slouží výše uvedená prostředí jako:

- A) online knihovny teoretických textů (např. náboženské spisy)
- B) vhodné místo pro kazatele (lze zde oslovit spoustu osob, které by na běžné kázání nikdy nepřišli)
- C) místo pro diskuzi o ideologických otázkách

Přestože šíření ideologických informací cestou internetu je nezpochybnitelným jevem posledních dvou desetiletí, vede se stále diskuze o jeho významu. Sageman (2008) se domnívá, že internet má klíčový význam pro samotnou existenci tzv. „odboje bez vůdců". Poukazuje přitom na skutečnost, že internet transformuje mezilidské vztahy do zcela nové sociální struktury, která je pro „odboj bez vůdců" velmi příhodná. Na druhou stranu, ani Sageman (2008) nepředpokládá, že by informace dostupné na internetu byly samy o sobě schopny generovat nové teroristy. Někteří autoři, např. Mueller & Stewart (2015), se navíc domnívají, že internet přináší daleko víc výhod protiteroristickým jednotkám než samotným osamělým vlkům, kteří mají obvykle méně prostředků a horší vzdělání. To bezprostředně souvisí se skutečností, že osamělí vlci po sobě zpravidla zanechávají na internetu velké množství stop a jsou proto relativně snadno dohledatelní.

Dle výsledků výzkumu, který provedli Gill et al. (2017) na souboru 223 osamělých vlků, kteří působili ve Spojeném království (UK) v letech 1990 až 2014, byla u 61 % z nich zjištěna nějaká internetová aktivita související s provedením nebo přípravou teroristického útoku. Jednalo se především o využití internetu při přípravě teroristického útoku (32 % případů), tj. zejména pro získání informací o objektu, který byl cílem útoku, a komunikaci s ostatními radikály na internetu (29 % případů).

Výše uvedené údaje s sebou přinášejí otázky ohledně možností využití online aktivit osamělých vlků pro účely jejich včasné detekce, tj. jejich identifikace ještě předtím než připravovaný teroristický čin provedou. Osamělí vlci, kteří na internetu vyjadřují své radikální názory a postoje, mohou být dohledání prostřednictvím automatických nebo poloautomatických metod. Cohen et al. (2014) poukazují na to, že pokud mají být tyto metody využitelné v praxi, musí umožňovat přinejmenším poloautomatické provedení následujících úkonů:

- A) překlad internetových zdrojů (radikálové spolu komunikují v různých jazycích, pro následnou analýzu je proto často nutné původní texty nejprve přeložit)
- B) analýza sentimentu (slouží pro identifikaci radikálních autorů na základě klíčových slov v jejich příspěvcích v diskuzních fórech apod.)
- C) mapování webových stránek s radikálním obsahem
- D) identifikace autorů vytipovaných příspěvků (radikální autoři na internetu obvykle publikují pod přezdívkou, své skutečné jméno zpravidla neuvádějí, v poslední fázi je proto nutné zjistit totožnost vytipovaných radikálních autorů)

Jak ukázali Scrivens et al. (2017) z technického hlediska lze výše uvedené překážky v dnešní době již překonat. Ani úspěšná identifikace radikálních autorů nám ovšem nezaručí, že osoby, které takto odhalíme, jsou skutečně osamělými vlky. Jak ostatně poukazují sami Scrivens et al. (2017), radikální postoje některého uživatele internetu ještě neznamenají, že tento uživatel by byl v reálném světě schopen provést teroristický útok, natož to, že nějaký teroristický útok skutečně připravuje.

ZÁVĚR

V posledních dvou desetiletích došlo na území USA a EU k významnému nárůstu počtu teroristických útoků spáchaných osamělými vlky. Tento nárůst může souviset s prudkým rozvojem internetu, k němuž došlo ve stejném čase. Je prokazatelné, že velká část osamělých vlků internet využívá jak při přípravě teroristického útoku tak při komunikaci s ostatními radikály na internetu. Na druhou stranu, užitečnost a význam internetu pro osamělé vlky jsou některými autory zpochybňovány, neboť na internetu jsou velmi často uveřejňovány nepřesné, neúplné a zavádějící informace. Internet může být navíc efektivně využit nejen osamělými vlky při přípravě teroristických činů, ale také protiteroristickými jednotkami při identifikaci osamělých vlků. V současné době jsou již k dispozici nástroje umožňující identifikaci radikálních autorů na základě

analýzy sentimentu. Slabinou tohoto přístupu ovšem zůstává skutečnost, že zdaleka ne všichni autoři radikálních příspěvku mají v úmyslu provést teroristický útok.

ZOZNAM POUŽITEJ LITERATÚRY

Brandon, J. (2008). Virtual Caliphate Islamic extremists and their websites. Centre for Social Cohesion.

Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence, 26(1), 246–256. https://doi.org/10.1080/09546553.2014.849948

Ellis, C., Pantucci, R., van Zuijdewijn, J. de R., Bakker, E., Gomis, B., Palombi, S., & Smith, M. (2016). Lone-Actor Terrorism Final Report.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes. Criminology and Public Policy, 16(1), 99–117. https://doi.org/10.1111/1745-9133.12249

Hamm, M., & Spaaij, R. (2015). Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies.

Mueller, J., & Stewart, M. G. (2015). Terrorism, counterterrorism, and the Internet: The American cases. Dynamics of Asymmetric Conflict, 8(2), 176–190. https://doi.org/10.1080/17467586.2015.1065077

Rudner, M. (2017). "Electronic Jihad ": The Internet as Al Qaeda's Catalyst for Global Terror. Studies in Conflict & Terrorism, 40(1), 10–23. https://doi.org/10.1080/1057610X.2016.1157403

Sageman, M. (2008). Leaderless Jihad: Terror Networks in the Twenty-First Century. Philadelphia: University of Pennsylvania Press.

Scrivens, R., Davies, G., & Frank, R. (2017). Searching for signs of extremism on the web: an introduction to Sentiment-based Identification of Radical Authors. Behavioral Sciences of Terrorism and Political Aggression, 0(0), 1–21. https://doi.org/10.1080/19434472.2016.1276612

Semenov, A., Veijalainen, J., & Kyppo, J. (2010). Analysing the presence of school-shooting related communities at social media sites. International Journal of Multimedia Intelligence and Security, 1(3).

Tsfati, Y., & Weimann, G. (2002). www.terrorism.com: Terror on the Internet. Studies in Conflict and Terrorism, 731, 317–332. https://doi.org/10.1080/1057610029010121

ADRESA

Tomáš ZEMAN, Jan BŘEŇ, Rudolf URBAN
Katedra krizového řízení
Fakulta vojenského leadershipu
Univerzita obrany v Brně
Kounicova 65, 662 10 Brno, Česká republika
tomas.zeman2@unob.cz

ZÁVER

Záverečné slovo mal prof. PhDr. Ján BUZALKA, CSc., ktoré najdete vo videopríspevkoch.

MENNÝ REGISTER

ISBN 978-80-8054-750-9
EAN 9788080547509

KYBERNETICKÁ BEZPEČNOSŤ AKO NOVÝ PRVOK V REALIZÁCII OPATRENÍ KRÍZOVÉHO MANAŽMENTU

Z medzinárodnej vedeckej video konferencie,
ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave

Zostavili:	mjr. Ing. Marian SUJA, PhD., pplk. Ing. Igor PAVLOVIČ
Vydala:	Akadémia Policajného zboru v Bratislave
Počet strán:	88
Náklad:	40 CD
Rok vydania:	2018
Vydanie:	prvé
Technická redakcia:	mjr. Ing. Marian SUJA, PhD., pplk. Ing. Igor PAVLOVIČ
Jazyková úprava:	za obsah publikovaných príspevkov zodpovedajú autori

ISBN 978-80-8054-750-9
EAN 9788080547509