Akadémia Policajného zboru v Bratislave

Katedra informatiky a manažmentu

Vedecká konferencia s medzinárodnou účasťou

AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI
(v podmienkach bezpečnostných zložiek)

Zborník príspevkov

Bratislava

2019

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

ZBORNÍK PRÍSPEVKOV

z vedeckej konferencie s medzinárodnou účasťou

Aktuálne výzvy kybernetickej bezpečnosti
(v podmienkach bezpečnostných zložiek)

konanej dňa 4. 6. 2019

pod záštitou rektorky Akadémie Policajného zboru v Bratislave
Dr. h. c. prof. JUDr. Lucie Kurilovskej, PhD.
a riaditeľa Národného bezpečnostného úradu
plk. JUDr. Romana Konečného

Bratislava 2019

Hlavní partneri:

FORTINET

Microsoft ASBIS SUCCESS THROUGH FOCUS

SOITRON INSPIRUJEME K NAROCNOSTI

Mediální partneri:

PC REVUE

TOUCHIT

Partneri:

RCTT COMMUNICATION

veri2

DOKUMENTA

INTERWAY

SPOJNET

virtė

DELL EMC

veracomp we inspire IT

Vedecká konferencia bola organizovaná v rámci realizácie projektu zameraného na prevenciu páchania počítačovej kriminality s názvom „Správaj sa bezpečne!“

VEDECKÝ VÝBOR KONFERENCIE:

Dr. h. c. prof. JUDr. Lucia KURILOVSKÁ, PhD. (Akadémia PZ v Bratislave)
Dr. h. c. prof. Ing. Pavel NEČAS, PhD., MBA (Univerzita Mateja Bela v Banskej Bystrici)
prof. Ing. Marcel HARAKAĽ, PhD. (Akadémia ozbrojených síl v Liptovskom Mikuláši)
prof. Ing. Zdeněk DVOŘÁK, PhD. (Žilinská univerzita v Žiline)
prof. JUDr. Jozef METEŇKO, PhD. (Akadémia PZ v Bratislave)
plk. doc. Ing. Ľubica BARIČIČOVÁ, PhD. (Akadémia PZ v Bratislave)
doc. Mgr. Dr. Vladimír BLAŽEK, CSc. (Akadémia PZ v Bratislave)
doc. Ing. Martin HROMADA, Ph.D. (Univerzita T. Bati v Zlíne)
pplk. doc. Ing. Petr HRŮZA, Ph.D. (Univerzita obrany, Brno)
doc. Ing. Antonín KORAUŠ, PhD., LL.M., MBA (Akadémia PZ v Bratislave)
pplk. doc. PhDr. Magdaléna ONDICOVÁ, PhD. (Akadémia PZ v Bratislave)
plk. doc. Ing. Stanislav ŠIŠULÁK, PhD. (Akadémia PZ v Bratislave)
doc. Ing. Jan VÁŇA, CSc. (Akadémia PZ v Bratislave)
JUDr. Miroslav BRVNIŠŤAN, PhD. (AFCEA Slovakia)
Ing. Jozef HALCIN (Ministerstvo vnútra SR)
plk. Mgr. Rastislav JANOTA (Národný bezpečnostný úrad)
por. Mgr. Matej ŠALMÍK (Národný bezpečnostný úrad)
plk. Mgr. Stanislav ŠPANKO (Prezídium PZ)
pplk. Ing. Mgr. Jana TKÁČIKOVÁ (Prezídium PZ)

ORGANIZAČNÝ VÝBOR KONFERENCIE:

mjr. JUDr. Matej KOSTREC, PhD.
npor. Bc. Mgr. Liliana RÉVESZOVÁ
Mgr. Štefan ZACHAR
pplk. RNDr. Tatiana HAJDÚKOVÁ, PhD.
por. Mgr. Jana KUCHTOVÁ
JUDr. Katarína JUNASOVÁ
pplk. Ing. Igor PAVLOVIČ
Ing. Pavol KOPAČKA - AFCEA Slovakia
Ing. Ladislav KOLLÁRIK - AFCEA Slovakia

RECENZENTI:

doc. Ing. Anna HAMRANOVÁ, PhD.
RNDr. Eva KOSTRECOVÁ, PhD.

ZOSTAVILI:

Mgr. Štefan ZACHAR
npor. Bc. Mgr. Liliana RÉVESZOVÁ

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.
ISBN 978-80-8054-819-3
EAN 9788080548193

Obsah

Úvodné slovo **7**

Ciele a tematické zameranie konferencie **8**

Program konferencie **9**

Ciele kyberútokov sa rozširujú na menej chránené zariadenia sietí **11**

Alexander Hambalík

Vzdělávání v oblasti kybernetické bezpečnosti **21**

Petr Hrůza

Kybernetický boj ako jeden z nekonvenčných spôsobov boja **25**

Radoslav Ivančík

Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí **35**

Radoslav Ivančík, Ľubica Baričičová

Podvod – jedno z najväčších bezpečnostných rizík **48**

Antonín Korauš, Stanislav Backa, Matej Bárta

Alternatívne kybernetické meny v súčasnosti **54**

Antonín Korauš, Pavel Kelemen, Stanislav Backa, Jozef Polák

Riadenie rizika podvodu z pohľadu bezpečnosti a včasného odhalenia **66**

Antonín Korauš, Pavel Kelemen, Štefan Zachar

Procesné riadenie – firemný nástroj bezpečnosti, ochrany majetku a neželanej manipulácie s údajmi **72**

Antonín Korauš, Jozef Polák, Jana Kuchtová

Ochrana osobných údajov - Výsledky výskumov vykonaných vo Francúzsku, na Slovensku a v Českej republike **78**

Matej Kostrec

Digitálna stopa ako základ kybernetickej bezpečnosti **97**

Jana Kuchtová

Vybrané aspekty vzdelávania v oblasti kybernetickej bezpečnosti na základných školách **102**

Filip Lenko

Príprava bezpečnostných manažérov v oblasti kybernetickej bezpečnosti - výsledky testovania 108

Ladislav Mariš, Viktor Šoltés

Úloha sociológie v rozvoji digitálnych kompetencií študentov Akadémie PZ v Bratislave 114

Karol Murdza

Aktuálny pohľad na vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni 125

Pavel Nečas, Radoslav Ivančík

Kyberpriestor, kybernetická kriminalita a komparácia jej nárastu vzhľadom na dynamiku jej vývoja 138

Liliana Réveszová

Problematika sextingu u detí a mládeže 149

Zuzana Dobrovanov Šimová

„Fake news“ a propaganda v kybernetickom priestore..... 156

Stanislav Šišulák, Martina Cíchová

Požiadavky na vzdelávanie používateľov informačných systémov v oblasti kybernetickej bezpečnosti 168

Viktor Šoltés, Anton Šiser

Role manažera kybernetické bezpečnosti v procesu řízení hrozeb 176

Vladimír Šulc

Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom..... 185

Kristián Ujváry, Jana Kuchtová

Využitie znakov digitálnej stopy pri riešení problematiky blockchain 196

Štefan Zachar

Recenzné posudky 206

Úvodné slovo

Vážené dámy, vážení páni!

Dovoľte, aby som úvodom poďakoval organizátorom tohto podujatia – občianskemu združeniu AFCEA Slovakia a Katedre informatiky a manažmentu Akadémie Policajného zboru v Bratislave – za zorganizovanie vedeckej konferencie s medzinárodnou účasťou, ktorá je pokračovaním pilotnej medzinárodnej vedeckej konferencie organizovanej v roku 2018 so zameraním na prevenciu počítačovej kriminality. Osobitne chcem vyjadriť ocenenie zástupcom súkromného sektora za podporu a prezentáciu technických a technologických riešení spojených s obsahovým zameraním podujatia.

Potreba komunikácie, výmeny informácií a skúseností medzi aplikačnou praxou a akademickou obcou sa s narastajúcou informatizáciou spoločnosti nevyhýba ani bezpečnostných zložkám.

Bezpečnosť kybernetického prostredia a bezpečnosť občana v kybernetickom prostredí je čoraz náročnejšou úlohou. Aby ju bolo možné zabezpečiť, je potrebné o téme nielen diskutovať, ale okrem teoretických znalostí preniesť do policajnej praxe aj nové praktické poznatky z oblasti využitia modernej techniky a technológií.

Policajný zbor totiž bez moderných technológií nedokáže aktuálne držať krok so sofistikovanými metódami páchania kriminality.

Miesto akademickej pôdy preto spočíva tak vo výchove budúcich príslušníkov Policajného zboru a pracovníkov verejnej správy, ako aj v prepájaní teórie s praxou. To nie je možné bez rozvoja teoretických poznatkov, vedomostí a praktických znalostí.

Som presvedčený, že takéto podujatia sú dobrou cestou, ako to reálne zabezpečiť.

Vyslovujem presvedčenie, že podpora zo strany súkromného sektora sa pretaví aj do podpory a realizácie vedecko-výskumných projektov, zapojenia študentov do praxe a aj prezentácií technológií a ich možností v rámci vyučovacieho procesu.

Ctení, čitatelia,

prajem Vám príjemné čítanie zborníka z predmetnej vedeckej konferencie plné inšpiratívnych informácií.

plk. doc. Ing. Stanislav Šišulák, PhD.
prorektor
pre informatizáciu a koordináciu
s policajnou praxou
Akadémia Policajného zboru v Bratislave

Ciele a tematické zameranie konferencie

Hlavným cieľom konferencie je vymedzenie a analyzovanie aktuálnych problémov spojených s kybernetickou bezpečnosťou, zovšeobecnenie teoretických prístupov a praktických skúseností kompetentných subjektov jednotlivých bezpečnostných zložiek ako základného predpokladu pre vytvorenie systematického prístupu k oblasti kybernetickej bezpečnosti a návrhu systému vzdelávania v štátnej a verejnej správe. K ďalším cieľom konferencie patrí identifikácia predpokladov a teoretických väzieb na prepojenie teórie s aplikačnou praxou, ako aj zabezpečenie transferu relevantných poznatkov do praxe subjektov štátnej a verejnej správy pre empirické skúmanie špecifických problémov a aktuálnych potrieb bezpečnostnej praxe v oblasti zvyšovania úrovne kybernetickej bezpečnosti SR.

V zmysle vytýčených cieľov a obsahového zamerania konferencie sa budú jednotlivé vystúpenia a prezentované príspevky koncentrovať najmä na nasledovné okruhy súvisiace s predmetnou problematikou:

- vedecké základy vzťahu ľudského faktora a kybernetickej bezpečnosti,
- možnosti a perspektívy vzdelávania v oblasti kybernetickej bezpečnosti,
- východiská skvalitňovania spolupráce Akadémie Policajného zboru v Bratislave s ostatnými vysokými školami doma i v zahraničí, ako aj s inými inštitúciami v oblasti kybernetickej bezpečnosti s jej dopadom na systém odborného vzdelávania nielen študentov ale aj zamestnancov štátnej a verejnej správy,
- bezpečnosť občana v kybernetickom prostredí, možnosti ochrany občana v oblasti kybernetickej bezpečnosti (od analýzy hrozieb, pomoci bezpečnostných zložiek občanovi až po vzdelávanie),
- teoretické východiská riešenia prevencie kybernetickej kriminality,
- spolupráca so súkromným sektorom.

Pôjde predovšetkým o riešenie nasledovných otázok:

- aktuálne problémy a výzvy ochrany kybernetického priestoru,
- postavenie a úlohy bezpečnostných zložiek pri realizácii bezpečnosti kybernetického priestoru,
- analýza možných činností a úloh PZ v oblasti kybernetickej bezpečnosti,
- trestnoprávne aspekty kybernetickej kriminality,
- technické aspekty kybernetickej bezpečnosti - analýza rizík, odhaľovanie a dokumentovanie bezpečnostných incidentov,
- zaisťovanie digitálnych stôp,
- miesto a úloha súkromného sektora pri zabezpečovaní kybernetickej bezpečnosti a spolupráca s bezpečnostnými zložkami,
- úlohy Akadémie Policajného zboru v Bratislave vyplývajúce z realizácie Koncepcie kybernetickej bezpečnosti SR vo vzťahu k vzdelávaniu príslušníkov PZ v tejto oblasti,
- spolupráca Akadémie Policajného zboru v Bratislave a Národného bezpečnostného úradu na vytvorení systému vzdelávania v oblasti kybernetickej bezpečnosti,
- úloha súkromného sektora pri budovaní odborných a technických spôsobilostí bezpečnostných zložiek.

Program konferencie

Otvorenie (8.00 - 8.45 h)

- plk. doc. Ing. Stanislav Šišulák, PhD. - prorektor pre informatizáciu a koordináciu s policajnou praxou
- JUDr. Miroslav Brvnišťan, PhD. - AFCEA Slovakia

1. **Blok (8.45-10:15 h): Bezpečnosť občana a možnosti prevencie kybernetickej kriminality, ciele a perspektívy vzdelávanie v oblasti kybernetickej bezpečnosti**

    1. Petr Hrůza – Katedra taktiky, Fakulta vojenského leadershipu, Univerzita obrany v Brně
    Vzdělávaní v oblasti kybernetickej bezpečnosti

    2. Jana Uramová - Fakulta riadenia a informatiky, Žilinská univerzita v Žiline
    Vzdelávanie v kybernetickej bezpečnosti a efektívne monitorovanie a detekcia anomálií v sieťovej prevádzke

    3. Zdeněk Dvořák - Žilinská univerzita v Žiline
    Nutnosť celoživotného vzdelávania v oblasti kybernetickej bezpečnosti

    4. Petr Jirásek
    Kybernetické hrozby – jak na ně? Vzdelávanie, kybernetická súťaž

    5. Jaroslav Sivák, Albert Vajányi - VIRTE
    Kybernetická bezpečnosť v praxi

2. **Blok (10:30-12:00 h): Kybernetická bezpečnosť - úlohy bezpečnostných zložiek, analýza a dokumentovanie bezpečnostných incidentov a digitálnych stôp, miesto a úlohy súkromného sektora pri zabezpečovaní kybernetickej bezpečnosti, spolupráca s bezpečnostnými zložkami**

    1. Rastislav Janota - riaditeľ Národnej jednotky SK-CERT NBÚ
    Úloha Národnej jednotky SK-CERT v procese reakcie na kybernetické bezpečnostné incidenty u Prevádzkovateľov základných služieb

    2. Peter Veselý - Fakulta managementu UK v Bratislave
    Etický hacking ako aktívna súčasť kybernetickej obrany

    3. Ivan Bacigál - PPZ - odbor počítačovej kriminality

    4. Jan Pilař - Microsoft
    Pokročilá ochrana koncových zariadení a identít užívateľov, analýza chovania

5. Soitron
   Vnímanie kybernetickych hrozieb na Slovensku

6. Peter Košinár – ESET
   Bezpečnostné incidenty spôsobené cielenými útokmi

3. Blok (12:45-15:30 h): Kybernetická bezpečnosť a súkromný sektor, budovanie odborných a technických spôsobilostí bezpečnostných zložiek, možnosti ochrany občana v oblasti kybernetickej bezpečnosti

1. Matej Šalmík – riaditeľ technická sekcia, odbor kybernetickej bezpečnosti NBÚ
   Národné Table Top cvičenia

2. IBM
   Využitie moderných technológií pre zvýšenie schopností činnosti polície.

3. DOKUMENTA
   Ochrana mailovej komunikácie prostredníctvom šifrovaného mailu

4. SPOJNET
   Zodolnené zariadenia vo výkone činností bezpečnostných zložiek, charakteristika a technické parametre

5. Karol Mareš – VERACOMP SLOVAKIA
   Odhaľte kybernetického útočníka v reálnom čase, ukážka technológií a ich možností, praktické prípady

6. Fortinet
   Fortinet Security Fabric, end-to-end ochrana v prostredí bezpečnostných zložiek

7. Juraj Zelenay, Ľudmila Gregušová - MPI Consulting s.r.o.
   Využitie európskych cloudových technológii na bezpečnú komunikáciu a kolaboráciu-prípadová štúdia

8. Alexander Hambalík - UIM FEI STU v Bratislave
   Ciele kyberútokov sa rozširujú na menej chránené zariadenia sietí

Ciele kyberútokov sa rozširujú na menej chránené zariadenia sietí

Alexander Hambalík

Abstrakt:
Okrem klasickej, výkonnejšej výpočtovej techniky (servery, pracovné stanice, osobné počítače) v súčasnosti zapájame do siete aj také zariadenia, ktoré sú omnoho menej chránené voči útokom. Patria sem hlavne tlačiarne, kopírky, snímače odtlačkov, kamery, zariadenia patriace do IoT a mnoho ďalších z medicínskej, fitnes, resp. wellness oblastí. Namiesto proprietrárneho a jednoduchého riadenia majú už optimalizovaný OS. Môžu spracovávať aj chránené údaje. Uvedomelosť používateľov, správcov sietí, ale ani ochrana zariadení nie je ešte na žiadanej úrovni, preto sa dnes stávajú terčom kyberútokov.
Kľúčové slová:
Sieťové zariadenia pracovísk, optimalizovaný OS, IoT, kyberútoky.

Abstract:
In addition to the classic, more powerful computers (servers, workstations, PC), we connect devices to network, that are less protected against attacks. These devices is mainly printers, copiers, fingerprint readers, cameras, IoT and many devices from medicals, fitness, or wellness areas. Instead of proprietary and simple management, they have optimized OS. These devices can process protected data. Awareness of users, network administrators and the protection of equipment is not on desired level, so today they are target of cyber-attacks.
Key words:
Network devices of workplaces, optimized OS, IoT, cyber-attacks.

Úvod

Obdobie, v ktorom pri pracovnej alebo každodennej činnosti nás obklopujú rôzne zariadenia, trvá už desiatky rokov. Dnes drvivú väčšinu z nich tvoria zariadenia, u ktorých elektronická časť je konštruovaná na báze výpočtovej techniky. Funkčne plnia úlohy, ktoré siahajú od jednoduchého ovládania cez inteligentné riešenia až po „smart“, teda inteligentné zariadenia. Zvláštnu kategóriu tvoria zariadenia internet vecí (IoT), ktoré primárne nie sú určené na komunikáciu s ľuďmi, ale v konečnom dôsledku slúžia pre nich.

Všetky menované zariadenia sa dajú pripojiť dočasne alebo trvalo do siete lokálnej (LAN) alebo rozsiahlej (WAN), ktorej verejne dostupnú časť tvorí internet. Pomocou nich vyhľadávame a získame potrebné informácie, spracúvame, ukladáme alebo archivujeme a ak treba, tlačíme dôležité časti z nich. Naše činnosti a zároveň aj životná úroveň závisí od ich využitia, lebo bez nich niektoré úlohy nemôžeme ani vykonať. Medzi nimi patria vzdialené operácie s bankami, pracoviskami, automatizovaný zber a vyhodnotenie údajov pomocou IoT. Zvláštnu dôležitosť to má v zdravotníctve, organizácii a riadení dopravy, systémoch bezpečnosti v mestách alebo rôzne činnosti v štátnej, vojenskej, justičnej a policajnej sfére.

Cez všetky súčasti týchto systémov môžu prúdiť aj chránené alebo citlivé informácie, ktoré mali by byť dostatočne zabezpečené vhodnou ochranou. Technologickú hranicu zabezpečenia ohraničujú vlastnosti použitého hardvéru. Najslabšie články týchto systémov sa stávajú novými alebo frekventovanejšími cieľmi útokov a rozširujú tak rad potenciálnych cieľov útokov. Dnes okrem klasických počítačových systémov sú častým terčom útokov komponenty inteligentných budov, riadiace systémy áut, koľajových súprav. Výrazné zvýšenie záujmu útočníkov sa registruje o útoky na priestranstvách alebo na pracoviskách zriadené kamerové systémy, medicínske alebo fitnes zariadenia, skenery a v neposlednom rade o skoro všade prítomné tlačiarne.

Prečo práve dnes je o tieto zariadenia zvýšený záujem?

Dôvody môžeme nájsť čiastočne v ich historickom vývoji. Ďalšie dôvody vznikli s globálnym rozvojom a prechodom na používanie nových, najmä sieťových technológií. Na základe analýzy rozvoja môžeme stručne charakterizovať zmeny, ktoré to vyvolali, takto:

Minulosť

- Prvé útoky na počítače (digitálnu infraštruktúru) sú známe už z ranného obdobia využívania tejto techniky.
- Boli to ojedinelé prípady a pre konkrétne stroje.
- Boli cielené skôr na znefunkčnenie činnosti stroja alebo systému.
- **Malý výkon, malá pamäť bez operačného systému na vytvorenie a spustenie škodlivých kódov nebol vhodný.**
- Len malá skupina odborníkov vedela ako presne pracujú.
- Takéto informácie boli ťažko dostupné a realizácia útoku by vyžadovalo nákladné vybavenie.
- **Nepredstavili by hromadnú hrozbu – rôznorodosť strojov, ich hardvérového a softvérového vybavenia.**

Dnes

- Výkonné stroje a siete sú prakticky neustále pod útokom – veľa ľudí vie ako pracujú.
- Na šťastie medzičasom vyvíjali sa aj technológie a prostriedky na ich ochranu.
- Správcovia sietí a používatelia počítačov už vnímajú stav neustáleho ohrozenia.
- Častejšie (skoro povinne) aplikujú pre nich ochranné prvky a riešenia – reverzné inžinierstvo.
- **Dnes pripojiť do siete možno prakticky čokoľvek.** Všetko, čo má vlastný procesor, je pripojiteľný aj na sieť v nejakej forme (IoT, kamery, autá, zdravotnícke a fitnes zariadenia, tlačiarne, skenery (odtlačkov) – obr. 1, atď.).
- **Môžu snímať, spracovať a dočasne (trvalejšie) uchovať cenné alebo aj chránené údaje (podľa GDPR, atď.).**

Útočníci využívajú slabé časti reťazca. Rýchly vývoj málokedy dokáže dostatočne zabezpečiť nové prvky v systéme. **Sú slabo chránené - zároveň (cez sieťové pripojenie) sa rýchlo môžu odhaliť a stať terčom útokov.**

Vývojári majú po odhalení zraniteľnosti veľkú výhodu v tom, že veľmi dobre poznajú zraniteľnosť vykazujúci systém a majú k dispozícii všetky potrebné plány, zdrojové kódy systému. Vo väčšine prípadov dokážu pomerne rýchlo odstrániť objavenú zraniteľnosť.

Útočníci musia k útoku najprv dokonale analyzovať systém, aby mohli naplánovať a realizovať útok. Sieťové pripojenie ale znásobí počet potenciálnych záujemcov o útok. Zvyšuje sa aj pravdepodobnosť systematického alebo náhodného odhalenia zraniteľnosti, pričom útočníci nedodržiavajú žiadne zákony.

Podľa zistiteľných príznakov a zverejnených údajov o bezpečnostných incidentoch je možné usúdiť, že každá strana sa snaží svoje výhody využiť, ale väčšinou len so striedavými úspechmi. Vojnu technológií dodnes ani jedna strana nevyhrala!

Čo môžeme od nich očakávať, keď ich pripojíme na sieť?

Pripojíme ich do siete hlavne preto, lebo očakávame, že ich využiteľnosť, prístupnosť, komfort obsluhy ale aj údržba sa výrazne zlepší. Väčšinou sa tieto očakávania darí aj splniť, najmä čerstvo po pripojení. Každá zmena môže mať ale dve stránky.

Obr. 1 a, b: Pomerne výkonný hardvér majú aj špecializované skenery odtlačkov prstov
Zdroj: vlastné spracovanie

Kladnú, ktorú predvídame a očakávame, a zápornú, ktorú sme nečakali ale ak nastane, budeme musieť riešiť alebo znášať následky v kratšom, poprípade dlhšom horizonte. V uplynulom období zmenil sa hardvér, technológie ale aj podmienky ich využívania.

Aj to najmenšie elektronické zariadenie má väčší výkon procesora a väčšiu pamäť (aj hračky), ako prvé počítače.

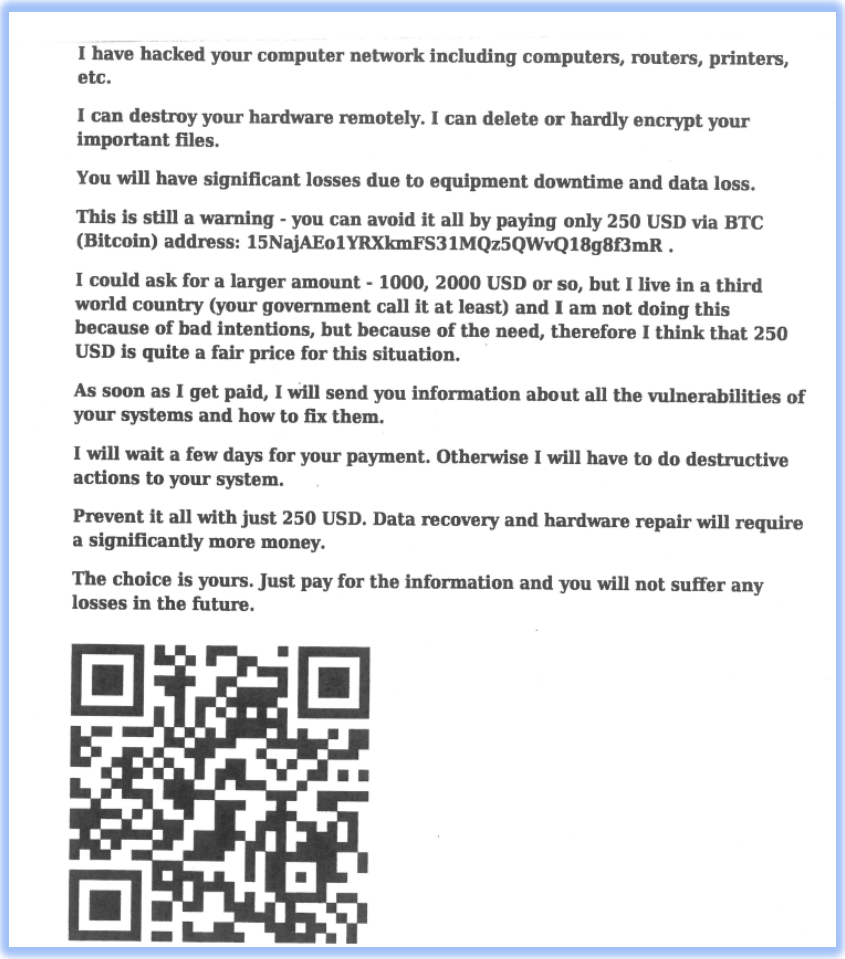
Veľa ľudí pozná túto skutočnosť a na ich prelomenie sú aj potrebné informácie ľahko dostupné – internet.

Vždy sa nájdu ľudia, ktorí to skúsia urobiť (zo zlomyseľnosti, za zisk, za „slávu“, atď.).

Netreba nič podceniť a hlavne nenechať na náhodu. Treba mať plán „B“ pre prípad ohrozenia – núdze. Najväčší záujem sa javí v poslednej dobe o zariadenia, ktoré sú všade prítomné, prechádzajú cez nich aj citlivé, chránené údaje, alebo aj dokumenty s vyšším stupňom utajenia. Sú dostatočne výkonné a menej chránené.

V kurze sú hlavne tlačiarne

Do siete pripojené tlačiarne môžu ušetriť veľké náklady pri vyššej kvalite a komforte tlače. Často sú kombinované aj inými zariadeniami ako je skener, telefón (fax). Ak ich nepripojíme dostatočne chránením spôsobom, namiesto vytlačenia nami žiadaného dokumentu čoskoro môžeme získať nečakaný výstup, ktorý sa bude neustále opakovať pri každej tlači.


I have hacked your computer network including computers, routers, printers, etc.

I can destroy your hardware remotely. I can delete or hardly encrypt your important files.

You will have significant losses due to equipment downtime and data loss.

This is still a warning - you can avoid it all by paying only 250 USD via BTC (Bitcoin) address: 15NajAEo1YRXkmFS31MQz5QWvQ18g8f3mR .

I could ask for a larger amount - 1000, 2000 USD or so, but I live in a third world country (your government call it at least) and I am not doing this because of bad intentions, but because of the need, therefore I think that 250 USD is quite a fair price for this situation.

As soon as I get paid, I will send you information about all the vulnerabilities of your systems and how to fix them.

I will wait a few days for your payment. Otherwise I will have to do destructive actions to your system.

Prevent it all with just 250 USD. Data recovery and hardware repair will require a significantly more money.

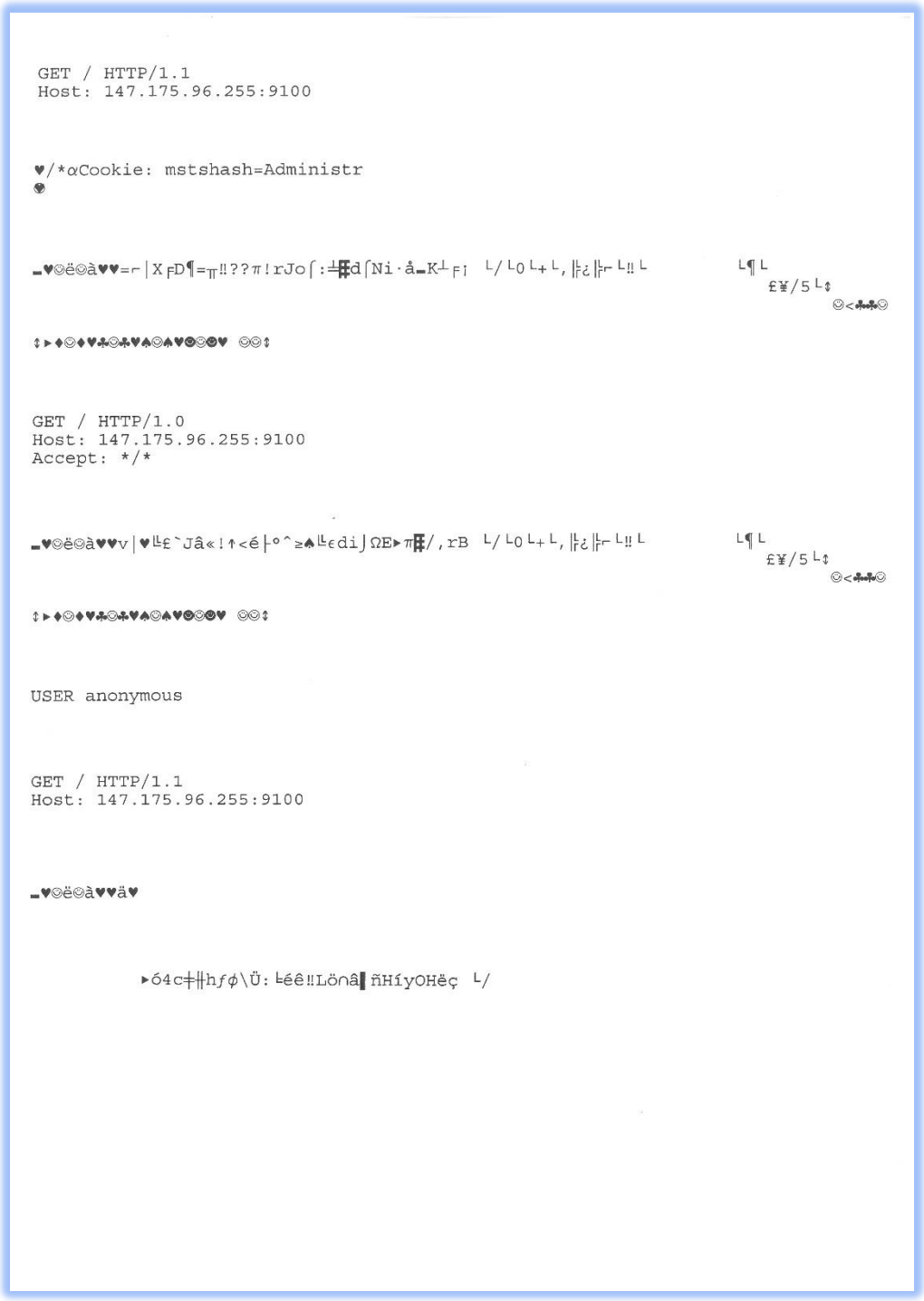
The choice is yours. Just pay for the information and you will not suffer any losses in the future.

Obr. 2: Výstup napadnutej sieťovej tlačiarne po každom spustení tlače
Zdroj: vlastné spracovanie

Toto je už väčšinou výsledok napadnutia, pričom dosiahnutie tohto stavu predchádza jeden alebo viac útokov, ktorým ale používatelia z neznalosti nevenujú dostatočnú pozornosť.

Ako sa to začína?

Strany vytlačené v čase, kedy obsluha alebo používatelia nie sú v práci sú veľmi podozrivé a treba tieto prípady dôkladne vyšetriť. Môžu to byť len prázdne papiere, ale aj písmenká alebo fragmenty zrozumiteľných slov (aj príkazov) v prítomnosti bežne netlačených symbolov.



Obr. 3: Ukážka vytlačených dokumentov počas útočenia na tlačiareň (každá časť bola vytlačená pôvodne na samostatnej strane)
Zdroj: vlastné spracovanie

- Väčšinou sa to začína vytlačením strán s nezmyselnými sériami znakov (pár riadkov), niekedy len jeden znak na strane.
- Pre tlač nezmyselná séria vytlačiteľných alebo neviditeľných znakov pre tlačiareň môže byť vykonateľná postupnosť kódov – to sa zneužíva na útok.
- Postupne sa potom môže zmeniť činnosť OS tlačiarne, v krajnom prípade sa môže zameniť priamo firmvér.

Takéto útoky na strane prevádzkovateľa vyvolajú rad otázok, na ktoré treba nájsť odpovede, lebo zásadným spôsobom môžu ovplyvniť spôsob obnovy činnosti a vybudovanie správnej ochrany zariadenia.

Kto je za útokmi?

Stroje bez účasti človeka by cielene neútočili. Sú len vykonávajúcou časťou človekom plánovaného a spusteného útoku.

- **Človek je najslabším článkom a zároveň hybnou silou útokov.**
- Preto treba dôkladne preskúmať každú zanechanú stopu útoku – aj zdanlivo nezmyselnú.

Prečo útočiť na tlačiareň?

Keďže za útokmi je človek, jeho ciele môžu byť hlavne:

- Znemožniť prácu na pracovisku.
- Získať kontrolu nad nimi a útočiť z nich z vnútra LAN.
- Zapojiť ich do siete a tak útočiť na iné siete.
- Získať obsah dokumentov vytlačených – skenovaných od doby napadnutia ale aj z minulosti.

Čo môže získať útočiaci?

- Kontrolu nad činnosťou pracoviska.
- Môže odpočúvať sieť a zaútočiť neskoršie cielene z vnútra – ťažšie sa dá zabrániť útoku z vnútra LAN.
- Získať obsah dokumentov vytlačených – skenovaných od doby napadnutia, aj z minulosti.

Pripomíname k tomu málo známe vlastnosti digitálnych tlačiarní:

- Najmä väčšie stroje majú dokumenty dlhšie v pamäti (do vymazania) – môžu byť cieľom útokov.
- Sieťové tlačiarne majú plnohodnotný operačný systém, len prístup k operačnému systému je obmedzený – po prelomení ochrany vzniká dobré útočisko.

Výslednú bilanciu útokov môžu znásobiť aj kroky správcov a obsluhy zariadení pred, počas a po útokov.

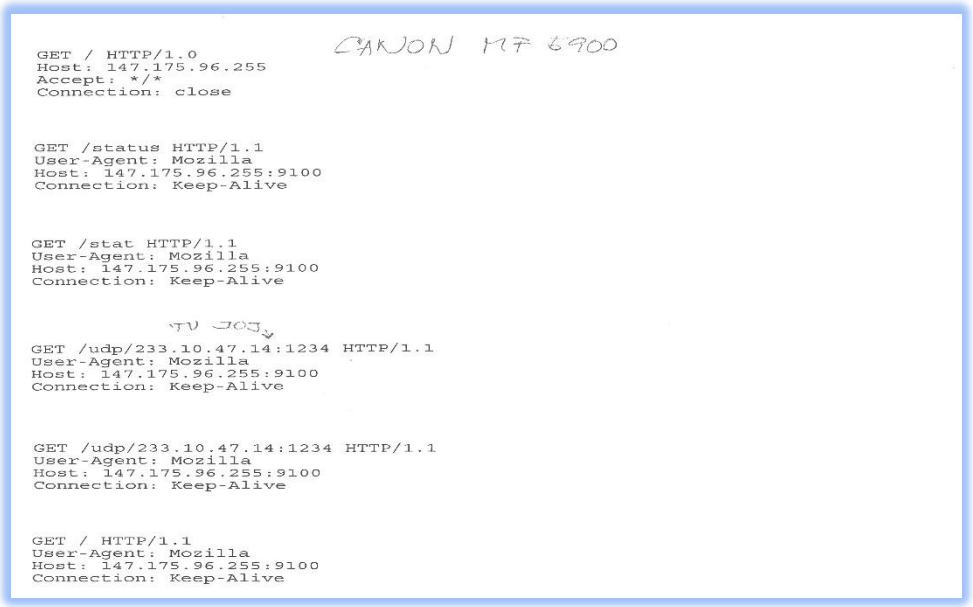
- Nevymazané dokumenty (kódy) z dočasných pamätí.
- Nesprávne alebo vôbec nechránené siete v mieste pripojenia.
- Neaktuálny alebo chybný továrenský softvér (firmvér) – dobré útočisko.
- Prežívajúce, staršie ale funkčne bezchybné tlačiarne (nemeníme ich tak často).
- Slabé poznatky personálu o možnom zneužití týchto strojov – podcenenie ich významu správcami.

To, že na Slovensku nie sme práve najlepšie pripravení na nekalú činnosť útočníkov zistili aj zverejnené Eurostat previerky (2017). **Podľa ich hodnotenia Slovensko sa nachádza až na posledných priečkach zo štátov Európskej únie v pripravenosti na kybernetické útoky.**

Útočiaci nemusia využívať len tie najnovšie zraniteľnosti. Nedávno zverejnený prípad svedčí o tom, že nedokonalé programátorské kódy môžu predstaviť veľký problém. Najmä v skriptovacích jazykoch používaných dodnes, ktoré na tlačiarňach nepripojených na sieť vôbec nerobili problém, ale v súčasnosti predstavujú veľkú zraniteľnosť. Známy je šokujúci prípad 32 ročnej (!!!) chyby skriptovacieho jazyka na napadnutie tlačiarne – len pri sieťovej prevádzke sa to odhalilo[1].

Môžu používať aj nástroje zverejnené na internete. Príkladom toho je nástroj, ktorý bol zverejnený na programátormi frekventovane navštívenom mieste internetu github.com[2].

Z pohľadu sieťovej prevádzky je najčastejšie napadnutý port 9100/tcp, ale aj ostatné, predovšetkým tlačiarňami využívané porty môžu byť pre tento účel zneužívané.



Obr. 4: Vytlačené „stopy“ po útokoch na tlačiareň (každý záznam bol vytlačený pôvodne na samostatnú stranu)
Zdroj: vlastné spracovanie

Čo používali nami nedávno odhalené prípady?

Na našom pracovisku počas pomerne krátkeho obdobia sme museli riešiť dva prípady napadnutia tlačiarní. Každý z nich mal inú techniku a cieľ útoku.

V prvom prípade bola napadnutá tlačiareň EPSON AL-M300. Stručne môžeme charakterizovať tento útok takto:

- Útok znefunkčnil tlačiareň, ktorá tlačila stále iba útočníkom posielaný vydieračský text (obr. 2).
- Útok bol ukončený po zablokovaní prístupu na verejnú IP tlačiarne mimo vlastnej LAN. Jednoduchý RESET, alebo vypnutie tlačiarne nepomohol.
- Nepomohol ani HW RESET (kombinácia tlačidiel + power), ktorý nemusí mať každá tlačiareň. Jeho použitie je veľmi účinné riešenie, lebo nastaví pôvodné továrenské stavy.
- Výsledkom útoku bol upravený firmware – ovládanie tlačiarne útočníkom cez sieť

[1] MILLMAN, R. 2017. *Postscript printers open to password theft through 32-year-old flaw*. [online]. [cit. 2019-06-04]. Dostupné na:<https://www.scmagazineuk.com/postscript-printers-open-password-theft-32-year-old-flaw/article/1475363>

[2] GITHUB. 2018. *Printer Exploitation Toolkit - The tool that made dumpster diving obsolete*. [online]. [cit. 2019-06-04]. Dostupné na:<https://github.com/RUB-NDS/PRET>

V druhom prípade veľmi zaujímavým spôsobom (večer) vedené útoky smerovali na CANON MF5900. Štýl a cieľ útoku tu bol iný.

- Na útok sa nepoužívala priamo verejná IP adresa tlačiarne (obr. 3,4), ale špeciálna IP adresa z daného rozsahu – broadcast (x.x.x.255 a port 9100/tcp).
- Cieľom útoku tu nebolo znemožniť prácu s tlačiarňou, ale vytvoriť podmienky pre útok na inú verejnú IP mimo LAN.
- Vypnutie, RESET stroja nepomohol. Dočasne sme obmedzili dobu zapnutia na dobu využitia – tlačiareň takto pracovala. Činnosť bola obnovená naplno po neskoršom blokovaní prístupu z vonka.

Samozrejme sme v obidvoch prípadoch postupovali čo najdôslednejšie. Po napadnutí tlačiarní často ostávajú aj stopy vytlačené v papierovej forme. Tie sa nám podarilo pozbierať v plnom rozsahu a nezmenenom poradí hárkov, ktoré sme dôkladne prezreli. Na základe výsledkov sme určili ďalšie kroky k ukončeniu útokov a obnove funkčnosti tlačiarní. V obi dvoch prípadoch sme museli riešiť problém aj na úrovni sieťovej, ktoré prinieslo aj nečakané odhalenie.

Čo sme odhalili nečakane?

Okrem toho, že bolo treba tlačiarne najprv dostať do stavu, ktorý je nastavený výrobcom, sme sa rozhodli upraviť aj nastavenia v sieťovom pripojení tlačiarní. Po naštudovaní možností sa nastavili nové pravidlá. Potom už len bolo treba overiť ich účinnosť v praxi. Na naše prekvapenie výsledky vykazovali nevysvetliteľné anomálie.

- Po nastavení nových pravidiel blokovania útoky prestali, ale potom znova sa objavili. Ako?
- Preskúmaním logov a debugovaním podporu zabezpečujúca firma zistila, že profesionálny firewall typu FirePower (CISCO) nevykoná správne nastavené pravidlá – našlo sa bug (pravdepodobne náhodná programátorská chyba).
- Podľa kuloárnych informácií chyba sa mala odstrániť najnovšou obnovou továrenského softvéru (deň pred zverejnením nájdenej chyby).
- Pre nedostatok času na testovanie, odstránenie chyby v dobe písania článku nebolo možné ešte potvrdiť.

Ako zabrániť takýmto útokom?

Tak, ako sme to demonštrovali na našich dvoch odhalených útokoch, zneužiť tlačiareň sa dá veľmi rôznymi spôsobmi a technikami útokov. Neexistuje teda jednotný postup na ich zabránenie alebo elimináciu následkov. Napriek tomu možno konštatovať, že sa oplatí venovať pozornosť dodržiavaniu niekoľkých ustálených zásad, ktoré výrazne môžu znížiť riziko napadnutia tlačiarní.

- Pokiaľ možno pripojte sieťové tlačiarne na sieť iba v rámci LAN, najlepšie v samostatnom VLAN (VPN).
- Blokujte prístup z vonka na tlačiareň a nenechajte voľný (raw) port 9100.
- Dôkladne overte činnosť po nastavení nových pravidiel (firewall, prepínače, iné zariadenia – softvér).
- Ak sa dá, obnovujte firmware pravidelne aj u tlačiarní.
- Nezabudnite zmeniť štandardne používané (továrenské) nastavenia.
- Obnovujte pravidelne ovládače zariadení.
- Pravidelne oboznamujte používateľov o možnostiach útokov; činnosti pred, počas a po ich zistení – mať plán „B“.

- Pokiaľ je to možné vylúčte, alebo minimalizujte použitie starších skriptovacích jazykov PostScript – PCL, PJL Cez nich sa realizujú útoky DDoS. Používajte radšej formát PDF (ak sa dá).
- Pri verejných IP adresách, vrátane „služobnej“ adresy broadcast, zabráňte prístup k adresám a portom, ktoré nemajú byť z vonka dostupné (:515,:531,:9100 a manažment (MFP) tlačiarní :80, :443).
- Dôkladnejšie a pravidelne preverte známe zraniteľnosti tlačiarní (najmä starších) a podľa toho zmeňte nastavenie prostredia tak, aby zabránil útok.

Podľa zverejnených informácií[3] vážnu zraniteľnosť majú tieto staršie tlačiarne:

- HP LaserJet 1200, 4200N, 4250N ...
- Dell 3130cn ...
- Samsung Multipress 6345N ...

Majú chybný softvér – démon (LPD) nedokáže správne spracovať viac ako 150 znakové mená používateľov.

Samozrejme nielen tlačiarne znamenajú potenciálne nebezpečenstvo na pracoviskách. Cenné informácie sa dajú získať aj z medicínskych alebo fitnes zariadení a všade prítomných zabudovaných kamier chytrých zariadení. Kameru D-Link DCS-2132L ponúkal na Slovensku aj Telekom v rámci svojho riešenia Magenta SmartHome[4]. Táto kamera má vážne zraniteľnosti. Zistilo sa, že pomerne ľahko možno zameniť firmvér a tak získať kontrolu nad kamerou. Navyše snímané video putuje cez sieť v nekódovanej forme. Výrobca po upozornení na tieto zraniteľnosti opravil iba prvú, druhá ostala neošetrená.

Lacnejšie fitnes hodinky nosí už pomerne veľa ľudí, samozrejme aj do práce. Opisy postupov prelomenia v lacnejšej kategórii lepšie vybavených a populárnych fitnes hodiniek Xiaomi MiBand3[5] a MiBand2[6] boli zverejnené na internete. Pri nekontrolovanom nosení aj cez ne možno získať veľmi cenné alebo chránené informácie podobne, ako z mobilných telefónov. Tie sú ale voči takýmto útokom omnoho lepšie chránené.

Záver

Životnosť tlačiarní, ako aj iných zariadení (IoT), už nebude ohraničená len ich mechanickými alebo elektrickými vlastnosťami (upotrebovania) ale skôr odolnosťou softvérového vybavenia voči útokom. Bude to veľká závislosť od výrobcov a ich serióznosti. Veľký výrobcovia výkonnejších strojov (EPSON, HP, Xerox, atď.) už sa snažia držať krok aj v tomto smere, zatiaľ striedavým úspechom. Lacné výrobky zrejme budú pomalšie reagovať na takýto vývoj. Nespoliehajte sa nato, že všetky vaše problémy vyriešia výrobcovia. Preventívne obmedzte použitie starších skriptovacích jazykov tlačiarní. U starších, mechanicky a funkčne ešte výborne pracujúcich zariadení na odstránenie problémov už bude treba vypracovať inú taktiku, ako obnova firmvéru. Budete ich môcť využiť iba ak budú pripojené do dobre chránenej siete LAN (VPN). Je možné aj to, že si pre bezpečnú prevádzku budete musieť zakázať využitie niektorých sieťových funkcií (manažovanie zariadenia na diaľku), ktoré vykazujú zraniteľnosť.

---

[3] MILLMAN, R. 2017. *Postscript printers open to password theft through 32-year-old flaw*. [online]. [cit. 2019-06-04]. Dostupné na:<https://www.scmagazineuk.com/postscript-printers-open-password-theft-32-year-old-flaw/article/1475363>

[4] KOSNO, L. 2019. *V domácej kamere D-Link objavili zraniteľnosti, môžu vás sledovať na diaľku.* [online]. [cit. 2019-06-04]. Dostupné na:<https://zive.aktuality.sk/clanok/139854/v-domacej-kamere-d-link-objavili-zranitelnosti-mozu-vas-sledovat-na-dialku/>

[5] REDDIT. 2019. *Hacks for the Mi Band 3 (on Android)*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.reddit.com/r/miband/comments/afl83u/hacks_for_the_mi_band_3_on_android/>

[6] NIKISHAEV, A. 2019. *How i hacked Xiaomi MiBand 2 to control it from Linux.* [online]. [cit. 2019-06-04]. Dostupné na:<https://www.bitcoininsider.org/article/21633/how-i-hacked-xiaomi-miband-2-control-it-linux>

Nezabudnite na pravidelné preškolenia personálu o možných zraniteľnostiach využívaných zariadení. Vypracujte podrobné pravidlá evidovania, zapájania a využívania takýchto zariadení aj s plánom „B“. Ak máte miestnosti s prísnym režimom utajenia, potom pravdepodobne budete musieť určiť aj pravidlá používania elektronických zariadení, ktoré vlastní, nosí (používa) personál na pracovisko.

Domnievame sa, že aj platná legislatíva Európskej únie a členských štátov by mohla tieto trendy už zachytiť. Pomocou nich by sa dali výrobné a obchodné procesy zmeniť tak, aby výrobcovia, resp. dodávatelia deklarovali ihneď po začatí predaja produktov údaj, ktorý by určil na ako dlhé obdobie bude výrobca podporovať firmvér, ovládače, atď. daného výrobku. Potom by zákazník mohol relevantne rozhodnúť o kúpe produktu bez toho, aby musel jeho prevádzku zastaviť predčasne, pre nedostatok nového, dobre chráneného firmvéru.

V našom príspevku sme chceli upriamiť pozornosť na niektoré aktuálne trendy kyberútokov na menej chránené časti sietí, ako sú sieťové tlačiarne, kamery, skenery, zdravotnícke, fitnes, welness a IoT zariadenia. Tie sú vyvolané a podporované novými možnosťami ich hardvérového a softvérového vybavenia. Problematika je ale omnoho zložitejšia, ako sa to zdá na prvý pohľad, preto úplný prehľad o tejto problematike v danom rozsahu nie je možné podať. Z tohto dôvodu sme to robili pomocou skúseností, ktoré sme získali z dvoch nedávno riešených útokov na tlačiarne, umiestnených na našom pracovisku a na základe niektorých zaujímavejších informácií z tejto oblasti. Na stránkach internetu sa dá vyhľadať a nájsť pomerne veľa zdrojov na túto tematiku. Prípadné konkrétne udalosti možno aj pomocou nich riešiť, ale je omnoho lepšie sa z nich poučiť a preventívnymi opatreniami, resp. odolnými riešeniami minimalizovať alebo úplne zabrániť kyberútokom.

Zoznam použitej literatúry:

1. GITHUB. 2018. *Printer Exploitation Toolkit - The tool that made dumpster diving obsolete.* [online]. [cit. 2019-06-04]. Dostupné na: <https://github.com/RUB-NDS/PRET>
2. KOSNO, L. 2019. *V domácej kamere D-Link objavili zraniteľnosti, môžu vás sledovať na diaľku.* [online]. [cit. 2019-06-04]. Dostupné na: <https://zive.aktuality.sk/clanok/139854/v-domacej-kamere-d-link-objavili-zranitelnosti-mozu-vas-sledovat-na-dialku/>
3. MILMANN, R. 2017. *Postscript printers open to password theft through 32-year-old flaw*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.scmagazineuk.com/postscript-printers-open-password-theft-32-year-old-flaw/article/1475363>
4. NIKISHAEV, A. 2019. *How i hacked Xiaomi MiBand 2 to control it from Linux.* [online]. [cit. 2019-06-04]. Dostupné na: <https://www.bitcoininsider.org/article/21633/how-i-hacked-xiaomi-miband-2-control-it-linux>
5. REDDIT. 2019. *Hacks for the Mi Band 3 (on Android).* [online]. [cit. 2019-06-04]. Dostupné na: <https://www.reddit.com/r/miband/comments/afl83u/hacks_for_the_mi_band_3_on_android/>

Kontaktné údaje:

Ing. Alexander Hambalík, PhD.
Ústav informatiky a matematiky
FEI STU v Bratislave
alexander.hambalik@stuba.sk

Vzdělávání v oblasti kybernetické bezpečnosti

Petr Hrůza

Abstrakt:
Autor příspěvku se zaměří na vzdělávání v oblasti kybernetické bezpečnosti na Univerzitě obrany v Brně. Popíše starší, stávající ale hlavně nové studijní programy v oblasti kybernetické bezpečnosti. Zaměří se také na osvětu kybernetické bezpečnosti u studentů, kteří nestudují specializaci blízkou informačním technologiím. Na závěr se zmíní o jednom projektu, který řeší studenti, kteří nestudují kybernetickou bezpečnost.
Klíčová slova:
Kybernetická bezpečnost, informační technologie, komunikační technologie, vzdělávání, univerzita.

Abstract:
The author of this paper will focus on cyber security education in the University of Defence in Brno. He describes the older, existing and especially new study programs in the field of cyber security. It will also focus on raising awareness of cyber security among students who are not specialized in information technology. Finally, he mentions one project that solves students who do not study cyber security.
Key words:
Cyber Security, Information Technology, Communication Technology, Education, University.

Úvod

V úvodu několik málo informací o Univerzitě obrany v Brně. **Univerzita obrany v Brně**[1] (dále UO) poskytuje akreditované vzdělání v bakalářských, magisterských a doktorských studijních programech, které jsou vojensko-manažerského, ekonomického, technického a zdravotnického zaměření. Vzdělávání na UO se dále uskutečňuje v programech celoživotního vzdělávání v rámci kariérových a jiných odborných kurzů postgraduálního charakteru. Univerzita obrany v Brně má své nezastupitelné místo v systému českých vysokých škol a poskytuje vzdělání srovnatelné se vzděláním získaným na civilních vysokých školách v České republice. Jedná se o jedinou vojenskou státní vysokou školu v České republice.

Univerzita obrany v Brně připravuje vojenské profesionály a další odborníky působící ve sféře bezpečnosti a obrany státu na základě potřeb Armády ČR a státní správy. Všestrannost vzdělání rovněž vytváří předpoklady pro uplatnění absolventů univerzity i v civilním životě. Vzdělávání na UO absolventům poskytuje ucelený rozsah znalostí, umožňujících zvládnutí činností v oblasti řízení a velení. Vojenské a velitelské dovednosti studenti získávají především při vojenském praktickém výcviku, který je fakultami realizován během studia. Absolventi UO jsou připraveni i pro působení v jednotkách zahraničních misí a v rámci aktivit NATO.

Příprava studentů v oblasti kybernetické bezpečnosti

Přípravu studentů v oblasti kybernetické bezpečnosti lze rozdělit do tří částí. V první části se zaměřím vzdělávání prvních studentů v kybernetické bezpečnosti od roku 2011. Ve druhé části popíši aktuální programy se zaměřením na informační a komunikační systémy. V poslední, třetí části, popíši obsah a zaměření nového studijního programu, který je možné od podzimu 2019 na univerzitě začít studovat. Dále se zmíním o zavádění výuky kybernetické bezpečnosti do všech ostatních studijních programů v malém či větším rozsahu.

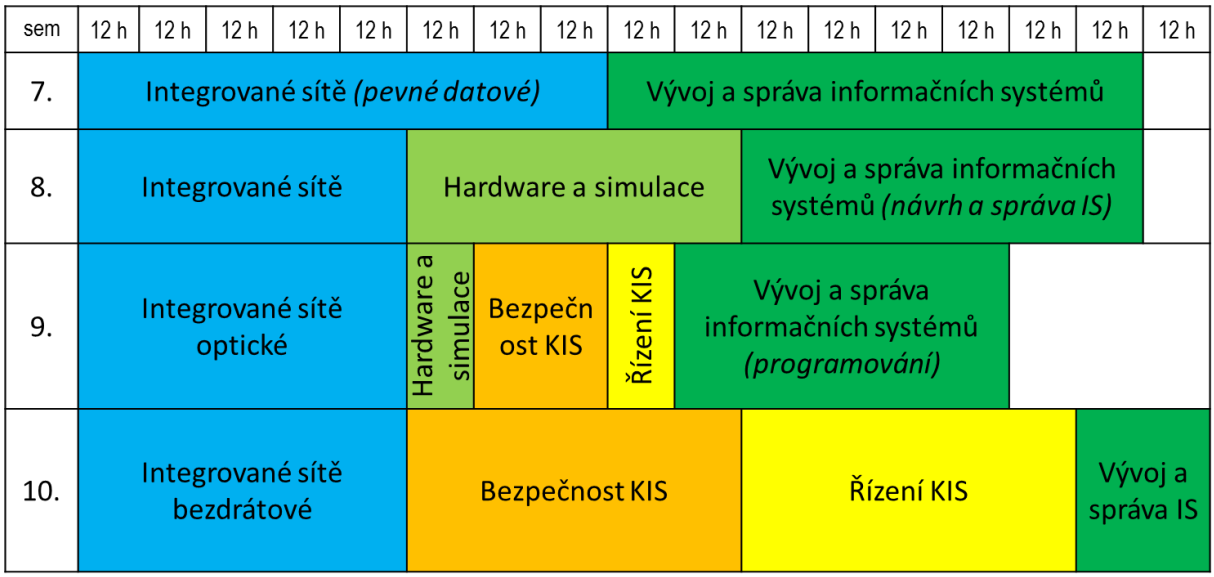
Univerzita obrany měla jako první univerzita v ČR akreditovaný **studijní modul** „**Kybernetická bezpečnost**“. První studenti začali modul studovat **od podzimu 2011**. Modul „Kybernetická bezpečnost“ byl součástí **studijního oboru „Bezpečnostní management“.** Studijní obor „Bezpečnostní management“ byl a stále je součástí studijního programu „Ekonomika a management“. Studijní obor „Bezpečnostní management“ je určen pro absolventy, kteří budou vykonávat své funkce na manažerských nebo dalších odborných

[1] Univerzita obrany v Brně. [online]. [cit. 2019-06-02]. Dostupné na: <https://www.unob.cz/Stranky/default.aspx>

pozicích řízení bezpečnostních procesů v privátním i veřejném sektoru s orientací na bezpečnost majetku, osob a systémů. Studijní modul „Kybernetická bezpečnost“ byl zaměřen na přípravu odborníků pro výkon analytických a manažerských funkcí v organizačních strukturách subjektů obrany a bezpečnosti České republiky v oblasti řízení procesů souvisejících se zajišťováním bezpečnosti informačních systémů. Student si v rámci modulu osvojil odborné znalosti z problematiky kyberprostoru, hrozeb a rizik v kyberprostoru. Znal ochranu a obranu proti útokům na informační systémy, informační války, kybernetickou kriminalitu, bezpečnostní technologie komunikačních a informačních systémů. Dokázal používat nástroje kybernetického managementu a uplatňovat základy práva v oblasti kybernetické kriminality. Studium bylo určeno jak pro vojenské, tak i civilní uchazeče. Univerzita toto studium otevřela pouze pro civilní studenty a jednalo se pouze o bakalářské studium. **Poslední studenti tohoto modulu promovali v roce 2017**. Celé studium bylo zaměřeno hlavně na management kybernetické bezpečnosti. Každým rokem do modulu nastoupilo okolo 12-15 studentů. Protože modul byl součástí studijního programu „Ekonomika a management“, po prvním semestru odešlo ze studia více jak polovina studentů. Buď studium nezvládali, nebo spíše očekávali více výuku orientovanou na výpočetní techniku a ne na ekonomii. Odborné předměty studenti začali studovat až ve třetím semestru (tzn. ve druhém ročníku studia). Do druhého ročníku vždy postoupili pouze čtyři studenti. V prvním běhu to byli tři kluci a jedna dívka, v posledním běhu pouze čtyři dívky. Musím konstatovat, že všichni studenti (i když se jednalo o civilní studium) našli po skončení studia buď zaměstnání, nebo dále pokračovali v magisterském studiu v příbuzném oboru. Jednalo se ale o ojedinělý modul v systému vzdělávání v České republice. Všechny obdobné studijní moduly na jiných vysokých školách v České republice byly více zaměřeny na technickou stránku řešení kybernetické bezpečnosti. Tento modul jako jediný byl zaměřen na chybějící mezičlánek ve státním i soukromém sektoru a tím byly osoby – manažeři, kteří rozumí technické stránce bezpečnosti a dokáží uplatnit přitom své získané manažerské dovednosti.

V současnosti je možné na Univerzitě obrany v Brně studovat v bakalářském **civilním** studiu prezenčně integrovaný obor „**Komunikační a informační technologie**“. V magisterském studiu navazujícím na civilní bakalářské studium formou prezenčního studia a kombinovaného studia je možné pak studovat dva různé moduly – „**Komunikační technologie**“ nebo „**Informační technologie**“. Jiné je to u vojenského studia. To je od akademického roku **2014/2015** možné studovat pouze jako **magisterské studium[2] (tedy ucelené pětileté), pro vojáky již neexistuje tříleté bakalářské studium**. Je možné studovat 2 studijní programy a v nich několik specializací. Součástí studijního programu „**Vojenské technologie elektrotechnické**“ jsou specializace „**Informační technologie**“, „**Komunikační technologie**“ a „**Radiolokace a elektronický boj**“. Studium je zaměřeno na technické a programové vybavení počítačů, počítačových sítí a bezpečnosti komunikačních a informačních systémů. Druhým studijním programem jsou „**Vojenské technologie strojní**“, které nemají žádnou specializaci zaměřenou do oblasti kybernetické bezpečnosti či informačních a komunikačních systémů. Odborné předměty jsou vyučované až od čtvrtého ročníku studia (od 7. semestru), jak je uvedeno na následujícím obrázku.

[2] Přijímací řízení: Vojenské magisterské studium - Nabízené studijní programy a specializace. [online]. [cit. 2019-06-02]. Dostupné na: <z: https://www.unob.cz/fvt/studium/Stranky/PR_voj_mgr-nabizene-obory.aspx>



Obr. 1: Odborné předměty od 7. semestru studia
Zdroj: prezentace Katedry informatiky, kybernetické bezpečnosti a robotiky

Od podzimu roku 2019 (od akademického roku 2019/2020) je možné na Univerzitě obrany v Brně nově začít studovat studijní program „**Kybernetická bezpečnost**“. Oblast vzdělávání je „2. Bezpečnostní obory“ a výuka probíhá v rozsahu 30 hodin za týden, 12 týdnů za semestr. V tomto studijním programu budou studenti skládat státní závěrečné zkoušky z následujících tří předmětů „Kybernetická bezpečnost, „Informatika“ a „Bezpečnost počítačových sítí“.

Obsahem předmětu „**Kybernetická bezpečnost**“ je:

- Legislativa v kybernetické bezpečnosti.
- Kybernetická kriminalita.
- Bezpečnostní architektury OS.
- Forenzní analýza.
- Penetrační testování.
- Malware.
- Otevřené zdroje v kybernetické bezpečnosti.
- Kryptografické protokoly.
- Sociální inženýrství a bezpečnost.
- Orgány a řízení kybernetické bezpečnosti ve státní správě.

Obsahem předmětu „**Informatika**“ je:

- Vývoj aplikací.
- Architektura výpočetních systémů.
- Databázové a informační systémy.
- Webové aplikace a jejich vývoj.
- Operační systémy.
- Virtualizace výpočetních systémů.
- NoSQL, BigData.
- Web scraping OSINT.
- EDA, Data Mining.

Obsahem předmětu „**Bezpečnost počítačových sítí**“ je:

- Vrstvené modely síťové architektury ISO/OSI, TCP/IP.
- Protokoly jednotlivých vrstev.
- Ethernet.
- Směrování, směrovací protokoly.
- Bezpečnost na jednotlivých vrstvách.
- Rozsáhlé sítě.
- Monitorování a správa sítí.
- Komunikační vedení a přenosové technologie.
- IP telefonie a VoIP.

I u studentů na Univerzitě obrany v Brně u ostatních specializací, které nejsou zaměřeny na kybernetickou bezpečnost či na informační a komunikační systémy, se zavádí výuka kybernetické bezpečnosti v omezeném rozsahu. Jedná se o výuku u obou fakult dislokovaných v Brně. U studentů civilního studia na **Fakultě vojenského leadershipu** je zaveden předmět „**Kybernetická bezpečnost II**“. Předmětu je vyučován ve třetím ročníku studia v pátém semestru. Obsahem je seznámit studenty se základy kybernetické bezpečnosti. U studentů vojenského studia na **Fakultě vojenského leadershipu** je do výuky zařazeno několik hodin základů kybernetické bezpečnosti v rozsahu od dvou do šesti hodin, většinou v posledním roce studia na univerzitě. U některých modulů, jak je například modul management informačních zdrojů, je rozsah výuky kybernetické bezpečnosti navýšen na 16 hodin výuky. Takový počet již je postačující, aby studenti pochopili obsah kybernetické bezpečnosti a začali ji brát vážně. Obsahem výuky je rozbor několika kybernetických útoků, možné metody kybernetické bezpečnosti a také obrany a hlavně zásady bezpečného chování v kybernetickém prostoru.

Závěr

Výuka kybernetické bezpečnosti je v dnešní době neodmyslitelně spjatá se všemi studijními programy a obory. S první výukou v modulu kybernetická bezpečnost začala na podzim 2011. V současné době je možné studovat na Univerzitě obrany v Brně obory obor „Komunikační a informační technologie“ v rámci civilního bakalářského studia a v magisterském studiu „Komunikační technologie“ nebo „Informační technologie“. Od akademického roku 2019/2020 lze nově studovat studijní program „Kybernetická bezpečnost“. Základy kybernetické bezpečnosti se zavádějí do všech specializací na celé univerzitě.

Seznam použité literatury:

1. Univerzita obrany v Brně. Brno. [online]. [cit. 2019-06-02]. Dostupné na: <https://www.unob.cz/Stranky/default.aspx>
2. *Přijímací řízení: Vojenské magisterské studium-Nabízené studijní programy a specializace.* [online]. [cit. 2019-06-02]. Dostupné na: <https://www.unob.cz/fvt/studium/Stranky/PR_voj_mgr-nabizene-obory.aspx>
3. *Kybernetická bezpečnost FVT*. [online]. [cit. 2019-06-02]. In Elektronická prezentace. Brno: Katedra informatiky, kybernetické bezpečnosti a robotiky, 2019. s. 7.

Kontaktní údaje:

doc. Ing. Petr Hrůza, PhD.
Fakulta vojenského leadershipu
Katedra taktiky
Univerzita obrany v Brně
petr.hruza@unob.cz

Kybernetický boj ako jeden z nekonvenčných spôsobov boja

Radoslav Ivančík

Abstrakt:
Ku koncu druhej dekády 21. storočia sa kyberpriestor stal definitívne po zemi, vzduchu, vode a vesmíre piatou dimenziou pre vedenie vojny. Dokonca je možné konštatovať, že ovládnutie kyberpriestoru má dnes z hľadiska vojenstva rovnaký význam ako ovládnutie vzdušného priestoru v 20. storočí. Počítače a ich klávesnice sa stali zbraňami, komunikačné a informačné technológie, systémy a prostriedky predstavujú zbraňové systémy, kybernetickí bojovníci využívajú v boji softvér i hardvér a verejné i súkromné siete sú bojiskom. Konvenčné spôsoby boja sú nahrádzané nekonvenčnými a klasické pojmy ako obrana, útok, miesto, identita (identifikácia), násilie alebo rýchlosť dostávajú úplne nový význam, resp. rozmer. To je aj dôvod prečo je kybernetický boj predmetom nášho skúmania a vedeckého záujmu.
Kľúčové slová:
Kybernetický boj, kybernetické útoky, kybernetická bezpečnosť.

Abstract:
By the end of the second decade of the 21st century, cyberspace had finally become, except of land, air, water and space, the fifth dimension for warfare. It can even be said that the control of the cyberspace now has the same meaning in military terms as the control of the airspace in the 20th century. Computers and their keyboards have become weapons, communication and information technologies, systems, means and devices are weapon systems, cyber warriors use software and hardware to fight, and public and private networks are battlefields. Conventional ways of fighting are being replaced by unconventional, and classical terms such as defence, attack, place, identity (identification), violence or speed are given a completely new meaning, resp. dimension. All the above-mentioned facts are reasons why cyber combat is the subject of our research and scientific interest.
Key words:
Cyber combat, cyberattacks, cyber security.

Úvod

V úzkej súvislosti s masívnym nasadzovaním a využívaním komunikačných a informačných technológií, systémov a prostriedkov a zároveň s nevyhnutnou potrebou čeliť novým symetrickým i asymetrickým bezpečnostným hrozbám, dochádza vo väčšine krajín sveta vo väčšej či menšej miere (podľa miery ohrozenia, objemu disponibilných zdrojov, prístupu k novým technológiám, atď.) k transformácii vojenstva, reorganizáciám organizačných štruktúr ozbrojených síl a k budovaniu nových moderných spôsobilostí a špeciálnych vojenských jednotiek. Súčasne, v nadväznosti na uvedené, sa v ostatných rokoch vedie, a to nielen v rámci odbornej komunity, intenzívna debata o tzv. nových spôsoboch, metódach či formách vedenia boja. Prevažná časť tejto diskusie vychádza z predpokladu, že v konkrétnom prípade využívania komunikačných a informačných technológií, systémov a prostriedkov ide o kvalitatívne novú, nekonvenčnú formu vedenia boja, ktorá má unikátne parametre, charakteristiku a vyžaduje si úplne nový prístup. Prístupy využívané pri tradičných, konvenčných spôsoboch boja totiž nie je možné pri nich uplatniť.

Aká je teda analógia medzi tradičnými spôsobmi vedenia boja a novými nekonvenčnými formami? V prvom rade je potrebné vychádzať z toho, že v ostatných rokoch síce došlo k posunu ťažiska v oblasti využívania bojovej techniky, zbraní a zbraňových systémov, stratégie a taktiky a väčšiu úlohu než v minulosti zohrávajú nové formy vedenia ozbrojeného zápasu, označované ako nekonvenčné, nejde však o nejaký veľmi zásadný, výrazný či dokonca prelomový kvalitatívny posun. Ide skôr o prirodzený vývoj, nadväzujúci na vývoj v oblasti vedy a techniky, vyvolaný hľadaním čo najefektívnejšieho a najúčinnejšieho spôsobu ako dosiahnuť víťazstvo, resp. ako poraziť protivníka, alebo aspoň spôsobiť mu čo najväčšie straty a škody a odradiť ho od ďalších bojových aktivít. Avšak spolu s tým, ako rastie význam, vplyv a frekvencia využívania nekonvenčných foriem boja, rastie aj tlak na revíziu a modifikáciu vojenských doktrín a následne, či v súvislosti s tým, aj pravidiel vedenia vojny.

Práve v úzkej súvislosti s masívnym nasadzovaním a využívaním komunikačných a informačných technológií, systémov a prostriedkov môže ako vhodný príklad na ilustráciu slúžiť kybernetický boj ako relatívne nový spôsob vedenia boja a terorizmus ako spôsob vedenia psychologickej vojny, ktorá má, na rozdiel od kyberterorizmu, veľmi dlhú tradíciu. Význam oboch týchto foriem vedenia boja v posledných rokoch výrazne stúpa, najmä preto, že predstavujú efektívny a účinný spôsob boja proti technologicky vyspelým protivníkom s masívnou vojenskou a logistickou prevahou, s ktorými nie je možné viesť konvenčnú vojnu.

Konvenčná vojna predstavuje typ ozbrojeného konfliktu, v ktorom bojujúce strany (protivníci) používajú konvenčné zbrane, t. j. všetky zbrane s výnimkou zbraní hromadného ničenia – nukleárnych, biologických, rádiologických a chemických, a bojujú otvorene na zemi, vo vzduchu, či na vode. Sily oboch strán (protivníkov) sú jasne definovateľné, organizované a zbrane používajú na boj proti ozbrojeným vojenským jednotkám protivníka. Základným cieľom konvenčnej vojny je zničiť alebo oslabiť ozbrojené sily protivníka, obsadiť jeho územie a celkovo narušiť jeho schopnosť viesť konvenčnú vojnu. Dôležité je doplniť, že za konvenčnú vojnu sa považujú také bojové operácie, ktoré sú vedené v súlade medzinárodným vojnovým právom (Haagskymi konvenciami, Ženevským dohovorom a celým radom ďalších dohôd a dokumentov). To znamená, že konvenčná vojna má určitý právny rámec a zúčastnené strany konfliktu rešpektujú určité pravidlá týkajúce sa vojny (napr.: označenie bojujúcich strán, používanie zbraní, ochrana civilistov, dodržiavanie práv vojnových zajatcov, atď.).

Konvenčná zbraň je taká zbraň, ktorá neobsahuje toxické, nukleárne, rádiologické, chemické alebo biologické zložky. Konvenčné zbrane pokrývajú široké spektrum pozemných, vzdušných a na/vo vode použiteľných zbraní zahŕňajúcich napr. rôzne druhy a typy ručných zbraní, pušiek, samopalov, guľometov, tankov, obrnených transportérov, húfnic, raketometov, bojových člnov, vojnových lodí, vrtuľníkov, lietadiel, ale aj nábojov, granátov, mín, bômb, rakiet a obrovské množstvo ďalších typov zbraní a munície do nich. Vo všeobecnosti ide teda o zbrane, ktorých schopnosť poškodenia pochádza z kinetickej, zápalnej, výbušnej alebo chemickej energie; v žiadnom prípade nejde o chemické zbrane alebo zbrane využívajúce jadrovú energiu. Používanie všetkých druhov konvenčných zbraní v čase vojny sa riadi Haagskymi konvenciami a Ženevským dohovorom. Používanie niektorých druhov konvenčných zbraní je však zakázané alebo regulované na základe Dohovoru OSN o zákazoch alebo obmedzeniach používania určitých druhov konvenčných zbraní, Dohovoru o kazetovej munícii alebo Zmluvy o zákaze mín, atď.

V tejto súvislosti je potrebné pre lepšie pochopenie skúmanej problematiky uviesť, že konvencie predstavujú prijaté a všeobecne (resp. v dostatočne významnom počte prípadov) uznávané normy upravujúce spôsob vedenia boja. Konvencie, ktoré platia po určité obdobie, nie sú a podľa Kazanského ani nemôžu byť nadčasové.[1] Navyše, konvencie, ktoré sú prijímané najsilnejšími (resp. víťaznými) aktérmi, čo v prípade konvencií upravujúcich pravidlá vedenia vojny bezpochyby platí, môžu sa presadzovať, uplatňovať, avšak ťažko budú akceptované a chápané ako legitímne slabšími (resp. vojnu, ozbrojený zápas prehrávajúcimi) aktérmi, ktorým nevyhovujú. Na druhej strane, v prípade zásadnej zmeny situácie, môžu byť niektoré konvencie odvrhnuté, resp. porušované aj aktérmi silnými, pretože im za danej zmenenej situácie znemožňujú využitie, posilnenie alebo znásobenie ich vojenského potenciálu.

V niektorých prípadoch sa preto môže objaviť na jednej strane politický (mocenský) dopyt a tlak na legalizáciu niektorých nekonvenčných foriem vedenia boja, ktoré posilnia vojenské spôsobilosti silných aktérov, a na druhej strane, formy vedenia boja, ktoré by silným aktérom neprinášali výhody a profit, môžu byť prostredníctvom politického (mocenského) tlaku naďalej udržiavané mimo uznávaných konvencií. Toto môže byť aj prípad kybernetického boja na jednej strane a terorizmu na strane druhej.

[1] KAZANSKÝ, R. *Súčasné problémy výskumu medzinárodných konfliktov a kríz a ich riešenia*. Banská Bystrica: Vydavateľstvo UMB – Belianum, 2013. s. 152.

Teoretické východiská

Vojenstvo a vedenie vojny bolo vždy určitým spôsobom obmedzované, takže začatie a vedenie boja ako organizovaného násilia bolo vždy zviazané s určitými normami. Kľúčové boli predovšetkým úpravy toho, za akých podmienok a kvôli čomu možno viesť vojnu, t. j. dôvod k vedeniu vojny, a – najmä – akým spôsobom má boj prebiehať.[2] Súčasné pravidlá pre rozlišovanie vojny, chápanej ako legálne vedenia boja, a zločinu, vrátane zločinov vojnových, teda nelegálnych foriem a metód vedenia boja, je do značnej miery výsledkom vývoja nasledujúceho po uzavretí Vestfálského mieru v októbri 1648. Ten, ako uvádzajú Lasicová a Ušiak, priniesol do medzinárodného práva viac odpovedí na otázky suverenity štátu, riešenia problémov medzinárodnej politiky a zásad sporov, ktoré odvtedy ovplyvňovali medzinárodné vzťahy na veľmi dlhý čas.[3] Zároveň potvrdil dva základné rozmery suverenity štátov – vonkajšiu (t. z. že všetky štáty sú si z právneho hľadiska rovné) a vnútornú (t. z., že každý štát je zvrchovaný v oblasti vnútornej suverenity, nie je nikým obmedzený, a je sám správcom svojho územia a obyvateľstva).[4]

Najvýznamnejšiu úlohu v oblasti kodifikácie pravidiel vedenia vojny (boja) zohralo s najväčšou pravdepodobnosťou prijatie Haagskych a Ženevských dohovorov a konvencií, ktoré upravovali pravidlá vedenia vojny, a vypracovanie a ustanovenie medzinárodného vojnového a humanitárneho práva. Snahy kodifikovať pravidlá vedenia boja sa však po celý čas stretávali s rozdielnymi záujmami významných aktérov (medzinárodného práva), rozdielnymi kultúrnymi prístupmi k vedeniu boja a v neposlednom rade s technologickým vývojom, ktorý zásadným spôsobom ovplyvňoval aj oblasť vojenstva. Po zmenách, ktoré so sebou do vojenstva priniesli zbrane hromadného ničenia, najmä nukleárne zbrane, sa vývoj koncom minulého storočia začal uberať iným smerom.

Technologické zmeny, predovšetkým veľmi rýchly rozvoj a stále širšie uplatnenie informačných a komunikačných technológií, systémov a prostriedkov, ktoré umožnili okrem iného tzv. Revolúciu vo vojenstve (Revolution in Military Affairs – RMA), výrazne posilnili schopnosť bohatých, rozvinutých a technologicky vyspelých štátov viesť vojnu. Ich protivníci, chudobnejšie, rozvojové a technologicky menej vyspelé štáty, povstalci, partizáni, neštátne zoskupenia a siete tak fakticky nemôžu v konvenčne vedenej vojne proti silným aktérom zvíťaziť. Tento fakt bol na jednej strane cieľom a dôvodom prebiehajúcej transformácie armád vyspelých štátov, na druhej strane tým ale RMA čiastočne anuluje samu seba, pretože motivuje protivníkov hľadať také nekonvenčné spôsoby, metódy a formy boja, ktoré kompenzujú konvenčné prevahu veľmocí.[5]

Chápanie pravidiel známych ako „jus ad bellum“ a „jus in bello“[6] je preto závislé od kontextu tradičného chápania vojny ako masívneho konvenčného ozbrojeného stretu medzi štátmi,[7] alebo v prípadoch občianskych vojen, v ktorých dochádza k masovým stretom organizovaných strán, kde prinajmenšom jednou zo strán je štát.[8] Je úplne jasné a evidentné, že masový stret organizovaných strán je krajne nepravdepodobný v tých prípadoch, kedy by pre

---

[2] ROBERTS, A. 2007. *Counter-terrorism, Armed Force and the Laws of War*. [online]. [cit. 2019-04-18]. Dostupné na: <http://essays.ssrc.org/10yearsafter911/counter-terrorism-armed-force-and-the-laws-of-war/>

[3] LASICOVÁ, J., UŠIAK, J. *Bezpečnosť ako kategória*. Bratislava : Veda – vydavateľstvo SAV, 2012, s. 14.

[4] BRHLÍKOVÁ, R. Suverenita štátu. In: *Právny obzor*, roč. 80, č. 3/1997. s. 363.

[5] DARTON, G. Information Warfare and the Laws of War. In: *Cyberwar, Netwar and the Revolution in Military Affairs*. New York : Palgrave Macmillan, 2016. s. 296.

[6] *Poznámka*: „Jus ad bellum“ odkazuje na podmienky, za ktorých sa štáty môžu uchýliť k vojne alebo k použitiu ozbrojených síl vo všeobecnosti. Zákaz používania sily medzi štátmi a výnimky z nej (sebaobrana a autorizácia OSN na použitie sily), ustanovená v Charte Organizácie Spojených národov z roku 1945, sú základnými zložkami „jus ad bellum“. „Jus in bello“ reguluje konanie strán zapojených do ozbrojeného konfliktu.

[7] EICHLER, J. *Mezinárodní bezpečnost na počátku 21. století*. Praha: AVIS, 2006. s. 182.

[8] MAREŠ, M. 2007. *Vymezení pojmů terorismus, válka a guerilla v soudobé bezpečnostní terminologii*. [online]. [cit. 2019-04-18]. Dostupné na: <https://www.obranaastrategie.cz/filemanager/files/6330.pdf>

väčšinu protivníkov technologicky vyspelých štátov bola takáto forma boja doslova samovražedná, vopred odsúdená na neúspech. A práve v takýchto prípadoch sa ponúka využitie nekonvenčných taktík, metód a spôsobov boja a zbraní.

Jednoznačne najdiskutovanejším nekonvenčným spôsobom boja je v posledných rokoch nepochybne terorizmus. V boji proti ozbrojeným silám a zložkám technologicky vyspelých štátov sa však už dlhé roky využívajú aj iné nekonvenčné formy boja, napr. partizánsky spôsob boja, guerillové kampane, sabotáže, atď., ktoré prekračujú obmedzenia dané konvenciami. Ďalšou z nekonvenčných možností, najmä v súčasnosti, je využitie úplne nových foriem boja, ako je napr. kybernetický boj.

Kybernetický boj ako jeden z nekonvenčných spôsobov boja

Podstatou kybernetického boja je premiestnenie bojových operácií zo zeme, vzduchu alebo vody do kybernetického priestoru. Kybernetický priestor je vo svojej rozhodujúcej časti prepojený, i keď existujú aj separátne časti, napr. počítače nepripojené k sieti, izolované LAN (Local Area Network) alebo WAN (Wide Area Network), príp. SIPRNET (The Secret Internet Protocol Router Network). Prepojené sú tak národné kybernetické priestory, ako aj privátne a verejné či vojenské a civilné priestory. Prechody (hranice) medzi nimi, sú často nezreteľné, nepozorovateľné. Akcie môžu prebiehať rýchlosťou limitovanou iba výkonom procesora a kapacitou infraštruktúry, teda oveľa rýchlejšie ako operácie prebiehajúce vo fyzickom svete. Miznutie hraníc (teritoriálnych, sociálnych, atď.) nesie so sebou aj popieranie dlhého niekoľko storočného vývoja, ktorý smeroval práve k narysovaniu ostrých kontúr medzi vojnou a mierom, vojenským a civilným, legálnym a zločinným, na ktorých je vystavané súčasné vojnové a humanitárne právo.[9]

Kybernetický boj môže byť obranný aj útočný. Súčasťou obrany je kontinuálna, permanentná ochrana, výstavba robustných a veľmi dobre chránených počítačových sietí, zriaďovanie tímov monitorujúcich kybernetický priestor, schopných rýchlo reagovať, odhaliť a zastaviť kybernetický útok, eliminovať a napraviť vzniknuté škody, atď. Problém však spočíva predovšetkým v útočnom kybernetickom boji. Útočný kybernetický boj predpokladá, okrem priamej pomoci jednotkám na bojisku, aj útoky na nepriateľskú infraštruktúru.

Infraštruktúra, proti ktorej sú kybernetické útoky zamerané, sa pritom príliš nezmenila: priemysel, poľnohospodárstvo, zdroje potravín a energií, dopravný systém, zásobovanie vodou, kanalizácia, komunikačné a informačné systémy, finančníctvo, zdravotníctvo, atď. Nič z toho dnes nefunguje bez podpory počítačov. Kyberpriestor je tak miestom, odkiaľ je možné ovládať celú „nervovú sústavu“ nášho moderného sveta. Účinný a efektívny kybernetický útok môže poškodiť komunikačné a informačné technológie a systém štátu natoľko, že sa jeho ekonomická, sociálna a bezpečnostná štruktúra úplne zrúti. Úspešný útok z internetu by mohol bez preháňania viesť dokonca ku kolapsu celého štátu, ak by nemal pripravené obranné prostriedky. Dnes je totiž možné dostať krajinu na kolená bez lietadiel a tankov a žiadna vojenská sila na svete tomu nemôže zabrániť.[10]

Terčom kybernetických operácií sú dáta v počítačoch a počítačových sieťach, pričom tieto dáta sa nemusia ani zďaleka nachádzať iba vo vojenských počítačoch a sieťach, ale naopak, celý rad scenárov (napr. v rámci strategickej informačnej vojny, neobmedzenej kybernetickej vojny a pod.) predpokladá práve využitie slabín protivníkovej infraštruktúry k realizácii plošných kybernetických útokov, ktoré majú ochromiť ekonomiku, hospodársky život, vyvolať strach, paniku, spôsobiť fyzické a materiálne škody a celkovo vo svojom účinku viesť k morálnemu rozvratu protivníka a zlomeniu jeho vôle pokračovať v odpore. Cieľom

[9] DAHL, E. 2014. *Too Good to Be Legal? Network Centric Warfare and International Law*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.princeton.edu/~jpia/pdf2004/Chapter%203.pdf>

[10] ŠITRIT, M. 2015. *Cyber fight and the resulting dangers*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.israelnetz.com>

kybernetického boja z podstaty veci nie je a nemôže byť fyzické zničenie (vojenských síl) protivníka.[11]

Útočný kybernetický boj vo svojej podstate popiera a prekračuje hranice medzi vojenskou a civilnou sférou. Vo všeobecnej rovine sa diskutuje o vedení kybernetického boja v kontexte princípov:

- rozlišovania – je jedným z kľúčových princípov, odkazuje na striktné rozlišovanie medzi vojenskými a civilnými cieľmi, aby bola výzbroj a taktika zákonné, nesmie spôsobovať ani nepriame škody civilnému sektoru a nekombatantom[12];
- primeranosti – stanovuje, že použité zbrane a taktika musia byť primerané vojenským cieľom operácie, čo má predchádzať neodôvodnene masívnemu použitiu sily;
- zákonnosti – odkazuje na medzinárodné zmluvy (dohovory, dohody), na základe ktorých použitá vojenská výzbroj a spôsob jej nasadenia nesmie odporovať takýmto zmluvám;
- nevyhnutnosti – vychádza z predpokladu, že použité zbrane a taktika musia byť odôvodniteľne nevyhnutné na dosiahnutie vojenských cieľov operácie;
- ľudskosti – spočíva v zákaze použitia zbraní a spôsobu ich nasadenia, ktorý by spôsobil obetiam zbytočné utrpenie a kalkuloval so šírením strachu;
- neutrality – nasadené zbrane ani spôsob ich použitia by nemali viesť k poškodeniu zdravia alebo smrti ľudí v neutrálnych krajinách, poškodeniu ich majetku alebo životného prostredia.[13]

V prípade útočnej kybernetickej vojny nie je možné týmto princípom vyhovieť. Princíp rozlišovania je neuplatniteľný v prípade strategickej informačnej vojny alebo neobmedzenej kybernetickej vojny jednak preto, že vojenská a civilná infraštruktúra sú úzko previazané, nakoľko armády využívajú aj komerčnú (civilnú) komunikačnú infraštruktúru, a jednak preto, že aby mal kybernetický boj skutočne účinný dosah, je často počítané s útokmi na kritickú infraštruktúru štátu, ktorá ovplyvňuje život celej populácie, a to úplne úmyselne. Princíp primeranosti nie je v prípade kybernetického boja uplatniteľný v prípadoch, keď kybernetické operácie nemajú žiadne priame vojenské ciele, pričom zjavne tento fakt hrá úlohu aj v prípade princípe nevyhnutnosti. Princíp zákonnosti by síce bol dodržaný v tom zmysle, že kybernetické zbrane nie sú priamo zakázané, na druhej strane ich využitie porušuje celý rad rôznych zmlúv a dohovorov, počnúc napr. ochranou komunikácií a pošty. Princíp ľudskosti predpokladajúci zamedzenie vyvolávania strachu je ťažko uplatniteľný v prípadoch, keď cieľom kybernetického boja je alebo má byť narušenie morálky nepriateľskej populácie a vyvolanie strachu, paniky by bolo jedným z kľúčových komponentov takejto operácie. Vo prepojenom kyberpriestore absolútne nie je možné zaručiť dodržanie princípu neutrality, nakoľko môže byť nevyhnutné využiť kybernetický priestor a komunikačné trasy neutrálnych štátov, ale nemusí to byť ani úmyselné. Navyše dopad kybernetického útoku nedá presne alokovať.[14]

Napriek tomu patrí kybernetický boj medzi tie oblasti vojenstva, ktorá sa najmä v poslednej dekáde teší značnej pozornosti, pretože môžu slúžiť k posilneniu či multiplikácii vojenského potenciálu technologicky vyspelých krajín. Nie je vôbec prekvapujúce, že najväčší záujem táto oblasť pritiahla v USA, to znamená v krajine jednoznačne patriacej k technologicky najpokročilejším a s najväčšími investíciami do vojenstva. Doktríny, ktoré boli v tejto oblasti

[11] ELLIS, B. W. 2011. *The International Legal Implications and Limitations of Information Warfar*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_01.pdf>

[12] *Poznámka*: Kombatant je príslušník ozbrojených síl s bojovým poslaním, bojovník, resp. príslušník ozbrojenej moci plniaci konkrétne vojnové úlohy, a preto požívajúci podľa príslušných medzinárodných noriem určitú ochranu (Slovník cudzích slov, 2005).

[13] GREENBERG, L., T., GOODMAN, S., E., SOO HOO, K., J. 2008. *Information Warfare and International Law*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.dodccrp.org/files/Greenberg_Law.pdf>

[14] DARTON, G. Information Warfare and the Laws of War. In *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave Macmillan, 2016. s. 299.

rozpracované v ďalších krajinách NATO (napr. vo Veľkej Británii), v Ruskej federácii alebo Číne ani zďaleka nedosahujú taký stupňa komplexnosti ako teoretické či doktrinálne materiály americkej armády. Americké doktríny sú z toho dôvodu aj pre ostatné spomínané krajiny referenčnými.

V USA pritom v súvislosti s kybernetickými hrozbami silnejú v posledných rokoch pozície zástancov názoru, že obranná kybernetická vojna je v horšom prípade odsúdená na neúspech, v lepšom prípade by bola neúmerne nákladná a náročná. Počas niekoľkých vykonaných cvičení zameraných na kombináciu prírodnej katastrofy a/alebo fyzického a kybernetického útoku sa opakovane ukazovalo, že infraštruktúra je zraniteľná kybernetickými útokmi, ktoré môžu spôsobiť alebo znásobiť obrovské škody aj straty na ľudských životoch. Obrana proti kybernetickým útokom je však nesmierne ťažká. Jedným z dôvodov je veľmi výrazný podiel komerčnej alebo privátnej infraštruktúry na obrannej infraštruktúre, ktorý sa pohybuje podľa krajín v rozmedzí 80 až 95 %.[15] Do úvahy je v tomto prípade nutné vziať ten fakt, že komerčné infraštruktúry vždy boli a aj teraz sú budované tak, aby pri čo najmenších nákladoch generovali čo najvyšší zisk.

V priebehu predchádzajúcich desaťročí bol na internet či do kybernetického priestoru prevedený celý rad aktivít, ktoré boli predtým ošetrené mechanicky alebo boli kontrolované ľudskými supervízormi, čo – úplne v duchu informačnej spoločnosti – šetrí náklady na pracovnú silu, priestor a čas. Na druhej strane sa tieto aktivity stali zraniteľnejšími.[16] Komerčné infraštruktúry neboli budované primárne s ohľadom na bezpečnosť. Do úvahy treba vziať v nadväznosti na vyššie uvedené informácie aj ďalší fakt, a to, že škody spôsobené útokmi či zlyhaniami môžu byť nižšie, než by boli náklady na zvýšené zabezpečenie. V privátnych segmentoch informačnej infraštruktúry môže byť situácia ešte výrazne horšia s ohľadom na fakt, že značný podiel užívateľov komunikačných a informačných systémov a prostriedkov nedisponuje ani zďaleka dostatočnými znalosťami a skúsenosťami, aby dokázali zabezpečiť infraštruktúru vo svojom vlastníctve.[17] Príkladom hrozby založenej na privátnych zdrojoch môžu byť obrovské botnety[18], ktoré sa opierajú najmä o tisíce osobných pracovných staníc.

Zabezpečenie komerčnej a privátnej infraštruktúry by si vyžiadalo značné finančné náklady, náročnú úpravu legislatívy a uzatvorenie dohôd medzi privátnym a verejným sektorom, pričom istotne by všetko ani v najlepšom prípade nemohlo byť stopercentné. A hoci sa situácia v oblasti ochrany počítačov a počítačových sietí výrazne zlepšuje, silnejú hlasy, že armády technologicky vyspelých štátov potrebujú útočnú doktrínu kybernetického boja. To, čo je nevýhodou pri obrannej kybernetickej vojne, je v prípade ofenzívneho kybernetického boja výhodou.[19] A tak sa objavuje doktrína ofenzívneho kybernetického boja. Na rozdiel od

---

[15] CHILDS, J. Vojenská revoluce I. Přechod k modernímu válečnictví. In *Historie moderní války*. Praha: Mladá fronta, 2007. s. 36.

[16] ANDRASSY, V., GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, roč. 5, č. 2, 2015. s. 12.

[17] KORAUŠ, A., VESELOVSKÁ, S., KELEMEN, P. Cyber security as part of the business environment. In *Zborník z medzinárodnej konferencie Medzinárodné vzťahy 2017: Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice, 2017. s. 568.

[18] *Poznámka*: Za botnet je zvyčajne považovaná sieť počítačov infikovaných bez vedomia majiteľa či autorizovaného používateľa programami umožňujúcimi ich úplnú alebo čiastočnú kontrolu útočníkom. Tieto siete môžu byť obrovské (obsahujúc desiatky tisíc počítačov) vzhľadom na to, že sa na ich získavanie v posledných rokoch využívajú automatizované nástroje, sú využívané ako infraštruktúra, z ktorej sú vedené útoky (od rozosielania spamu, cez prenikanie do ďalších sietí, na defraudáciu až po útoky zamerané na odmietnutie služby). Vytváranie botnetov je v súčasnosti samostatným biznisom, útočníci s botnetmi alebo ich časťami obchodujú – predávajú ich záujemcom na čiernom trhu, ktorí ich využívajú k ďalšej nelegálnej činnosti. (Turek, 2008. *Botnety*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.itnews.sk/buxus_dev/generate_page.php?page_id =53630>).

[19] *Poznámka*: J. Langevin – vtedajší predseda House Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology – koncom septembra 2008 konštatoval, že najlepšou obranou je

defenzívneho, pri ktorom si možno predstaviť dodržiavanie konvencií, je ofenzívny boj nekonvenčný. V tomto bode sa zbieha niekoľko tendencií. V prípade slabších hráčov je to, ako už bolo naznačené, snaha kompenzovať prevahu protivníka. V prípade silných aktérov snaha využiť ich potenciál, ich technologické kapacity k vedeniu útočného kybernetického boja a tiež nízka efektivita obranného kybernetického boja. Výsledkom je všestranné nerešpektovanie konvencií.

Vzhľadom na to, že diskusie o medzinárodnom a právnom postavení útočného kybernetického boja sú nápadne podobné diskusiám o postavení terorizmu, vynára sa otázka, či vo vzťahu k vojnovým konvenciám nejde o ten istý problém a tú istú otázku.

Terorizmus ako taký nebol doteraz uspokojivo definovaný. Existuje síce celý rad viac či menej obsiahlych definícií teroristického násilia, od definície vypracovanej P. Wilkinsonom, ktorý terorizmus definoval ako „*donucovacie zastrašovanie, systematicky užívané vraždenie a ničenie alebo hrozba vraždenia a ničenia k terorizovaniu jednotlivcov, skupín, komunít či vlád s cieľom dosiahnuť uznanie politických požiadaviek teroristov*“ až po syntetickú definíciu vychádzajúce z textu A. Schmida, ktorá terorizmus chápe ako „*metódu vzbudzovania strachu prostredníctvom opakovaných násilných aktov, vykonávaných tajnými alebo polotajnými jednotlivcami, skupinami či štátnymi orgánmi z idiosynkratických, kriminálnych alebo politických dôvodov, pričom na rozdiel od atentátov nie sú priame obete násilia pravým terčom teroru. Okamžité ľudské obete násilných aktov sú obvykle buď vybrané náhodne (príležitostné terče) z cieľovej verejnosti, alebo zámerne (reprezentatívne, symbolické terče) a slúžia na odovzdanie správy. Komunikačné procesy medzi teroristami (teroristickými organizáciami), obeťami a hlavným terčom, založené na násilí a šírení strachu, sú využívané k manipulácii hlavného terča (verejnosti) tým, že sa z nich stávajú terče teroru, požiadaviek alebo na upútanie pozornosti v závislosti na tom, či ide o zastrašovanie, násilné nútenie alebo šírenie propagandy*“.[20]

Empirické definície, menej závislé na kultúrnom a politickom prostredí, sa pokúšajú o extrakciu podstatných rysov, ktorými sa terorizmus líši od iných foriem nekonvenčného násilia. Zvyčajne odkazujú na fakt, že v prípade terorizmu ide o špecifickú formu psychologického boja, ktorý využíva násilie s cieľom vyvolať psychologickú reakciu u širšieho počtu recipientov ako sú priame obete.[21] V paralele s kybernetickým bojom je možné konštatovať, že cieľom terorizmu nie je a nemôže byť fyzické zničenie vojenských síl protivníka, ale ochromenie jeho morálky.

Ambiciózny pokus o vypracovanie podrobného katalógu rysov či vlastností terorizmu podnikol A. Merari, ktorý porovnával vojnu, guerilllu a terorizmus. Podľa jeho názoru sa terorizmus a vojna líšia takmer vo všetkých zo sledovaných kritérií. Vojenská operácia má zahŕňať či zahŕňa akcie veľkých zoskupení, počas ktorých sa využíva široké spektrum vojenskej techniky a zbraní, ide o operácie, ktorých cieľom sú prevažne vojenské jednotky protivníka a ich fyzické (z)ničenie. Cieľom vojnových akcií je kontrola teritória, pričom vojnové zóny sú geograficky rozoznateľné, vojaci nosia uniformy a jasné identifikačné znaky. To zakladá zákonnosť vojenských operácií. Teroristi oproti tomu operujú v malých skupinách, používajú špecializované zbrane a osobitnú taktiku, ich cieľom nie sú vojenské sily protivníka, ale politickí oponenti, symboly a verejnosť, pričom zamýšľaným účinkom je psychologický nátlak,

"dobrý útok" a USA by sa preto mali koncentrovať v prvom rade na rozvoj útočných schopností v rámci kybernetického boja (WT, 2008).

[20] SCHMID, A. Problémy s definováním terorismu. In *Encyklopedie světový terorismus. Od starověku až po útok na USA*. Praha: Svojtka&CO, 2001. s. 178-182.

[21] STRMISKA, M. *Terorismus a demokracie*. Brno: Masarykova univerzita, 2001.

nie fyzické zničenie protivníka. Teroristi nenosia uniformy, nemožno ich identifikovať, boje prebiehajú v geograficky nerozoznateľných zónach. Teroristickým akciám chýba zákonnosť.[22]

To čo môže slúžiť ako ilustrácia zmeny charakteru vojenstva na prípade útočného kybernetického boja, je fakt, že kritériá, ktoré Merari ponúkol vo svojom výskume, a vlastnosti, ktoré pripisuje terorizmu a ktorými sa podľa neho terorizmus odlišuje od vojny, vcelku presne opisujú aj rozdiel medzi konvenčnou vojnou a kybernetickým bojom. Ofenzívny kybernetický boj, ako sa zdá, v mnohých svojich ohľadoch zodpovedá skôr terorizmu než vojnovej akciám tak, ako boli chápané v minulosti.

Kybernetický boj vo svojej podstate vykazuje znaky zásadne odlišné od konvenčného boja. Tieto znaky sú spoločné mnohým iným formám boja proti vyspelej spoločnosti a vymykajú sa normám, podľa ktorých je v súčasnej dobe posudzovaná oprávnenosť akcií a ich zákonnosť. Snaha predkladať kybernetický boj ako úplne novú, unikátnu a kvalitatívne odlišnú formu vedenia boja však môže byť založená tak na nepochopení podstaty jeho nekonvenčnosti, ako aj politickou snahou (vedomou i nevedomou) o kodifikáciu pravidiel vyhovujúcich najmä silným hráčom s dostatočným politickým (mocenským) vplyvom.

Záver

Na základe skúmania a evaluácie viacerých atribútov je možné v závere uviesť, že v prípade kybernetického boja ide o špecifický, nekonvenčný a vzhľadom na používané prostriedky unikátny prípad vedenia boja, hoci v bojoch proti superiórnym, technologicky, logisticky a početne silnejším protivníkom sú využívané aj iné, dlhodobo existujúce formy vedenia boja, ktoré vykazujú podobné charakteristiky. V tejto súvislosti je potrebné doplniť, aj vzhľadom na fakt, že význam všetkých nekonvenčných foriem vedenia boja neustále rastie v závislosti na posilňovaní konvenčných kapacít niektorých silných hráčov, že ide o symptóm všeobecného vývoja v oblasti vojenstva. Spoločným rysom prebiehajúcich zmien je presun ťažiska bojových operácií. Namiesto vojenskej porážky protivníka, zničení jeho ozbrojených síl sa cieľom operácií stáva morálka protivníka, hospodárstvo, vôľa bojovať a klásť odpor. Je zjavné, že slabší aktéri, ktorí nemôžu čeliť podstatne silnejším aktérom otvorene, na bojovom poli, nemajú dôvod a ani príliš nechcú dodržiavať konvencie. Silní hráči zasa vedia, že je pre nich nevýhodné konvenčným spôsobom čeliť nekonvenčným hrozbám. V niektorých prípadoch to dokonca ani nie je možné.

Tento vývoj, ako aj úzko súvisiace diskusie možno ilustrovať rovnako tak na príklade terorizmu, ako aj na príklade kybernetického boja. Možnosti, ktoré sa ponúkajú, sú v zásade dve. Prvá možnosť vychádza z toho, že dôjde k prehodnoteniu a modifikácii konvencií a následne k modifikácii vojenských doktrín, pretože doktríny orientujúce sa na porážku či fyzické zničenie vojenských síl protivníka sú nedostatočné v prípade použitia nekonvenčných foriem boja, pričom, ako už bolo naznačené, nekonvenčné formy boja sa budú v budúcnosti používať čoraz častejšie. Druhá možnosť je, že problém zostane neriešený a každý prípad bude považovaný za unikátny svojho druhu a analyzovaný v rámci existujúcich konvencií a podľa politického vplyvu konkrétnych aktérov. Vojenské doktríny zostanú v zásade nezmenené a nekonvenčné operácie budú realizované v rámci špeciálnych operácií ako podporné operácie, a to dovtedy, kým pôjde iba o marginálnu oblasť a okrajový komponent boja. Takýto vývoj s najväčšou pravdepodobnosťou povedie v budúcnosti k rozpadu systému konvencií ako takého a ku vzniku špecializovaných jednotiek, zložiek, organizácií a inštitúcií ktoré sa budú podieľať na boji, ale nebudú mať status armády. Vytvorí sa tak akýsi prechod medzi civilnou sférou a sférou vojenskou, pričom dualita systému bude oslabená a/alebo postupne úplne vymizne.

[22] MERARI, A. 2003. *Terrorism as a Strategy of Insurgency*. [online]. [cit. 2019-04-18]. Dostupné na: <https://www.researchgate. net/publication/254267590_Terrorism_as_a_Strategy_of_Insurgency>

Zoznam použitej literatúry:

1. ANDRASSY, V., GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In: *Košická bezpečnostná revue*, roč. 5, č. 2, 2015. s. 11-18. ISSN 1338-4880.
2. BRHLÍKOVÁ, R. Suverenita štátu. In: *Právny obzor*, roč. 80, č. 3, 1997. s. 362-368. ISSN 0032-6984.
3. DAHL, E. 2014. *Too Good to Be Legal? Network Centric Warfare and International Law*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.princeton.edu/~jpia/pdf2004/Chapter%203.pdf>
4. DARTON, G. Information Warfare and the Laws of War. In *Cyberwar, Netwar and the Revolution in Military Affairs*. New York : Palgrave Macmillan, 2016. ISBN 1-4039-8717-3.
5. EICHLER, J. *Mezinárodní bezpečnost na počátku 21. století*. Praha : AVIS, 2006. 303 s. ISBN 80-7278-326-2.
6. ELLIS, B. W. 2011. *The International Legal Implications and Limitations of Information Warfar*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.iwar.org.uk/law/resources/iwlaw/ Ellis_B_W_01.pdf>
7. GREENBERG, L., T., GOODMAN, S., E., SOO HOO, K., J. 2008. *Information Warfare and International Law*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.dodccrp.org/files/Greenberg_Law.pdf>
8. CHILDS, J. Vojenská revoluce I. Přechod k modernímu válečnictví. In *Historie moderní války*. Praha: Mladá fronta, 2007. s. 34-53. ISBN 978-80-204-1540-0.
9. IVANČÍK, R. 2012. Teoreticko-metodologický pohľad na bezpečnosť. In *Vojenské reflexie*, 2012, roč. 7, č. 1, s. 38-57. ISSN 1336-9202. [online]. [cit. 2019-04-19]. Dostupné na internete na: <http://www.aos.sk/casopisy/reflexie/vojenske_reflexieVII_1.pdf>
10. KAZANSKÝ, R. *Súčasné problémy výskumu medzinárodných konfliktov a kríz a ich riešenia*. Banská Bystrica : Vydavateľstvo UMB – Belianum, 2013. 215 s. ISBN 978-80-557-0573-6.
11. KORAUŠ, A., VESELOVSKÁ, S., KELEMEN, P. Cyber security as part of the business environment. In *Zborník z konferencie Medzinárodné vzťahy 2017: Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice, 30. novembra - 1. decembra, 2017, Vydavateľstvo Ekonóm, 2017. 1113 s. ISBN 978-80-225-4488-7.
12. LASICOVÁ, J., UŠIAK, J. *Bezpečnosť ako kategória*. Bratislava : Veda – vydavateľstvo Slovenskej akadémie vied, 2012. 264 s. ISBN 978-80-224-1284-1.
13. MAREŠ, M. 2007. *Vymezení pojmů terorismus, válka a guerilla v soudobé bezpečnostní terminologii*. [online]. [cit. 2019-04-18]. Dostupné na: <https://www.obranaastrategie.cz/filemanager/files/ 6330.pdf>
14. MERARI, A. 2003. *Terrorism as a Strategy of Insurgency*. [online]. [cit. 2019-04-18]. Dostupné na: <https://www.researchgate.net/publication/254267590_Terrorism_as_a_Strategy_of_Insurgency>
15. RMA. 2008. *The RMA Debate*. [online]. [cit. 2019-04-17]. Dostupné na: <http://www.comw.org/rma/>
16. ROBERTS, A. 2002. *Counter-terrorism, Armed Force and the Laws of War*. Social Science Research Council. [online]. [cit. 2019-04-18]. Dostupné na: <http://essays.ssrc.org/10yearsafter911/counter-terrorism-armed-force-and-the-laws-of-war/>
17. SAV. 2005. *Slovník cudzích slov*. [online]. [cit. 2019-04-17]. Dostupné na: <http://slovniky.juls.savba.sk>

18. SCHMID, A. Problémy s definováním terorismu. In *Encyklopedie světový terorismus. Od starověku až po útok na USA*. Praha : Svojtka&CO, 2001. ISBN 80-7237-340-4.
19. STRMISKA, M. *Terorismus a demokracie*. Brno : Masarykova univerzita, 2001. ISBN 80-210-2755-X.
20. ŠITRIT, M. 2015. *Cyber fight and the resulting dangers*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.israelnetz.com>
21. TUREK, R. 2008. *Botnety*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.itnews.sk/buxus_dev/ generate_page.php?page_id=53630>
22. WATERMAN, S. 2015. *U.S. urged to develop offensive cyberwar capabilities*. [online]. [cit. 2019-04-18]. Dostupné na: <http://www.upi.com/Emerging_Threats/2008/09/29/US_urged_to_develop_ offensive_cyberwar_capabilities/UPI-49311222720057>
23. WT. 2008. U.S. urged to go on offense in cyberwar. In *The Washington Times*. [online]. [cit. 2019-04-18]. Dostupné na: <https://www.washingtontimes.com/news/2008/sep/29/us-urged-to-go-on-offense-in-cyberwar/>

Kontaktné údaje:
plk. gšt. v. z. Ing. Radoslav Ivančík, PhD. et PhD.
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
radoslav.ivancik@minv.sk

Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. storočí

Radoslav Ivančík, Ľubica Baričičová

Abstrakt:
Uvoľnenie medzinárodného napätia po skončení tzv. studenej vojny, dynamický nárast intenzity vzájomnej spolupráce na nadnárodnej úrovni a vplyv globalizačných procesov priniesli koncom druhého a začiatkom tretieho milénia prudký rozvoj viacerých odvetví, vrátane sféry komunikačných a informačných technológií. Intenzívna internacionalizácia, kooperácia a prepojenosť participujúcich aktérov spolu s oslabovaním časových a priestorových bariér však so sebou priniesli okrem mnohých pozitív aj viaceré negatíva. Tie sa prejavili najmä v postupnom zhoršovaní bezpečnostného prostredia, bezpečnostnej situácie a raste asymetrických bezpečnostných hrozieb v podobe medzinárodného terorizmu, nelegálnej migrácie, cezhraničného organizovaného zločinu, či stále častejšie sa vyskytujúcich kybernetických útokoch na verejné i súkromné počítačové siete. Z toho dôvodu sa kybernetické hrozby stávajú jednou z najvýznamnejších asymetrických bezpečnostných hrozieb v 21. storočí.
Kľúčové slová:
Kybernetické hrozby, asymetrické bezpečnostné hrozby, komunikačné a informačné technológie.

Abstract:
Release of international tension after the end of the Cold War, the dynamic increase in the intensity of cooperation at the transnational level and the impact of globalization processes have brought about a rapid expansion of several sectors, including the sphere of communications and information technologies at the end of the second and the beginning of the third millenniums. However, intensive internationalization, cooperation and interconnection of participating actors, together with weakening of time and space barriers, brought along with lots of positives also many negatives. These were reflected mainly in the gradual deterioration of the security environment, the security situation and the growth of asymmetric security threats in the form of international terrorism, illegal migration, cross-border organized crime and recently still more often in the form of cyberattacks on public and private computer networks. Therefore, cyber threats are becoming one of the most significant asymmetric security threats in the 21st century.
Key words:
Cyber threats, asymmetric security threats, communication and information technologies.

Úvod

Dynamický vývoj ľudstva, prebiehajúce procesy prehlbujúcej sa globalizácie, spoločenskej i hospodárskej modernizácie a politickej, ekonomickej i sociálnej liberalizácie ľudskej spoločnosti, spolu s prudkým nástupom vedecko-technického rozvoja najmä v oblasti komunikačných a informačných technológií, vygenerovali po skončení studenej vojny a rozpade bipolárneho usporiadania sveta mnohé nepriaznivé sprievodné javy, ktoré sa dnes výrazným spôsobom podieľajú na kontinuálnom zhoršovaní globálneho bezpečnostného prostredia. Neustále sa zvýrazňujúce ekonomické a sociálne rozdiely vo vývoji ľudskej spoločnosti, zlyhávanie štátnych štruktúr v krajinách tzv. tretieho sveta a ich zaostávanie za vývojom vytvárajú spolu s neschopnosťou dostatočne rýchlo sa adaptovať na novú situáciu vhodné podmienky pre rast nových bezpečnostných hrozieb a negatívne pôsobenie neštátnych aktérov. Aj preto sa dnes oveľa častejšie stretávame s informáciami o asymetrických bezpečnostných hrozbách, asymetrických operáciách či asymetrických protivníkoch, ktorí na dosiahnutie svojich cieľov využívajú nekonvenčné prostriedky, vrátane najnovších technológií.

Práve bezprecedentný rozvoj komunikačných a informačných technológií spojený s mohutným nasadením a využívaním komunikačných a informačných systémov a prostriedkov prináša na jednej strane vyššiu kvalitu takmer do všetkých sfér života spoločnosti, no na strane druhej zvyšuje zraniteľnosť spoločnosti i jednotlivca. Podľa Patela je vývoj v tejto oblasti tak rýchly, že legislatíva, morálka, písané i nepísané zásady slušnosti a korektnosti v súkromných i verejných vzťahoch a ďalšie sociálne atribúty nie sú v mnohých

prípadoch rešpektované, a tým nedokážu adekvátne rýchlo reagovať na zmenenú situáciu.[1] Vytvorením nového virtuálneho priestoru v podobe kyberpriestoru, podporujúceho virtuálnu existenciu, dochádza ku vzniku a postupnému nárastu kriminálnych a nelegálnych aktivít v tomto priestore.[2]

Vznik kyberpriestoru nadväzuje na vznik modernej informačnej spoločnosti, ktorá je všeobecne definovaná ako „*spoločnosť, v ktorej kvalita života a jej sociálny a ekonomický rozvoj závisia na informáciách a schopnosti ich výmeny, spracovania a využitia; to znamená, že informácia predstavuje kľúčový faktor takejto spoločnosti*“.[3] Z technologického pohľadu sa termínom informačná spoločnosť označuje spoločnosť, ktorá vo vysokej miere využíva informačno-komunikačné technológie založené na prostriedkoch výpočtovej techniky a s tým spojenú digitalizáciu. Dôsledkom toho dochádza k vytvoreniu spoločnosti sietí, vďaka ktorej si ľudia môžu kdekoľvek na svete vymieňať obrovské množstvo informácií. Túto skutočnosť výstižne odráža komerčne znejúci slogan „všetko je na webe“. Keďže zásluhou rýchleho rozvoja komunikačných technológií sa výmena informácií odohráva prakticky v reálne možnom čase bez ohľadu na miesto pobytu účastníkov interpersonálnej komunikácie, dovtedy obmedzujúci faktor vzdialenosti stráca na význame.[4]

Samotný kyberpriestor je označovaný ako „*svet virtuálnej reality, v ktorom sa odohrávajú rôzne, paradoxne reálne veci, napríklad telefonické hovory, e-mailová komunikácia, bankové prevody a pod.*“[5] Iná definícia hovorí, že: „*Kyberpriestor je človekom vytvorené prostredie na vytváranie, prenos a využitie informácií vo viacerých formátoch, pričom je tvorený hardvérom, sieťami, operačnými systémami a prenosnými štandardmi*“.[6] V odbornej literatúre sa nachádzajú aj podstatne zložitejšie definície kybernetického priestoru so širším pohľadom najmä na aktivity prebiehajúce v tomto priestore. Zároveň sa ale možno stretnúť aj s veľmi jednoduchými definíciami, ako napríklad: „*Kyberpriestor je informačný priestor tvorený súčtom všetkých počítačových sietí*“.[7]

Keďže informácie v modernej informačnej spoločnosti predstavujú veľmi cenný zdroj,[8] v kyberpriestore prebiehajú, ako už bolo naznačené vyššie, aj mnohé nelegálne a kriminálne aktivity, ktoré sú zdrojom veľmi špecifických a vysoko nebezpečných nových asymetrických bezpečnostných hrozieb – kybernetických hrozieb. Z tohto pohľadu narastá význam a dôležitosť kybernetickej bezpečnosti. Bezpečnosť a ochrana pred kybernetickou kriminalitou totiž predstavuje čoraz väčšiu výzvu aj pre bezpečnostné zložky štátu. Bezpečnosť, tak ako sme ju doteraz boli zvyknutí vníma, sa mení a je tomu potrebné prispôsobiť zaužívané nástroje ochrany a prevencie, prípadne vytvoriť a aplikovať nové.

Kybernetická bezpečnosť predstavuje súhrn organizačných, politických, právnických, technických a vzdelávacích opatrení a nástrojov smerujúcich k zaisteniu chráneného a odolného kyberpriestoru pre subjekty verejného a súkromného sektora. Pomáha identifikovať, hodnotiť a riešiť hrozby v kyberpriestore, znižovať ich riziká a eliminovať

---

[1] PATEL, D., R. *Information Security: Theory and Practice*. New Delhi: PHI Learning Pvt. Ltd., 2008. 312 s.

[2] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. 284 s.

[3] WEBSTER, F. *Theories of the Information Society*. New York: Routledge, 2002. s. 56.

[4] BARIČIČOVÁ, Ľ. *Kompetencie policajných manažérov*. Bratislava: APZ, 2011. s. 67.

[5] KREMMER, J., F., MÜLLER, B. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin: Springer Science & Business Media, 2013. 284 s.

[6] RATTRAY, G., J. *Strategic Warfare in Cyberspace*. Cambridge: MIT Press, 2001. 517 s.

[7] DENNING, D. 2000. *Cyberterrorism*. [online]. [cit. 2019-06-04]. Dostupné na: <http://palmer.wellesley.edu/~ivolic/ pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>

[8] Viac pozri: ANDRASSY, V., GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, roč. 5, č. 2, 2015. s. 12. BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 8.

dopady kybernetických útokov, ktoré sa realizujú napríklad prostredníctvom kyberterorizmu, kyberšpionáže, či kyberkriminality.[9]

Kyberterorizmus

Pojem kybernetický terorizmus alebo jeho skrátený tvar kyberterorizmus sa stal v posledných rokoch veľmi frekventovaným pojmom, čo súvisí tak so širšou percepciou terorizmu najmä po útokoch z 11. septembra 2001 v New Yorku a vo Washingtone[10], ako aj s prudkým rozvojom a využívaním moderných informačno-komunikačných technológií. Kyberterorizmus je označovaný za nový druh terorizmu, od ktorého sa odlišuje práve použitím (využitím) komunikačných a informačných technológií, systémov a prostriedkov. Ide v podstate o zneužitie kyberpriestoru na teroristické účely.

Kyberterorizmus je podľa Denningovej konvergenciou terorizmu a kybernetického priestoru. Všeobecne ho možno chápať ako nezákonný nebezpečný útok proti počítačom, počítačovým sieťam a informáciám v nich skladovaných v prípade, že tento útok je realizovaný za účelom zastrašiť alebo donútiť vládu alebo obyvateľstvo k podporovaniu útočníkových politických, náboženských alebo sociálnych cieľov.[11]

Vzhľadom na skutočnosť, že zatiaľ neexistuje jednotná univerzálna definícia terorizmu, preto v súčasnosti neexistuje ani žiadna jednotná univerzálna definícia kyberterorizmu. Ak by sme však vychádzali z pomerne často používanej definície, podľa ktorej „*terorizmus predstavuje násilie, resp. vyhrážanie sa násilím a zastrašovanie uplatňované proti odporcovi až do jeho fyzického zničenia*," tak potom „*kyberterorizmus predstavuje rovnakú aktivitu, len vykonávanú v rámci sveta informačných systémov*".[12]

V zmysle iného chápania kyberterorizmus „*predstavuje použitie útokov na báze internetu v teroristickej činnosti, vrátane aktov úmyselného rozsiahleho narušenia počítačových sietí, najmä osobných počítačov pripojených k internetu, prostredníctvom nástrojov, ako sú počítačové vírusy a pod. Ciele takéhoto konania musia byť politické alebo ideologické*".[13] Kyberterorizmus je možné tiež vnímať ako „*premyslený, politicky motivovaný útok organizovaných skupín, jednotlivcov alebo tajných agentov namierený proti informačným sieťam, počítačovým programom a dátam*".[14]

Severoatlantická aliancia za kyberterorizmus považuje „*kybernetický útok za použitia alebo zneužitia počítača alebo informačných a komunikačných sietí tak, aby bola spôsobená dostatočná deštrukcia alebo narušenie za účelom generovania strachu alebo zastrašovania spoločnosti v mene ideologického cieľa*".[15]

Množstvo ďalších definícií, ktoré sa zaoberajú týmto fenoménom modernej informačnej spoločnosti, sa namiesto všeobecne platnej definície zaoberá skôr možným scenárom vývoja určitej situácie, ktorá zodpovedá kyberteroristickému útoku. Medzi často sa vyskytujúcimi scenármi sa nachádza napríklad ten, v ktorom kyberterorista ovládne systém riadenia leteckej

---

[9] BREZULA, J. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním. Zborník príspevkov*. Bratislava: APZ, 2018. s. 143.

[10] Historicky známe sú tiež krvavé útoky na mnohých ďalších miestach sveta - Moskva, Londýn, Petrohrad, Madrid, Istanbul, Paríž, Nice, Berlín, Manchester, Brusel, atď.

[11] DENNING, D. 2000. *Cyberterrorism*. [online]. [cit. 2019-06-04]. Dostupné na: <http://palmer.wellesley.edu/~ivolic/ pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>

[12] PŘIBYL, T. 2008. *Kyberterorizmus.* [online]. [cit. 2019-06-04]. Dostupné na:<http://www.virusy.sk/clanok.ltc? ID=402.html>

[13] DENNING, D. E. 2006. *Activism, Hacktivism and Cyberterorism: The Internet as a Tool for Influencing Foreign Policy*. [online]. [cit. 2019-06-04]. Dostupné na: <http: //www:nautilus.org/info-policy/workshop/papers/denning.html>

[14] JANCZEWSKI, L., COLARIK, A., M. *Managerial Guide for Handling Cyberterrorism and Information Warfare*. Idea Group Inc., 2005. s. 18.

[15] BOTTESINI, B. Medzinárodná kooperácia v boji proti kyberterorizmu. In *EAQ*, roč. 3, č. 4, 2008. s. 11.

premávky a letiskovej prevádzky pozostávajúci z rozsiahlej siete počítačov, a pod hrozbou poškodenia alebo vyradenia celej siete sa snaží dosiahnuť svoje ciele alebo ciele teroristickej skupiny (organizácie), ktorej je členom.[16]

Iný variant scenára kyberteroristického útoku predstavuje sofistikovaný útok na počítačové systémy nemocnice, pri ktorom kyberterorista vykoná zmeny v záznamoch o pacientoch a v tichosti sa stiahne do úzadia. Žiadny následok nie je na prvý pohľad badateľný, až do chvíle, keď začnú mať pacienti alergické reakcie na nesprávne lieky, keď sa na operáciu začnú pripravovať zdraví ľudia alebo dokonca niektorí začnú umierať na zdanlivo banálne diagnózy.[17] Ďalšie možné varianty počítajú s kybernetickými útokmi na finančné inštitúcie (banky, poisťovne, burzy a podobne) za účelom ich vydierania a následného peňažného zisku.[18]

Okrem vyššie uvedených scenárov existujú aj také, ktoré sú spojené s útokmi voči kritickej infraštruktúre štátu alebo tiež s nabúraním sa do vojenských i civilných bezpečnostných systémov. Ich narušenie, poškodenie alebo zničenie by malo ďalekosiahle následky a spôsobilo by škody strategického významu. Samozrejme, existujú i scenáre, ktoré nepočítajú s veľmi sofistikovanými útokmi. Napríklad útok zameraný na vyradenie zdroja energie môže spôsobiť, že obyvatelia moderného inteligentného mesta[19] si nebudú môcť kúpiť základné potraviny potrebné na ich obživu kvôli nefunkčnosti pokladní v obchodoch, či vyradeniu platobných terminálov z prevádzky a pod. I v takomto jednoduchom prípade však škody spôsobené výpadkom elektrickej energie na relatívne malom území môžu v priebehu krátkej doby narásť do obrovských výšok a spôsobiť ťažko zvládnuteľný chaos.

V mnohých prípadoch kyberterorizmu významnú úlohu zohráva politicky orientovaný terorizmus, separatizmus a ďalšie druhy terorizmu prejavujúce sa najmä na internete. Aktéri pritom nemusia byť priamymi členmi teroristickej skupiny (organizácie). Môžu to byť hackerské skupiny najaté na konkrétny kybernetický útok (napr. H4H)[20]. Najčastejšie však ide o špeciálne bunky teroristických skupín (organizácií), alebo zvláštne vojenské jednotky, príp. jednotky iných ozbrojených zložiek v prípade štátneho terorizmu.[21] Ich typickým znakom je vysoká kvalita útokov, špecifické stratégie a špecifické ciele.

Inú charakteristiku, ciele a spôsob majú kybernetické útoky realizované buď ideologickými sympatizantmi alebo tzv. hľadačmi vzrušenia. Kým prví sa snažia dať najavo svoju príslušnosť k istej názorovej skupine pomocou hackerských nástrojov, väčšinou dostupných na internete, u druhých je hlavným motívom exhibicionizmus. Významný počet kybernetických útokov je totiž ovplyvnený politickou atmosférou a snahou využiť niektorý mediálne známy prebiehajúci konflikt na vlastné zviditeľnenie sa a pod.[22]

---

[16] Bližšie pozri napr.: CAROLL, A. 2017. *Preparing for Worst-Case Scenarios with Cyber Attacks*. [online]. [cit. 2019-06-04]. Dostupné na: <https://lifelinedatacenters.com/data-center/cyber-attack-scenarios/>, alebo: SCHILLER, J. *Cyber Attacks & Protection: Civilization Depends on Internet & Email*. Baltimore: Create Space Inc., 2010. 204 s.

[17] Bližšie pozri napr.: CAROLL, A. 2017. *Preparing for Worst-Case Scenarios with Cyber Attacks*. [online]. [cit. 2019-06-04]. Dostupné na: <https://lifelinedatacenters.com/data-center/cyber-attack-scenarios/>, alebo: SCHILLER, J.: *Cyber Attacks & Protection: Civilization Depends on Internet & Email*. Baltimore: Create Space Inc., 2010. 204 s.

[18] Bližšie pozri napr.: KORAUŠ, A., DOBROVIČ, J., RAJNOHA, R., BREZINA, I. The safety risks related to bank cards and cyber attacks. In *Journal of Security and Sustainability Issues*, 2017. s. 563-574. KORAUŠ, A., DOBROVIČ, J., KLJUČNIKOV, A., GOMBÁR, M. Customer Approach to Bank Payment Card Security and Fraud. In *Journal of Security and Sustainability Issues*, 2016. s. 85–102.

[19] Bližšie pozri napr.: KUCHTOVÁ, J. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 95-97.

[20] H4H – akronym pre skupiny označované ako Hackers for Hire (Hackeri na prenájom).

[21] Napríklad nedávno opakované kybernetické útoky na servery USA boli spájané s vojenskými aktivitami Číny.

[22] JIROVSKÝ, V. Kyberterorismus – bezpečnostná hrozba 21. storočia. In *EAQ*, roč. 3, č. 4, 2008. s. 9.

V priamej súvislosti s uvedenými formami kyberterorizmu je nutné spomenúť aj tzv. nepriamy kyberterorizmus. Jeho existencia bola donedávna opomínaná aj napriek tomu, že latentnosť je v niektorých prípadoch nebezpečnejšia než priame kybernetické útoky. Do tejto skupiny patrí terorizmus úzko spojený s využívaním komunikačných a informačných technológií bez priameho vzťahu k existujúcej infraštruktúre, ale zviazaný najmä s vývojom informatiky a telekomunikácií. Všeobecne je založený na pocite slobody podporovanej percepciou voľnosti na internete. V tejto súvislosti rozlišujeme:

1. Mediálny terorizmus.
   Niekedy sa tiež zvykne označovať ako psychologický terorizmus, pri ktorom dochádza k zneužívaniu masových oznamovacích prostriedkov (aj internetu) a psychologických prostriedkov v čase mieru za účelom ovplyvnenia názorov celej populácie alebo cielene vybraných skupín obyvateľstva. V tomto prípade sú komunikačné a informačné technológie, systémy a prostriedky zneužité na šírenie ideologického posolstva alebo mediálnej manipulácie, ktorá môže byť doplnená niektorými prostriedkami psychologickej vojny.
2. Procesný terorizmus.
   Využíva výkon výpočtovej techniky k preťažovaniu nastavených demokratických systémov a mechanizmov, čo má za následok ich postupné zahltenie a nefunkčnosť (napr. generovanie veľkého množstva súdnych podaní vedie k znefunkčneniu súdneho systému, enormný počet volaní na záchranné linky vedie k znefunkčneniu záchranného systému, atď.).
3. IT governance.
   Spočíva v prevzatí exekutívneho rozhodovania subjektu IT zložkami daného subjektu (firmy, korporácie, inštitúcie). Závislosť od informačných technológií je možná najmä v takých subjektoch, kde IT ovláda len úzka skupina, ktorej požiadavky sú vrcholovým manažmentom ťažko posúditeľné.

Kybernetická špionáž

Kybernetickú špionáž je možné považovať za akt špionáže alebo špehovania s cieľom získania informácií o plánoch a/alebo činnostiach najmä zahraničnej vlády alebo konkurenčnej spoločnosti (organizácie, skupiny). Slúži predovšetkým ako prostriedok (nástroj) pre ekonomický, politický alebo vojenský zisk.[23] Ide teda o formu počítačovej kriminality, pri ktorej sa hackeri zameriavajú na počítačové siete s cieľom získať prístup k utajovaným, resp. iným citlivým informáciám, ktoré môžu byť pre hackera alebo objednávateľa ziskové alebo výhodné.[24]

Kybernetická špionáž predstavuje akt vykonávaný za účelom získania tajomstva, resp. utajovanej skutočnosti, bez súhlasu majiteľa alebo pôvodného držiteľa takejto informácie. Tieto informácie môžu pochádzať od jednotlivcov, rôznych ekonomických či politických organizácií, skupín alebo od vlád štátov, pričom môžu byť charakteru osobného, senzitívneho alebo oficiálne utajovaného. Záujem o ich získanie môže byť motivovaný z rôznych dôvodov, spravidla však ide najmä o osobné, ekonomické, politické alebo vojenské či bezpečnostné dôvody. Tieto informácie sa získavajú pomocou použitia rôznych metód v sieti internetu alebo cestou využitia jednotlivých počítačových systémov pomocou škodlivého softvéru, vrátane využitia trójskych koňov a/alebo spywarov.

Na páchaní kybernetickej špionáže sa môžu podieľať on-line odborníci vo vzdialených krajinách, alebo priamou infiltráciou domácich zariadení. Môže byť tiež dielom zlomyseľných

[23] CARBON, B. 2018. *What is Cyber Espionage*? [online]. [cit. 2019-06-04]. Dostupné na:<https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/>

[24] Techopedia. 2019. *Cyberspying*. [online]. [cit. 2019-06-04]. Dostupné na:<https://www.techopedia.com/definition/27101/cyberspying>

amatérskych hackerov či programátorov. Spoločným cieľom je prístup k tajomstvu a utajovaným informáciám alebo ovládanie jednotlivých počítačov, resp. celých sietí pre strategickú výhodu a psychologické, politické a fyzické podvratné činnosti a sabotáž.[25] Kybernetická špionáž môže byť aj formou kybernetického útoku zameraného na získanie duševného vlastníctva za účelom získania výhod oproti konkurenčnej spoločnosti (organizácii) alebo vládnemu subjektu.[26]

Kybernetické útoky

Kybernetické útoky v porovnaní s fyzickými teroristickými útokmi[27] predstavujú relatívne nenákladnú a nízkorizikovú aktivitu rôznej podoby, ako napríklad:

a) *modifikácia dát* – typickým príkladom môžu byť rôzne typy vírusov, ktoré po vstupe do počítača náhodne poprehadzujú slovosled v dokumentoch (napríklad šieste slovo z tretieho odseku zo strany päť sa vymení s piatym slovom z posledného odseku na strane desať a pod.), alebo zmenia poradie jednotlivých číslic v číselných údajoch;
b) *šírenie dezinformácií* – kybernetický priestor poskytuje rovnosť a slobodu každému sa vyjadriť a zdieľať informácie. To prináša jednu veľkú výhodu, ale zároveň aj obrovskú nevýhodu, riziko. Jedným z príkladov šírenia dezinformácie je prípad z USA, keď sa vo viacerých médiách objavila správa, že FBI vytvorila špeciálny sledovací softvér, ktorý umiestňuje do počítačov. Na základe toho sa zdvihla obrovská vlna protestu proti takémuto konaniu. Až neskôr sa ukázalo, že išlo o fámu;
c) *elektronická bomba* – ide o program, ktorý vykoná preddefinovanú akciu za určitých vopred naprogramovaných podmienok (stlačenie určenej kombinácie klávesov, dosiahnutie určitého dátumu a pod.). Tento program spôsobí viac či menej závažné škody v jednotlivých dokumentoch, súboroch alebo celých systémoch;
d) *odcudzenie informácií* – nabúraním sa do počítačov alebo informačných systémov, verejných alebo súkromných, môže dôjsť k odcudzeniu osobných, obchodných alebo verejných neutajovaných, ale i utajovaných údajov a informácií. Napríklad zamestnancom istej finančnej inštitúcie začali chodiť e-mailové správy s pripojeným súborom RESUME.TXT.VBS. Ak sa spustil tento súbor, objavila sa seriózne vyzerajúca žiadosť o zamestnanie. Toto bol však len zastierací manéver vírusu, ktorý sa snažil stiahnuť a spustiť súbor obsahujúci údaje o používaných heslách;
e) *vydieranie* – získanie (ukradnutie) osobných či obchodných údajov môže slúžiť na vydieranie konkrétnych osôb alebo inštitúcií. V USA sa napríklad hacker dostal do informačného systému jednej americkej banky a ukradol chránenú databázu informácií o klientoch. Onedlho kontaktoval riaditeľa banky s ponukou výmeny databázy za istú sumu peňazí. Riaditeľ banky túto skutočnosť oznámil polícii a celý prípad bol následne medializovaný. A to bolo pre banku priam likvidačné. Takmer okamžite začala strácať svojich klientov a veľmi dlho jej trvalo, kým si opäť získala ich dôveru;
f) *zaťažovanie komunikačnej infraštruktúry* – systematické preťažovanie alebo zahlcovanie určitého systému môže spôsobiť znefunkčnenie tohto systému. Typickým príkladom je vírus Firkin, zaregistrovaný v USA, ktorý z napadnutých počítačov vytáčal telefónne číslo núdzového volania záchrannej služby. Pokiaľ by sa mu podarilo dosiahnuť masovejšie rozšírenie, mohol ohroziť prevádzku celej záchrannej služby;

[25] PALMER, D. 2019. *Cyber espionage warning: The most advanced hacking groups are getting more ambitious*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.zdnet.com/article/cyber-espionage-warning-the-most-advanced-hacking-groups-are-getting-more-ambitious/>

[26] CARBON, B. 2018. *What is Cyber Espionage*? [online]. [cit. 2019-06-04]. Dostupné na:<https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/>

[27] Fyzické teroristické útoky sú na rozdiel od kybernetických spojené s nákupom a použitím fyzických zbraní a prostriedkov alebo symetrickými útokmi s použitím sofistikovaných zbraňových systémov za státisíce či milióny eur (dolárov).

g) *počítače vo vojne* – kyberpriestor možno s vysokou pravdepodobnosťou označiť za jedno z rozhodujúcich bojísk v budúcich konfliktoch. Napríklad taiwanská vláda priznáva, že vlastní arzenál agresívnych vírusov, ktoré sú v prípade potreby schopné napadnúť čínske ciele. Oficiálne to priznal vysoký úradník na oddelení informatiky taiwanského ministerstva obrany. Konštatoval, že budú použité ako regulárne zbrane v okamihu, keby Čína zaútočila ako prvá.[28]

Kybernetická kriminalita

Objem kriminálnych aktivít v kyberpriestore, podobne ako objem škôd spôsobených týmito nelegálnymi aktivitami, každým rokom rastie. Príčinu možno vidieť v zníženej možnosti odhalenia a následného potrestania páchateľov. Populácia v kyberpriestore je totiž reprezentovaná virtuálnymi osobnosťami, ktoré sú projekciou reálnych osobností v ňom. Tieto populácie vytvárajú virtuálne komunity, ktoré je možné chápať ako globálne zoskupenie virtuálnych osobností spojených spoločnými myšlienkami, vierou, politickým názorom, skúsenosťami a záujmami bez obmedzení hranicami štátov. Medzi objekty kyberpriestoru patria tiež virtuálne korporácie tvorené subjektmi zameranými na rovnaký tržný segment.[29]

Preto je možné skonštatovať, že kybernetická kriminalita predstavuje prenos kriminálnych aktivít do kyberpriestoru, mnohokrát s vylepšeniami, ktoré umožňujú najnovšie moderné technológie, i nové trestné činy. Podľa medzinárodnej dohody o kybernetickej kriminalite z roku 2001[30] možno definovať deväť druhov trestných činov, ktoré sa delia do ďalších štyroch kategórií:

1. *Trestné činy proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov*. Tieto zahŕňajú:
   a) neoprávnený prístup k systému,
   b) neoprávnené zachytenie informácií,
   c) neoprávnený zásah do údajov,
   d) neoprávnený zásah do systému,
   e) zneužitie zariadení.
2. *Trestné činy súvisiace s počítačmi*, ktoré zahŕňajú:
   a) falšovanie údajov súvisiacich s počítačmi,
   b) podvody súvisiace s počítačmi.
3. *Trestné činy súvisiace s obsahom*, ako napríklad trestné činy súvisiace s detskou pornografiou.
4. *Trestné činy súvisiace s porušením autorského práva a práv príbuzných autorskému právu*.

V roku 2003 bol k tomuto dokumentu vyhotovený dodatkový protokol týkajúci sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov. V podstate šlo o rozšírenie skupín trestných činov o nasledovné:

- rozširovanie rasistických a xenofóbnych materiálov prostredníctvom počítačových systémov,
- rasisticky a xenofóbne motivované vyhrážanie,
- rasistické a xenofóbne motivované útoky,

[28] VRBŇÁK, I. 2010. *Kyberterorizmus.* [online]. [cit. 2019-06-04]. Dostupné na: <http://edi.fmph.uniba.sk/Social ne Aspekty/.html>

[29] FOLTZ, B. C. 2004. *Cyberterrorism, computer crime, and reality*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.emeraldinsight.com/doi/abs/10.1108/09685220410530799>

[30] Dohovor Rady Európskej únie o počítačovej kriminalite bol prijatý v Budapešti 23. novembra 2001 po štvorročnej práci expertov Rady Európy, USA, Kanady, Japonska a ďalších krajín. Slovenská republika ho podpísala 4. februára 2005, ratifikovala 8. januára 2008 a v platnosti je od 1. mája 2008.

- popieranie, znižovanie, schvaľovanie alebo ospravedlňovanie genocídia alebo zločinov proti ľudskosti.

Z tohto pohľadu dokument upravil skupiny trestných činov, v rámci ktorých zaviedol prvú klasifikáciu počítačovej/kybernetickej trestnej činnosti v rámci určitého právneho predpisu.[31]

Vyšetrovanie a postih kybernetickej kriminality predstavujú stále veľký problém, pretože nové alebo modifikované spôsoby zneužívania kybernetického priestoru vyžadujú aj vytvorenie nových, príp. úpravu súčasne platných inštitútov, ktoré umožnia odhaliť páchateľa a zároveň zaistiť dôkazy, ktoré vedú k jeho usvedčeniu. Problém, spojený s týmto typom kriminality, spočíva jednak v nižšej erudovanosti sudcov, prokurátorov a vyšetrovateľov, jednak v nedokonalosti právnych inštitútov. Mnohé ustanovenia totiž nemajú oporu v trestnom poriadku, napríklad chýba pojem, definícia a závažnosť tzv. elektronického (digitálneho) dôkazu. S ohľadom na rýchly technologický rozvoj a sofistikovanosť páchateľov pri osvojení si nových spôsobov porušovania zákonom chránených záujmov je možné v blízkej budúcnosti predpokladať vznik ďalších medzinárodných dokumentov upravujúcich predmetnú oblasť. Avšak ani legislatívna pripravenosť spoločnosti nezabezpečuje následnú schopnosť implementácie legislatívy represívnymi a justičnými zložkami a najmä nezabezpečuje spoluprácu s ostatnými štátmi.[32]

Problém vyšetrovania a postihu kybernetickej kriminality nie je len problémom regionálnym, ale celosvetovým. Zásadný obrat by prinieslo predovšetkým kvalitné vyšetrovanie a fungovanie orgánov činných v trestnom konaní. Samotné predloženie elektronického (digitálneho) dôkazu je ale často problematické a značne zložité, pretože v mnohých prípadoch neexistuje v „čitateľnej“ alebo „hmotnej“ podobe. Bez včasného zaistenia dostatočného množstva dôkazov a veľmi rýchlej spolupráce orgánov činných v trestnom konaní so súdnymi znalcami a špecialistami je potom prakticky skoro nemožné odhaliť páchateľa.

Zavedenie tzv. „best evidence rule“ v USA síce pripúšťa, že výtlačok elektronického dokumentu a jeho pôvodná elektronická podoba sú pre účely súdneho riadenia totožné, napriek tomu vzniká množstvo problémov, pretože strata informácie obsiahnutej v elektronickom dokumente pri jeho vytlačení môže byť veľmi podstatná (napr. v najjednoduchšom prípade sa môžu stratiť tzv. hyperlinky) a môže zmariť celé vynaložené úsilie na usvedčenie a postihnutie páchateľa. O nič lepšie na tom nie sú ani európske inštitúcie, zvlášť s ohľadom na rozdielne ponímanie práva v jednotlivých členských krajinách Európskej únie. Kyberpriestor totiž nemá hranice a tak napríklad len určenie miesta, rozhodného pre uplatnenie príslušného práva je problém, ktorý nie je dosiaľ právne celkom doriešený, i keď k nemu bolo vydaných viacero rámcových rozhodnutí a smerníc Európskeho parlamentu a Rady Európy. Za doteraz najvýznamnejší krok v legislatíve Európskej únie v oblasti kybernetickej bezpečnosti možno považovať schválenie Smernice Európskeho parlamentu a Rady EÚ 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Smernica NIS).[33]

Slovenská republika v rámci postupných krokov smerujúcich k budovaniu bezpečnosti kybernetického prostredia prijala Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý

[31] MARKOVÁ, V. Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 111.

[32] KURILOVSKÝ, R. Vyšetrovanie počítačovej kriminality. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie*. Bratislava: APZ, 2018. s. 170.

[33] Táto smernica vytvára uniformný prístup ku kybernetickej bezpečnosti na najvyššej úrovni členských štátov a prináša jednoznačné práva a povinnosti subjektov v rámci tejto problematiky. Bližšie pozri: ŠIŠULÁK, S., ŠALMÍK, M. Smernica NIS a dopad jej transpozície v policajnom prostredí. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie*. Bratislava: APZ, 2018. s. 392-398.

nadobudol účinnosť dňa 01. 04. 2018. Aj keď zákon nesporne vytvoril základ systémového prístupu na úrovni štátu k riešeniu problematiky kybernetickej bezpečnosti, bude v tomto smere ešte potrebné realizovať množstvo ďalších súvisiacich krokov. Niektoré takéto kroky už boli definované v Koncepcii kybernetickej bezpečnosti a v Akčnom pláne realizácie koncepcie kybernetickej bezpečnosti na roky 2015 – 2016.[34]

Kybernetické vojny

Pri výpočte kybernetických hrozieb nemožno vynechať hrozbu kybernetických vojen, ktoré sú definované ako aktivity vedené alebo koordinované štátom s cieľom získať informačnú prevahu alebo vyradiť technologickú infraštruktúru protivníka. Neoddeliteľnou súčasťou kybernetickej vojny je informačná vojna, ktorú možno tiež chápať ako vojnu o informácie alebo ako boj, ktorý prebieha medzi ľuďmi pracujúcimi s informáciami, príp. stret, kde hlavnou zbraňou sú práve informácie – predovšetkým ich kvalita, presnosť, hodnovernosť a dostupnosť, ich cielené pozdržanie pred nepriateľskou stranou alebo cielená dezinformácia nepriateľskej strany.[35]

V súčasnosti už celý rad štátov veľmi intenzívne pracuje na koncepte informačnej vojny. V prípade tzv. zločinných štátov pritom hrá kľúčovú úlohu zistenie, že ich sily by len ťažko mohli uspieť v klasickom konvenčnom vojenskom konflikte s najvyspelejšími štátmi sveta. Preto svoje strategické aktivity zameriavajú predovšetkým smerom k možnostiam boja v kyberpriestore. Informačná vojna totiž predstavuje boj, ktorý je veľmi špecifický a v podstate personálne a materiálne relatívne nenáročný.

Často sa vyzdvihuje jej asymetrická povaha, pretože nezistený alebo prekvapivý útok môže podkopať obranyschopnosť značne silnejšieho a „bohatšieho“ protivníka a spôsobiť škody mnohonásobne väčšie, než boli náklady na jeho vykonanie. Kybernetické vojny prinášajú so sebou nový názov vojnového arzenálu – tzv. infoware. Pod týmto termínom sa rozumie súhrn všetkých bojových prostriedkov zameraných na zničenie komunikačnej, informačnej alebo elektronickej infraštruktúry protivníka a informačných prostriedkov potrebných na vedenie kybernetického boja.[36]

Na základe aktuálneho vývoja v tejto oblasti je možné skonštatovať, že zbrane kybernetickej vojny sú zaradené do arzenálov viacerých štátov (i skupín) a pripravené na použitie. Súčasná kybernetická vojna je vedená prostredníctvom počítačov a môže na seba previať veľa rôznych foriem – od odpočúvania alebo narušenia komunikačných a informačných sietí, cez rušenie televízneho a rádiového vysielania, šírenie dezinformačných kampaní cez „ukradnuté“ rádiové a televízne frekvencie, narušenie logistických sietí, prerušenie finančných tokov až po sabotáže produktovodov alebo rozvodných sietí elektrickej energie.

Kybernetická vojna už v žiadnom prípade nie je iba science-fiction, ale existujúcim, reálnym ohrozením, ktorého závažnosť stále stúpa s postupným prechodom do éry znalostnej spoločnosti. Zatiaľ si túto asymetrickú hrozbu väčšina populácie neuvedomuje v takej miere ako napríklad fyzický terorizmus alebo obmedzený prístup k energetickým zdrojom a má snahu tento vážny problém bagatelizovať. Zraniteľnosť modernej spoločnosti, stále viac odkázanej na elektronickú komunikáciu a využívanie komunikačných a informačných technológií, systémov a prostriedkov, je však veľmi vysoká.

---

[34] BRVNIŠŤAN, M. Kybernetická kriminalita a možnosti prevencie. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 26.

[35] CLARKE, R., A., KNAKE, R., K. *Cyber war: The Next Threat to National Security and what to do about it*. New York: Harper Collins, 2010. s. 22.

[36] JIROVSKÝ, V. Kyberterorismus – bezpečnostná hrozba 21. storočia. In *EAQ*, roč. 3, č. 4, 2008. s. 8.

Záver

Kybernetické hrozby sa pod vplyvom kontinuálne sa zhoršujúceho globálneho bezpečnostného prostredia a bezpečnostnej situácie vo viacerých regiónoch sveta stali v posledných rokoch jednou z najviac diskutovaných tém súvisiacich s bezpečnosťou štátov. Zaistenie bezpečnosti je totiž považované za jednu zo základných funkcií štátu. Rozdiel oproti minulosti, t. j. obdobiu spred pár desiatok rokov, spočíva v tom, že vďaka technickým a technologickým vymoženostiam v kyberpriestore sa už netýka iba najrozvinutejších, ekonomicky silných štátov, ale jeho rozmach možno pozorovať takmer vo všetkých štátoch sveta bez ohľadu na výšku priemernej životnej úrovne v nich. Vďaka globálnej previazanosti sa všetci aktéri stávajú súčasťou jedného globálneho informačného systému, do ktorého existuje nespočetné množstvo prístupov bez geografického obmedzenia. Participujúci aktéri, či už v podobe štátov, nadnárodných korporácií, verejných inštitúcií a organizácií alebo súkromných entít, sa tak stávajú nielen previazanejší, ale aj závislejší a omnoho zraniteľnejší.

Kybernetické útoky na vládne a súkromné informačné siete a servery vo viacerých krajinách (napr. v Estónsku, USA alebo v Gruzínsku, atď.) potvrdili reálnosť existencie nebezpečenstva kybernetických hrozieb bez ohľadu na to, či si to niekde alebo niekto uvedomuje viac alebo menej. Tieto útoky dokazujú, že štáty ako základné entity post-vestfálskeho medzinárodného systému čelia novému druhu asymetrických bezpečnostných hrozieb v meniacom sa globálnom i regionálnom bezpečnostnom prostredí. Vzhľadom na dynamický vývoj v sektore komunikačných a informačných technológií, systémov a prostriedkov je vysoko pravdepodobné, že sa tieto typy útokov budú v blízkej dobe s najväčšou pravdepodobnosťou iba rozširovať a kybernetické hrozby sa dostanú na čelo pomyselného rebríčka asymetrických bezpečnostných hrozieb.

Stále sa rozširujúce nástroje pre webové prezentácie zároveň vedú k väčšiemu množstvu slabín a nedostatkov na týchto stránkach. Napadnutie webových stránok alebo informačných sietí, súkromných alebo verejných, či už zo strany kyberteroristov šíriacich strach a svoju ideológiu, alebo zo strany hackerov – jednotlivcov, resp. hackerských skupín sledujúcich vlastné konkrétne záujmy (slávu, peniaze alebo likvidáciu konkurencie), príp. prenajatých hackerov v rôznych službách, pravdepodobne povedie k ďalšiemu rozvoju útočných aktivít v tejto oblasti. Predpokladá sa, že priame útoky na e-maily budú mať, vzhľadom na vzrastajúcu úroveň užívateľov, postupne nižšiu účinnosť a útočníci prejdú na iné sofistikovanejšie postupy. Naopak možno však očakávať nárast počítačového pirátstva, priemyselnej a ekonomickej špionáže, zvýšený počet pokusov o získanie osobných údajov jednotlivcov či dokonca ukradnutie celej identity, ako aj zvýšený počet priamych premyslených útokov na servery a virtuálne systémy bánk, poisťovní a veľkých korporácií, vrátane vládnych inštitúcií a ich ozbrojených a bezpečnostných zložiek.

Na záver je potrebné zdôrazniť, že kyberpriestor nemá hranice. Predstavuje nové bojisko, ktoré sa vyznačuje viacerými jedinečnými prvkami. Počítače a ich klávesnice sa stali zbraňami, komunikačné a informačné technológie, systémy a prostriedky predstavujú zbraňové systémy a kybernetickí bojovníci využívajú namiesto klasických konvenčných zbraní v boji softvér a hardvér. Kybernetickí útočníci sú zväčša skrytí, anonymní oproti útočníkom v klasickom konvenčnom boji, nehovoriac o nulovom riskovaní života v porovnaní s reálnym bojiskom, avšak výsledky ich relatívne nenákladných a nízkorizikových aktivít sú prekvapivo efektívne a ničivé. Vyvstáva tak dokonca možnosť, že budúce konflikty stratia svoj konvenčný rozmer a stanú sa nekonvenčnými vojnami, v ktorých jednotlivé strany konfliktu nebudú musieť vôbec použiť klasickú konvenčnú vojenskú taktiku alebo fyzické letálne zbrane. Naopak, je možné, že k likvidácii protivníka (štátu, koalície) bude stačiť vysoko špecializovaná skupina, ktorá vykoná niekoľko kybernetických útokov na kritickú infraštruktúru daného protivníka. Výsledkom bude destabilizácia, chaos a likvidácia protivníka (štátu, koalície) zvnútra a jeho neschopnosť adekvátnej odpovede. Preto tlak na vytváranie čo najbezpečnejších

informačných sietí a rozvoj metód, postupov, prostriedkov a zariadení obrany, ochrany a bezpečnosti kyberpriestoru v budúcnosti ešte viac vzrastie a dostane sa na jedno z popredných miest v ďalšom vývoji komunikačných a informačných technológií, systémov a prostriedkov. Rovnako tak vzrastie význam informačnej a kybernetickej bezpečnosti štátu, spoločnosti i jednotlivca.

Zoznam použitej literatúry:

1. ANDRASSY, V., GREGA, M. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, roč. 5, č. 2, 2015. s. 11-18. ISSN 1338-4880.
2. BARIČIČOVÁ, Ľ. *Kompetencie policajných manažérov*. Bratislava: APZ, 2011, 2011. 160 s. ISBN 978-80-8054-514-7.
3. BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 8-15. ISBN 978-80-8054-773-8.
4. BAYLIS, J., International and Global Security in the Post-Cold War Era. In Baylis, J., SMITH, S. *The Globalization of World Politics: An Introduction to International Relations*. Oxford: University Press, s. 302-305, 2005. ISBN 978-01-9956-909-0.
5. BOTTESINI, B. J. Medzinárodná kooperácia v boji proti kyberterorizmu. In *EAQ*, roč. 3, č. 4, 2008. s. 10-11. ISSN 1336-8761.
6. BREZULA, J. Vývoj kybernetickej bezpečnosti vzhľadom na nové hrozby v súčasnosti. In *Tradície a dynamika vývoja manažmentu a informatiky z pohľadu univerzít s bezpečnostným zameraním. Zborník príspevkov*. Bratislava: APZ, 2018. s. 143-151. ISBN 978-80-8054-767-7.
7. BRVNIŠŤAN, M. Kybernetická kriminalita a možnosti prevencie. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 26-37. ISBN 978-80-8054-773-8.
8. CARBON, B. 2018. *What is Cyber Espionage*? [online]. [cit. 2019-06-04]. Dostupné na: <https://www.carbonblack.com/ resources/definitions/what-is-cyber-espionage/>
9. CAROLL, A. 2017. *Preparing for Worst-Case Scenarios with Cyber Attacks*. [online]. [cit. 2019-06-04]. Dostupné na: <https://lifelinedatacenters.com/data-center/cyber-attack-scenarios/>
10. CLARKE, R., A., KNAKE, R., K. *Cyber war: The Next Threat to National Security and what to do about it*. New York : Harper Collins, 2010. 320 s. ISBN 978-0-06199-239-1.
11. DENNING, D., E. 2000. *Cyberterrorism*. [online]. [cit. 2019-06-04]. Dostupné na: <http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>
12. DENNING, D., E. 2006. *Activism, Hacktivism and Cyberterorism: The Internet as a Tool for Influencing Foreign Policy*. [online]. [cit. 2019-06-04]. Dostupné na: <http: //www:nautilus.org/info-policy/workshop/papers/ denning.html>
13. FOLTZ, B., C. 2004. *Cyberterrorism, computer crime, and reality*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.emeraldinsight.com/doi/abs/10.1108/09685220410530799>
14. JANCZEWSKI, L., COLARIK, A., M. *Managerial Guide for Handling Cyberterrorism and Information Warfare*. Idea Group Inc., 2005. 229 s. ISBN 978-1-59140-550-4.
15. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, 2007. 284 s. ISBN 978-80-247-1561-2.
16. JIROVSKÝ, V. Kyberterorismus – bezpečnostná hrozba 21. storočia. In *EAQ*, roč. 3, č. 4, 2008. s. 8-9. ISSN 1336-8761.

17. JURČÁK, V. Asymetrické hrozby v bezpečnostnom prostredí 21. storočia. In *Bezpečnostné fórum 2013 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Fakulta politických vied a medzinárodných vzťahov Univerzity Mateja Bela, 2013. s. 614-623. ISBN 978-80-557-0497-5.
18. KAZANSKÝ, R. *Bezpečnostná politika IV. – Teória konfliktov*. Banská Bystrica : Fakulta politických vied a medzinárodných vzťahov Univerzity Mateja Bela, 2011. 115 s. ISBN 978-80-557-0250-6.
19. KORAUŠ, A., DOBROVIČ, J., KLJUČNIKOV, A., GOMBÁR, M. Customer Approach to Bank Payment Card Security and Fraud. In *Journal of Security and Sustainability Issues*, 2016, roč. 6 (1), 2016. s. 85–102. ISSN 2029-7017.
20. KORAUŠ, A., DOBROVIČ, J., RAJNOHA, R., BREZINA, I. The safety risks related to bank cards and cyber attacks. In *Journal of Security and Sustainability Issues*, roč. 6 (4), 2017. s. 563-574. ISSN 2029-7017.
21. KREMMER, J., F., MÜLLER, B. *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin : Springer Science & Business Media, 2013. 284 s. ISBN 978-3-642-37481-4.
22. KUCHTOVÁ, J. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie*. Bratislava: APZ, 2018. s. 90-98. ISBN 978-80-8054-773-8.
23. KURILOVSKÝ, R. Vyšetrovanie počítačovej kriminality. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie*. Bratislava: APZ, 2018. s. 162-171. ISBN 978-80-8054-751-6.
24. MARKOVÁ, V. Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky. In *Aktuálne výzvy prevencie počítačovej kriminality*. Zborník príspevkov z vedeckej konferencie. Bratislava: APZ, 2018. s. 106-126. ISBN 978-80-8054-773-8.
25. PALMER, D. 2019. *Cyber espionage warning: The most advanced hacking groups are getting more ambitious*. Dostupné na: <https://www.zdnet.com/article/cyber-espionage-warning-the-most-advanced-hacking-groups-are-getting-more-ambitious/>
26. PATEL, D. R. *Information Security: Theory and Practice*. New Delhi: PHI Learning Pvt. Ltd., 2008. 312 s. ISBN 978-81-203-3351-2.
27. PŘIBYL, T. 2008. *Kyberterorizmus.* [online]. [cit. 2019-06-04]. Dostupné na: <http://www.virusy.sk/ clanok.ltc? ID=402.html>
28. RATTRAY, G., J. *Strategic Warfare in Cyberspace*. Cambridge, Massachussetts : Massachusetts Institute of Technology Press, 2001. 517 s. ISBN 978-0-26218-209-6.
29. SCHILLER, J. *Cyber Attacks & Protection: Civilization Depends on Internet & Email*. Baltimore: Create Space Inc., 2010. 204 s. ISBN 978-1-45360-913-2.
30. ŠIŠULÁK, S., ŠALMÍK, M. Smernica NIS a dopad jej transpozície v policajnom prostredí. In *Polícia ako garant bezpečnosti. Zborník z medzinárodnej vedeckej konferencie.* Bratislava: APZ, 2018. s. 392-402. ISBN 978-80-8054-751-6.
31. TECHOPEDIA. 2019. *Cyberspying*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.techopedia. com/definition/27101/cyberspying>
32. THORTON, R. *Asymmetric Warfare: Threat and Response in the 21st Century.* Cambridge: Polity Press. 2007. 256 s. ISBN 978-0-7456-3365-7.
33. VRBŇÁK, I. 2010. *Kyberterorizmus.* [online]. [cit. 2019-06-04]. Dostupné na: <http://edi.fmph.uniba.sk/ Socialne Aspekty/.html>
34. WEBSTER, F. *Theories of the Information Society*. New York : Routledge, 2002. 304 s. ISBN 978-0-41528-201-7.

Kontaktné údaje:
plk. gšt. v. z. Ing. Radoslav Ivančík, PhD. et PhD.
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
radoslav.ivancik@minv.sk

plk. doc. Ing. Ľubica Baričičová, PhD.
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
lubica.baricicova@minv.sk

Podvod – jedno z najväčších bezpečnostných rizík

Antonín Korauš, Stanislav Backa, Matej Bárta

Abstrakt:
Objem investícií do kontrolných systémov stúpa. Profesia špecialistov na boj s podvodmi je jedna z najžiadanejších, do praxe sú schvaľované a zavádzané nové regulácie a zákony, ale podvody neklesajú. Skôr naopak. Nielen počet postihnutých organizácií, variabilita schém, ale aj miera škôd je alarmujúca. Príčinami podvodov môžu byť schopnosti podvodníkov, nové technológie, sociálna situácia v spoločnosti, neefektívne systémy riadenia rizika podvodov, prípadne ďalšie.
Kľúčové slová:
Úver, úverový podvod, riziková skupina úverových podvodov, prevencia úverových podvodov, schémy podvodov.

Abstract:
The volume of investment in control systems is rising. The profession of anti-fraud specialists is one of the most demanding, new regulations and laws are being adopted and implemented, but fraud is not falling. On the contrary. Not only the number of affected organizations, the variability of schemes, but also the degree of damage is alarming. The causes of fraud can be the ability of fraudsters, new technologies, the social situation in society, ineffective fraud risk management systems, and possibly others.
Key words:
Credit, credit fraud, credit fraud risk group, credit fraud prevention, fraud schemes.

Úvod

Každá z činností vo fungujúcej organizácii, aj riadenie rizika podvodov bude vždy obmedzené dostupným rozpočtom. Vytvorenie perfektného a nepreniknuteľného kontrolného systému je nemožné. Bolo by príliš nákladné, vyžadovalo by skúsených, motivovaných a vyškolených zamestnancov, a vždy by bolo vystavené novým útokom prefíkaných podvodníkov. Efektívny kontrolný systém bude preto vždy zamedzovať výskytu najvýznamnejších, najčastejších a najškodlivejších podvodných schém a bude zavedený na ochranu kľúčových funkcií v organizácii.[1]

Zmeny v technickej oblasti, predovšetkým v oblasti informačných a komunikačných technológií kvalitatívne zmenili proces získavania, spracovávania a uchovávania informácií[2].

Napriek zavedeniu audítorských štandardov, ako sú ISA 240, alebo SAS 99, ktoré stanovujú postupy a zodpovednosť audítorov posudzovať výskyt podvodov v účtovníctve organizácie, primárna úloha finančného audítora nie je identifikovať a vyšetrovať podvody. Organizácie sa často zastrešujú audítorskou správou, ako dôkazom o neexistencii podvodov. Aj kvôli tejto mylnej predstave, možno že práve ich spoločnosť sa v tom čase rúti do záhuby kvôli výskytu skrytého nekalého konania. Stačí sa pozrieť na najväčšie finančné škandály posledných desiatich rokov a nájdu sa desiatky prípadov postihnutých firiem. Väčšina z nich bola auditovaná významnými globálnymi audítorskými spoločnosťami.[3]

Riziková skupina úverových podvodov

Za svoje konanie musí každý niesť zodpovednosť. Nie je tomu inak v prípade rizikových dlžníkov. Občas býva na vinne okrem precenenia vlastných finančných síl tiež

[1] KORAUŠ, A., VESELOVSKÁ, S., KELEMEN, P. Cyber security as part of the business environment. In *Zborník z konferencie Medzinárodné vzťahy: Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice 30. novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 2017. 1113 s.

[2] IVANČÍK, R., KAZANSKÝ, R. Kybernetická vojna, útoky a terorizmus. In *Bezpečnostné fórum*, Zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016. s. 11-18.

[3] MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. *Economic freedom – classification of its level and impact on the economic security.* AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157.

samotná nedbalosť, niekedy i zámer klienta vziať si úver aj napriek tomu, že si je vedomý svojej zlej finančnej situácie, a alebo vedomý, že úver splácať nebude.

Tí ľudia, ktorí si neuvážene zaobstarajú či už bezúčelový alebo účelový úver a nemajú dostatok peňazí na splátky a uzatvárajú ďalšie úverové zmluvy preto, aby mali peniaze na splatenie toho prvého úveru, a alebo tí, ktorí úver uzatvoria už s úmyslom ho neplatiť patria do rizikovej skupiny. Týka sa to najmä ľudí:

- Vo veku od 18-45 rokov, s nižšími alebo minimálnymi príjmami a tí, ktorí vďaka poskytovanému úveru získajú peniaze okamžite, avšak obratom ich minú za niečo bezcenného alebo za jedlo, oblečenie, elektroniku. Keď zistia, že nemajú peniaze ani na splátky, ani na živobytie, tak takto získané veci predávajú v bazároch za podstatne nižšiu cenu, avšak ich dlh to ani zďaleka nepokryje.
- Ľudia s nižším stupňov vzdelania, ktorí majú len základné vzdelanie alebo sú vyučení, nedokážu, a mnohokrát ani nechcú objektívne posúdiť danú situáciu, následkom čoho ju podcenia a myslia si, že budú schopní úver splácať, ale realita je iná. Výška a pravidelnosť splátok ich viac a viac zaťažuje.
- Ľudia vedení na úradoch práce a ľudia bez pracovného pomeru, t.j. ľudia s minimálnym príjmom, či úplne bez príjmu. Tento typ ľudí zväčša uzatvára úverové zmluvy s cieľom získania peňažných prostriedkov v hotovosti.
- Ľudia pochádzajúci zo slabého sociálneho prostredia, t.j. z rodín so zlým výchovným vzorom, kde rodinní príslušníci nepracujú a poberajú pravidelné sociálne dávky, alebo podporu v nezamestnanosti a sú s takýmto štýlom života spokojní. Tento výchovný vzor vedie k životu bez motivácie získať peniaze. Vziať si úver, pôžičku a čakať na dávky od štátu je predsa len jednoduchšia a v ich ponímaní normálna cesta.
- Ľudia s trestnou minulosťou, resp. i ľudia, ktorí boli v minulosti vyšetrovaní, trestaní. Tento typ človeka si len veľmi ťažko hľadá prácu a preto sa uchýli k tomu, že si peniaze opatrí iným ako bežným spôsobom.
  Celkovo sú to ľudia s nízkou finančnou gramotnosťou.

Prevencia úverových podvodov

Prevencia je menej nákladná ako neskoršia liečba, čo v prípade bankových inštitúcií platí dvojnásobne. Bankové, ale aj nebankové inštitúcie majú k dispozícii celý rad inštrumentov a databáz, ktoré im každodenne pomáhajú pri prevencii a riadení rizík spojených s poskytovaním úverov. S vývojom informačných technológií prichádzajú aj nové možnosti páchania trestných činov a to nielen úverových podvodov, ale aj ostatných majetkových podvodov.

Prevencia a detekcia úverového podvodu hrá dôležitú úlohu pri jeho riadení. Prevencia znamená sťažiť alebo zamedziť podvodníkovi jeho pokus o podvod, zabrániť, aby k úverovému podvodu došlo. Detekcia naopak znamená zachytiť a odhaliť úverový podvod ak k nemu dôjde. Tieto dva procesy sa teda navzájom dopĺňajú. Obidva procesy sa tiež odohrávajú v inom časovom horizonte. Problémom u úverových podvodov, s ktorými sa stretávajú bankové inštitúcie je ten, že nie sú ľahko odhaliteľné a trvá dlhšiu dobu, než sú detekované. Banky, ktoré sa spoliehajú na detekciu viac než na prevenciu ťažšie odhalia, že sú obeťou podvodu dlhodobého charakteru ako banky, ktoré majú správne nastavenú preventívnu politiku spolu s kontrolnými mechanizmami so zabránením podvodu alebo jeho odhalením v jeho začiatkoch.

Pracovníci bánk, ktorí dojednávajú úvery prídu do styku s rôznorodým segmentom klientov. Preverujú ich identitu, schopnosť vstupovať do záväzku resp. spôsobilosť na právne úkony a ich úverovú kapacitu. Základným nástrojom pre minimalizáciu aktívneho úverového rizika je zistenie bonity klienta, t.j. schopnosť poskytnutý úver splatiť v stanovom termíne. Riziko banka eliminuje tým, že úver poskytne len tým, ktorí budú mať dostatočne vysokú

bonitu. Medzi tradičné metódy merania úverového rizika slúži scoring, rating a kvalifikovaný odhad.

Banky zamestnávajú množstvo zamestnancov na rôznych pozíciách, s rôznymi zodpovednosťami a právomocami. Stále sa však vyskytujú pokusy o vylákanie peňažných prostriedkov z bánk, kde páchateľovi alebo páchateľom z vonkajšieho prostredia napomáha priamo zamestnanec banky. Preto jednou z veľkých a dôležitých oblastí prevencie podvodov je i nastavenie určitých (etických) noriem na pracovisku, ktoré formuluje vedenie spoločnosti. Zamestnanci naprieč úrovňami riadenia musia vedieť, že vedenie spoločnosti berie program prevencie podvodov vážne a musia si byť tiež vedomí čo sa stane, keď takéto pravidlá niekto poruší. Dôležitým predpokladom pre fungovanie tohto systému je i komunikácia a to primerane frekventovaná komunikácia najmä na vertikálnej úrovni. To zamestnancom dáva istú miery sebaistoty v prípade, keď na podobný problém narazia pri pracovnej činnosti, motivuje ich to zachovať sa správnym spôsobom a celú vec vyriešiť.

Jeden zo spôsobov prevencie je i špecializovaný softvér, ktorý dáva bankám možnosť odhaľovať vďaka modernej výpočtovej technike podvodné žiadosti o úver, odhaľovať pranie špinavých peňazí či odhaľovať podvody so zneužitím bežných účtov klientov pomocou elektronického bankovníctva. Svoje využitie tiež nájde u nebankových finančných inštitúcií práve v systémoch na schvaľovanie úverov.

Príslušný softvér musí spĺňať nasledujúce požiadavky: (Kalabis 2009[4])

- Je schopný sledovať a identifikovať podľa vopred delfínových parametrov podozrivé machinácie klientov a nimi vykonávaných obchodov.
- Musí byť schopný odovzdávať všetky podstatné informácie o podozrivých klientoch a obchodoch príslušným bankovým pracovníkom.
- Mal by pomáhať pri predvídaní podvodného konania alebo iné nezákonné aktivity nielen klientov bánk, ale tiež ich vlastných zamestnancov.

Najznámejšie schémy podvodov

Väčšina podvodov je v súčasnosti založená na dvoch schémach a to: Ponziho schéma a Pyramídová hra. V stručnosti vysvetlíme základné charakteristiky týchto schém a princíp, na ktorom sú založené. Často sa tieto schémy zamieňajú, a preto je dôležité zdôrazniť rozdiel medzi nimi.

Ponziho schéma

Charles Ponzi je autorom schémy, ktorá bola pomenovaná po ňom ako Ponziho schéma. Táto schéma označuje podvodné investičné operácie, v ktorých výnosy nie sú vytvorené skutočnými finančnými operáciami, naopak sú vyplatené z vkladov neskorších investorov.

Charles Ponzi vytvoril jednoduchý plán. Spočíval v tom, že prijímal vklady hotovosti a emitované príjmy vkladateľov, ktorým sľúbil 50% podiel v priebehu troch mesiacov. Hotovosť sa mala používať na nákup medzinárodných poštových kupónov, ktoré väčšina národov vydávala od roku 1907. Tieto kupóny boli nakupované v európskych krajinách, ktorých meny vo veľkom fluktuovali v povojnovom kolobehu deflácie a inflácie. Ale boli posielané do USA, kde bola pošta povinná ich obchodovať s plnou nominálnou hodnotou amerických známok, ktoré následne Ponzi predával firmám s 10% zľavou. Táto schéma krachuje keď prestanú pribúdať ďalší investori (Zuckoff, 2006)[5].

V skutočnosti to vyzerá nasledovne:

1. Páchateľ zláka investora A na sľuby vysokých úrokov.
2. Nový investor B vkladá do systému svoje peniaze.

[4] KALABIS, Z. *Boj bank proti praniu špinavých peňazí.* BIVŠ, 2009. s. 78.

[5] ZUCKOFF, M. *Ponzi's Scheme: The True Story of a Financial Legend, Random House Publishing Group*, 2006. 390 s.

3. Investor A obdrží sľubované výnosy, ktoré ale v skutočnosti tvoria vklad investora B. Páchateľ v tomto kroku rozmýšľa ako prísť k väčším peniazom a skúša minimalizovať výbery peňazí ponukou nových akcií s ešte väčšími výnosmi na dlhšie obdobie.
4. Investor A sa chváli ziskom a šíri svoje pocity medzi ďalšími potenciálnymi investormi Zuckoff, 2005).

Príkladom Ponziho schémy môže byť v podstate každá finančná bublina. Keď sa pozrieme na súčasnú situáciu vo svete, je možné si všimnúť ako sa štáty zadlžujú a veria tomu, že sa vždy nájde niekto, kto im požičia. Centrálne banky zvyšujú svoju monetárnu bázu a veria, že ich činy nebudú mať vplyv na meny. Spotrebitelia sa taktiež zadlžujú a veria, že im banka vždy požičia a oni si udržia svoju prácu, aby mohli úvery splácať. Banky naopak dôverujú tomu, že ich klienti sa nedostanú do finančných problémov a úvery dokážu na čas splatiť. Investori vedia, že akcie a komodity sú nadhodnotené, ale stále ich slepo kupujú, lebo veria, že sa vždy nájde niekto, kto ich kúpi za viac.

Aj v tomto prípade existujú tzv. „red flags“. Podľa SEC - U.S.Security and Exchange Commission sú nimi nasledovné[6]:

- Vysoká návratnosť investícií s malým alebo žiadnym riskom

Vo všeobecnosti platí, že investície s vyšším výnosom zvyčajne predstavujú aj vyššie riziko. Je preto potrebné byť viac podozrievavý a opatrný v prípade akejkoľvek zaručenej investičnej príležitosti.

- Príliš konzistentné výnosy

Investičné majú tendenciu stúpať a klesať v čase, najmä tie, ktoré ponúkajú vysoké výnosy. Je preto podozrivé ak investície prinášajú pravidelné pozitívne výnosy bez ohľadu na tržné podmienky.

- Neregistrované investície

Ponziho podvody sa týkajú hlavne investícií, ktoré neboli riadne registrované v SEC alebo iných štátnych regulátoroch. Táto registrácia je veľmi dôležitá, pretože poskytuje investorom informácie o riadení, produktoch, službách a financiách spoločnosti, do ktorej sa rozhodnú investovať.

- Predajcovia bez licencie

Federálne a štátne zákony o cenných papieroch vyžadujú, aby investori a ich firmy boli licencovaní a registrovaní. Väčšina Ponziho podvodov zahŕňa osoby bez povolenia alebo neregistrované firmy.

- Utajované a/alebo komplexné stratégie

Vyhýbanie sa investíciám, ktorým človek nerozumie alebo pre ktoré nie je možné získať úplné informácie, je jedno zo základných pravidiel.

- Problémy s papierovaním

Nie je vhodné prijať výhovorky, ktoré sa týkajú neúplnosti investície v písomnej podobe. Chyby a nekonzistencia výpisov z účtov môžu rovnako znamenať, že finančné prostriedky sa neinvestujú podľa dohody.

[6] Podľa SEC - U. S. Security and Exchange Commission, Investment Company Liquidity Risk Management Programs; Commission Guidance for In-Kind ETFs (Conformed to Federal Register version), File No: S7-03-18, Effective Date: March 29, 2018.

Pyramídová hra

Vo všeobecnosti sa často zamieňa vyššie objasnená Ponziho schéma s pyramídovou hrou, a preto je dôležité spresniť rozdiel medzi týmito podvodnými operáciami.

Ponziho schéma vychádza z toho, že investor sa znovu rozhodne vkladať svoje výnosy a rovnako tak páchateľ hľadá nových investorov. V prípade pyramídovej hry to funguje na princípe odmeňovania účastníkov za získavanie ďalších. Títo účastníci na začiatku zaplatia akýsi „poplatok za vstup" a môžu investovať peniaze do spoločnosti alebo produktu.

Pri produktových pyramídových hrách sa výrobok predáva iba účastníkom tejto schémy, nie širokej verejnosti. Tento princíp funguje tak, že účastníci sa domnievajú, že sú distribútormi, ktorí si musia zakúpiť svoj vlastné zásoby. Môže im byť povedané, že ich zisky budú založené na predaji a registrácii nových distribútorov. Čo však účastníci nevedia je, že pre tento konkrétny produkt neexistuje trh.

Rovnako ako Ponziho schéma aj pyramídová hra vyžaduje kontinuálny príchod nových účastníkov, aby mohla prežiť. Pre účastníkov na nižších priečkach pyramídy platí vyššie riziko straty peňazí, pretože majú najmenej príležitosti a času získať ďalších účastníkov. Na druhej strane tí, ktorí stoja na vyšších priečkach sa nechajú ľahšie prehovoriť na reinvestovanie peňazí a s tým je spojené aj väčšie riziko. A keďže účastníci väčšinou do hry privolajú svojich kamarátov a blízkych, nie sú to len peniaze čo pri tejto hre strácajú.

Záver

Vplyvom prudko sa rozvíjajúcich globalizačných procesov, intenzívnej liberalizácie, rastúcej vzájomnej previazanosti (ale aj závislosti), a pokračujúceho „zmenšovania vzdialeností" či „zrýchľovania času" postupne stále viac problémov presahuje národnú, regionálnu či kontinentálnu úroveň a negatívne vplýva na celú ľudskú populáciu[7].

Úverové obchody sú a budú pre finančné inštitúcie, najmä banky hlavnou podnikateľskou činnosťou aj naďalej. Bankové úvery tiež plnia v ekonomike niekoľko dôležitých funkcií. V našom bankovom systéme, ktorý prekypuje likviditou, sa banky snažia zo všetkých síl alokovať aktíva tým najlepším spôsobom. Snažia sa čo najviac zjednodušiť procesy schvaľovania bez väčších prieťahov a ponúknuť tak svojim klientom väčší komfort.

Kto z nás v súčasnej dobe nemá žiadnu skúsenosť s pôžičkou, či s úverom? Takých je len málo, ale nájdu sa. Vo väčšej miere sa stretneme s človekom, ktorý nejakú tú skúsenosť už má, alebo ich má viac. Nemalé percento zadlžených sa potom rýchlo dostáva do začarovaného kruhu, z ktorého niet možné sa vymaniť. Keď toho človek má už veľa, snaží sa jednu pôžičku, či úver splatiť inou pôžičkou, ale málokedy je schopný ich splácať, pretože úroky a výška splátok sa stále viacej kumulujú.

Aktivita a postoj vedenia firmy je v boji s podvodmi kľúčová. Aj pri nedokonalom kontrolnom systéme, pokiaľ vedenie aktívne šíri etickú kultúru s nulovou toleranciu proti podvodom, propaguje odhaľovanie podvodov, investuje do riadenia rizika podvodov a vzdelávania zamestnancov, takáto spoločnosť bude ďaleko úspešnejšia ako firma s najmodernejším prevenčným systémom bez záujmu svojho vedenia o jeho výstupy.

Zoznam použitej literatúry:

1. KALABIS, Z. *Boj bánk proti praniu špinavých peňazí.* BIVŠ, 78, 2009. ISBN: 978-80-7265-147-4.
2. IVANČÍK, R., KELEMEN, M. *Teória bezpečnosti: Globálne problémy ľudstva.* Košice : Vysoká škola bezpečnostného manažérstva v Košiciach, 2015. 319 s. ISBN 978-80-89282-94-4.

[7] IVANČÍK, R., KELEMEN, M. *Teória bezpečnosti: Globálne problémy ľudstva.* Košice: Vysoká škola bezpečnostného manažérstva v Košiciach, 2015. 319 s.

3. IVANČÍK, R., KAZANSKÝ, R. Kybernetická vojna, útoky a terorizmus. In *Bezpečnostné fórum 2016*, zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016. s. 11-18. ISBN 978-80-557-1093-8.
4. KORAUŠ, A., VESELOVSKÁ, S., KELEMEN, P. Cyber security as part of the business environment. In Zborník z konferencie Medzinárodné vzťahy 2017: *Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice 30. novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 2017. 1113 s. ISBN 978-80-225-4488-7. ISSN 2585-9412.
5. MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. *Economic freedom – classification of its level and impact on the economic security*. AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157. ISSN 1804-7890.
6. U.S.Security and Exchange Commission, Investment Company Liquidity Risk Management Programs; Commission Guidance for In-Kind ETFs (Conformed to Federal Register version), File No: S7-03-18, Effective Date: March 29, 2018.
7. ZUCKOFF, M. *Ponzi's Scheme : The True Story of a Financial Legend*. Random House Publishing Group, 2006. 390 s. ASIN: B004IYBHIS.

Kontaktné údaje:

doc. Ing. Antonín Korauš, PhD., LL.M, MBA
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
antonín.koraus@minv.sk

JUDr. Stanislav Backa
Fakulta manažmentu
Prešovská univerzita v Prešove
stanislav.backa@gmail.com

Ing. Matej Bárta
Katedra kriminalistiky a forenzných vied
Akadémia PZ v Bratislave
matej.barta@minv.sk

Alternatívne kybernetické meny v súčasnosti

Antonín Korauš, Pavel Kelemen, Stanislav Backa, Jozef Polák

Abstrakt:
Fenoménom 21. storočia sa stali digitálne meny, teda elektronické (kybernetické) peniaze. Vznikajú nezávisle od vlád a bánk, sú buď ťažené prostredníctvom počítačov, alebo vydávané ich autormi. Na začiatku histórie digitálnych mien sa stal najslávnejší Bitcoin, ktorý patrí medzi takzvané kryptomeny.
Kľúčové slová:
Kybernetická bezpečnosť, podnikateľské prostredie, globalizácia, informačné a komunikačné technológie.

Abstract:
Phenomenon of the 21st century have become digital currency, therefore electronic (cyber) money. They arise independently from governments and banks, either drawn through computers or published by their authors. At the beginning of the history of digital currency Bitcoin has become the most famous, one of the so-called cryptocurrency.
Key words:
Cyber security, business environment, globalization, information and communication Technologies.

Úvod

Kryptomena (alebo tiež virtuálna mena, virtuálne peniaze, virtuálne platidlo, cryptocurrency) je digitálne platidlo, ktoré je určené na on-line obchodovanie. Je založená na kryptografii, ktorej cieľom je zvýšiť bezpečnosť virtuálnej meny. Hlavná definícia kryptomeny je, že využíva a implementuje princípy kryptografie na vytvorenie distribuovanej, decentralizovanej a bezpečnej digitálnej meny. Virtuálne peniaze sú novým a perspektívnym odvetvím virtuálnej ekonomiky, čo prináša mnohé výhody i úskalia.

Kryptomena je digitálna internetová mena, ktorá je založená na zložitom a šifrovanom matematickom algoritme. Výpočtom, overením a zašifrovanie časti (bloku) tohto algoritmu, môžete časť meny v nájdenom bloku získať (vyťažiť). Môžete si ju tiež kúpiť, teda vymeniť doláre alebo eurá za Bitcoin a ten za ďalšie kryptomeny. Tak ako každá iná mena, sú kryptomeny určené predovšetkým na rýchle a bezpečné platenie služieb a výrobkov. Môžete teda veľmi rýchlo zaplatiť za výrobok alebo službu tomu, kto menu akceptuje. Vďaka kryptomenám sú platby kdekoľvek hneď a bez poplatku, čo je veľká výhoda, ak platíte za drobnosť ktorej cena je nižšia, než niektoré poplatky za online platby.

Kryptomeny delíme do dvoch základných skupín. Meny odvodené od Bitcoinu a meny odvodené od Litecoinu, nazývané tieť Altcoiny. Úplné prvenstvo bude mať navždy Bitcoin. V ďalšej vlne po ňom vznikla druhá generácia coinov, ako sú Peercoin, Litecoin a ďalšie. Ďalej bola tretia generácia kryptomien, ktorá priniesla veľmi zaujímavú menu Dogecoin, ktorá do komunity priviedla veľké množstvo nových priaznivcov a stále si drží prvenstvo v počte fanúšikov a užívateľov. V roku 2014 začala nová generácia medzi nimi sa zdá byť najúspešnejšie Monero – XMR. A ďalšie obrovské množstvo nových a nových mincí, z ktorých len málo má perspektívu prežitia.

To čo od seba delí tieto meny je hardvér na ťaženie a spôsoby distribúcie. Inak je možné ich v zmenárňach (na burzách) premieňať za fiat peniaze, alebo ich meniť navzájom. Každá nová mena prináša množstvo marketingových nápadov a sľubov. Od revolučných spôsobov distribúcie a bezpečnosti až po dôraz na ekológiu, poprípade vedu.

Dejiny kryptomien a Bitcoin

Kryptomeny z pohľadu vzniku a vývoja možno členiť:

- Token - historickým príkladom môžu byť Britské tokeny používané v 17. až 19. storočí a Scripy používané počas obdobia veľkej krízy v 30. rokoch v USA. Aktuálnym príkladom môžu byť lokálne a komunitné meny ako napr. Zvolenský živec, Bristol

pound alebo Salt Spring Dollar v Kanade. Token má nižšiu vnútornú hodnotu, pretože jeho použitie je viac špecifické a často späté s verejnými dohodami ako napr. výmena za konkrétny tovar alebo službu.

- Centralizované digitálne meny - príkladom môžu byť vernostné body od finančných, telekomunikačných alebo maloobchodných firiem. Míle od leteckých spoločností a zlato z počítačovej hry Worl of Warcraft sú uzavreté systémy s transakciami len medzi špecifickými subjektami. Už vyššie spomenuté Salt Spring Dollar taktiež spadajú do tejto kategórie. Štruktúra riadenia je centralizovaná.
- Distribuované a/alebo decentralizované digitálne meny - táto kategória v sebe zahŕňa kryptomeny ako Bitcoin, Litecoin a Dogecoin. Transakcie sa dejú bez tretej strany a štruktúra riadenia je decentralizovaná hlavne kvôli open-source softwaru. Neexistuje žiaden právny subjekt zodpovedný za vykonané aktivity a preto tento typ mien nie je klasicky regulovateľný[1].

Prvá kryptomena, s ktorou sa začalo obchodovať, bol Bitcoin v roku 2009. Dňa 3. januára 2009 bol vytvorený prvý blok v blockchaine (reťazi blokov, tzv. Bitcoin Genesis Block) a za jej autora sa považuje človek alebo skupina s prezývkou Satoshi Nakamoto. Onedlho nato nasledovali ďalšie kryptomeny (Litecoin v 2011, Namecoin v 2011, Peercoin 2013, atď.). Média venovali veľkú pozornosť najrozšírenejšiemu Bitcoinu, Bitcoin ale nie je zďaleka jedinou virtuálnou menu, v skutočnosti ich už existujú stovky. Dnes (november 2017) existuje viac ako 1.000 virtuálnych mien, z nich patria k najpopulárnejším kryptomenám Bitcoin, Litecoin, Ripple, Dash, Monero a Ether/Ethereum Classic. Ich trhová kapitalizácia sa odhaduje na 1460 miliárd USD (12. september 2018) a každým dňom výrazne rastie.

Fiat money

Fiat peniaze, resp. fiat meny typu dolár, euro, rubeľ či jen, sú v súčasnosti považované za univerzálne platidlo ovládané centrálnou bankou. Nie sú kryté majetkom alebo drahými kovmi čo znamená, že centrálna banka môže kedykoľvek do obehu pustiť nové mince. Väčšinou preto, aby bolo možné zaplatiť štátne výdavky alebo kvôli stimulácii ekonomiky. To, okrem iného, znamená, že súčasné meny sú v podstate bezcenné a máme ich k dispozícii nekonečne veľa. Dôvod, prečo pre nás majú hodnotu je jednoduchý. Kolektívne sme sa na tom dohodli. Slovo fiat pochádza z latinčiny a v doslovnom preklade znamená „nech sa stane“, v spojení s peniazmi je však častejšie chápané ako „príkaz, autorizácia, konkrétne od vlády, že sa peniaze stávajú zákonným platidlom.“ Tento vynález v posledných desaťročiach umožnil explozívny rast svetovej ekonomiky. Sme „bohatší“, ako kedykoľvek predtým. Benefity fiat peňazí však v poslednej dobe začínajú ustupovať a do popredia sa dostávajú rôzne problémy počnúc od inflácie až po fakt, že všetky „moderné“ krajiny (vrátane Slovenskej republiky) sú „po uši zadlžené“. Z toho, samozrejme, vyvstáva otázka, komu tie peniaze dĺžime. [2]

Virtuálne peniaze versus fiat meny

Pri porovnaní kryptomeny s klasickými menami (fiat peniaze ako napr. USD, EUR, CZK atď.) je základný rozdiel v tom, že žiadna skupina alebo indivíduum nemôže zvýšiť množstvo kryptomeny v obehu (pri súčasných klasických menách naopak zvyšuje počet peňazí v obehu centrálna banka a komerčné banky podľa vlastného uváženia). Predstavujú distribuovanú, decentralizovanú a bezpečnú alternatívu k fiat menám.

---

[1] LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Singapore: Elsevier, 2015.

[2] SLAVKOVSKÝ, S. 2017. Čo je kryptomena? [online]. [cit. 2019-06-04]. Dostupné na: <https://krypto magazin.sk/co-je-kryptomena/>

Výhody a nevýhody virtuálnych peňazí

Bitcoin a ďalšie virtuálne meny majú niekoľko rozdielnych vlastností, ktoré ho odlišujú od vládnych mien. Medzi výhody patria:

- decentralizácia a deregulácia – Kryptomeny nepoznajú hranice a regulácie klasických fiat mien. Aj to je dôvod, prečo každý deň naberajú na popularite. Napr. Bitcoinová sieť nie je kontrolovaná jedným ústredným orgánom a teda žiadna ústredná autorita nemôže ovplyvňovať menovú politiku. Transakcie sú spracovávané počítačmi, ktoré ťažia Bitcoin.
- jednoduchosť platieb – Platby sú rýchle v porovnaní s prevodmi vykonávanými cez banky. Minimálne alebo žiadne poplatky za prevod. V porovnaní s prevodom fiat peňazí, poplatky za prevod Bitcoinov sú typicky veľmi nízke (menej ako jeden cent za prevod jedného Bitcoinu). Pri posielaní fiat peňazí môžu byť poplatky v niektorých prípadoch až 5%.
- deflačný charakter – Väčšina krajín má právo vydať nové peniaze. Tým, že sa zvyšuje množstvo peňazí v cirkulácii sa daná mena znehodnocuje (inflácia). V prípade Bitcoinov je celkové množstvo peňazí v obehu konečné a dopredu známe, nemôže presiahnuť 21 miliónov Bitcoinov.
- anonymita – Na jednej strane je anonymita transakcií výhodou, ale na druhej strane virtuálne meny umožňujú nezákonné obchodovanie.[3]

Medzi hlavné a závažné nevýhody kryptomien patria:

- vysoká volatilita – Nie je nezvyčajné aby cena kryptomien narástla, alebo sa znížila aj o 10% a viac v priebehu jedného dňa.
- bezpečnosť – Údaje k Bitcoin peňaženkám môžu byť ukradnuté a sú terčom hackerov. Obchodovanie cez regulovaných brokerov umožňuje tento risk minimalizovať.
- nenávratnosť – Ak sa omylom pošlú Bitcoiny na nesprávnu adresu, sú nenávratne stratené. [4]

Ako funguje blockchain?

Blockchain (bločenka) je distribuovaná databáza chránená šifrovaním tak, že zaručuje bezpečnosť informácií a chráni pred prístupom a úpravami od nevyžiadaných tretích strán. Využitie blochkchain technológie je neobmedzené, umožňuje vytvárať bezpečné transakcie medzi stranami bez potreby sprostredkovateľa. Odstránením sprostredkovateľov a režijných nákladov, bločenkové technológie majú potenciál výrazne znížiť transakčné poplatky, skrátiť čas transakcií z dní na minúty a spracovávať ich 24 hodín denne. Najväčšou devízou blockchainu, resp. bločenky je ich transparentnosť (nazývajú sa aj ako technológia pravdy). Dáta sa ukladajú do samostatných úložných celkov zvaných block. Tieto bloky sa ukladajú do reťazca jeden za druhým, preto chain. Bločenka je bezpečná. V prípade globálnej katastrofy bude blockchain fungovať, kým bude na svete existovať aspoň jeden počítač, ktorý bude mať uložený tento reťazec. Stovky miliónov počítačov, na ktorých sa ten-ktorý blockchain nachádza, však zaisťujú, že táto situácia nehrozí. Blockchain je možné využiť napríklad na elektronické voľby, hodnoverné ukladanie katastrálnych a matričných informácií, na registráciu vozidiel a podobne.[5]

[3] *Aké má Bitcoin výhody a nevýhody?* 2016. [online]. [cit. 2019-06-04]. Dostupné na:<http://www.ako obchodovat.sk/ake-ma-bitcoin-vyhody-a-nevyhody/>

[4] *Aké má Bitcoin výhody a nevýhody?* 2016. [online]. [cit. 2019-06-04]. Dostupné na:<http://www.ako obchodovat.sk/ake-ma-bitcoin-vyhody-a-nevyhody/>

[5] *Čo je to blockchain?* 2019. [online]. [cit. 2019-06-04]. Dostupné na:<http://blockchainslovakia.sk/blockchain ako-technologia-pravdy/>

Výhody blockchain technológie

Prostredníctvom kryptomeny môžete prenášať tisícky eúr z jednej krajiny do druhej s poplatkom menej ako 5 eurocentov prakticky okamžite. Ak to porovnáme s platbou prostredníctvom bankového prevodu, budete musieť čakať celý deň a zaplatíte poplatok niekedy až 3 % z čiastky prevodu (ak ide o zahraničnú platbu). Okrem toho, banka bude registrovať, že sa koná presun peňazí, zatiaľ čo u kryptomeny nemá nad takouto transakciou dohľad. Výhodou blockchain technológie je:

- lacná a rýchla – nevyžaduje centralizované zabezpečené servery a dokáže zaznamenávať obchody v reálnom čase, čo znamená okamžité prevody peňazí či aktív
- transparentná ale anonymná – záznamy o prevodoch si môže prečítať každý, kto má verejne prístupný kľúč (nie sú však identifikovateľné osoby, kto a komu prevádza peniaze)
- bezpečná – šifrovanie zabezpečuje, že obchody môžu robiť len autorizovaní účastníci s potrebnými prostriedkami, pričom záznamy sa už nedajú spätne meniť[6]

Bezpečnosť kryptomien

Princíp bezpečnosti kryptomien je založený na jednoduchom princípe overovaní údajov všetkými účastníkmi v sieti. Teda pomyselne každý vie, koľko máte v peňaženke a komu ste koľko zaslali. Tvorcovia kryptomien ich označujú za bezpečné, nefalšovateľné a neodcudziteľné.

Alternatívne digitálne meny - ALTCOINY

Altcoin predstavuje pojem pre inú alternatívu Bitcoinu. Nazývame tak každú digitálnu menu s výnimkou Bitcoinu. Altcoiny sú napodobeninou Bitcoinu, ktoré potajme dúfajú, že raz nahradia Bitcoin, pretože budú iné. Odlišné sú však len v niekoľkých bodoch, napríklad v rýchlosti transakcii, metódy distribúcie a iné. Aj keď väčšina z Altcoinov je dopredu predurčená na zánik, pre Bitcoin aspoň predstavujú zdravú konkurenciu a sú niečo ako „testovacie laboratórium" nových možností a funkcií. Pretože ak sa nájde Altcoin, ktorý má aspoň jednu funkciu lepšiu ako Bitcoin, Bitcoin je schopný jej nastavenie kopírovať a upraviť tak svoj kód a zase sa z neho stáva tá lepšia vynovená mena.[7]

Súčasnosť kryptomien

Vývoj kurzu Bitcoinu na trhu

Čo sa týka celkového vývoja hodnoty kurzu Bitcoinu na trhu od jeho začiatku, možno konštatovať, že od svojho začiatku v roku 2009 sa držal až do roku 2016 skoro na rovnakej hodnote s občasnými výkyvmi, ktoré nastali vďaka udalostiam, ktoré Bitcoin ovplyvnili (zrušenie stránky Silk Road, pád najväčšej burzy MtGox a iné), avšak aj napriek týmto udalostiam bola mena schopná sa vrátiť na svoju pôvodnú úroveň alebo aj o niečo vyššie. Medzi rokmi 2013 a 2014 zaznamenal Bitcoin dočasný nárast hodnoty, ktorý sa mu ale nepodarilo udržať. Tento pád nastal najmä vďaka pádu burzy Mt.Gox a už sa hodnota meny nedostala na svoju pôvodnú hodnotu. Veľké prírastky hodnoty nastali v ďalších rokoch.

Aktuálne je na svete viac ako tisíc dvesto rôznych kryptomien a v priemere každý deň pribudne ďalšia. Bitcoin je z nich najúspešnejší, s viac ako polovičným trhovým podielom.

---

[6] *Čo je to blockchain?* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <http://blockchainslovakia.sk/blockchain-ako-technologia-pravdy/>

[7] Wikipedia: the free encyclopedia. 2001. *Proof-of-work system.* [online]. [cit. 2019-06-04]. Dostupné na: <https://en.wikipedia.org/wiki/Proof-of-work_system>

Jeden z hlavných argumentov vzniku Bitcoinu je jeho maximálny objem v obehu, bez možnosti ho v budúcnosti zvyšovať.[8]

Ako poznáme napríklad euro, dolár alebo libra, tak aj vo svete kryptomien existuje Bitcoin, Litecoin, Namecoin, Dogecoin a mnoho ďalších. Sú obchodovateľné na burze, čo v praxi znamená, že majú reálnu hodnotu. Každá z týchto digitálnych mien sa od seba trochu odlišuje, či už spôsobom ťažby alebo tým, čo predstavuje. V októbri v roku 2018 boli na prvých desiatich miestach tieto kryptomeny:

- Ethereum
- Ripple
- Litecoin
- Dash:Digital+cash
- NEM
- Ethereum Classic
- Monero
- Zcash
- Decred: Decentralized credit
- PIVX: Private Instant Verified Transaction

Altcoiny predstavujú alternatívnu náhradu Bitcoinu, väčšina z nich vznikla až po tom, čo Bitcoin zožal veľký úspech a majú predstavovať lepšiu verziu, s vylepšenými funkciami ako má Bitcoin.

Ethereum

Najviac skloňovanou digitálnou menou po Bitcoine je Ethereum, ktorá v posledných mesiacoch priťahuje na svoji stranu stále viac a viac záujemcov. Digitálna mena Ethereum vznikla ku koncu roka 2013. Podobne ako Bitcoin, aj Ethereum funguje na princípe decentralizovanej platformy, funguje pre aplikácie, ktoré pracujú tak, ako boli naprogramované bez akejkoľvek šance podvodu, cenzúry alebo prítomnosti tretej strany.[9]

Obr. 1: Ethereum
Zdroj: https://securecdn.pymnts.com/wp-content/uploads/2017/06/Ethereum.jpg

[8] LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Singapore: Elsevier*, 2015.
[9] SCHIRRIFF, K. 2014. *Bitcoin mining the hard way: the algorithms, protocols, and bytes.* [online]. [cit. 2019-06-04]. Dostupné na: <http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html>

Ethereum je open-source verejná platforma založená na blockchaine. Jej hlavnou výhodou je skriptovacia funkcionalita (smart kontrakty). Ponúka decentralizovaný Turingovsky kompletný virtuálny stroj známy ako Ethereum Virtual Machine (EVM), ktorý vykonáva skripty pomocou medzinárodnej siete verejných uzlov. Ethereum je novinkou v oblasti výpočtovej techniky, je postavený z technológií a koncepcií pôvodne vyskúšaných pri Bitcoine. Napriek tomu, že Ethereum bol zatienený Bitcoinom v rôznych oblastiach, nedávne správy a vývoj v oblasti Ethereum začali vzbudzovať hlboký záujem o túto kryptomenu. Rozdiel medzi Bitcoinom a Ethereom spočíva v tom, že zatiaľ čo Bitcoin blockchain sa používa na sledovanie vlastníctva digitálnej meny (Bitcoinu), blockchain pri Ethereu sa zameriava na spustenie programovacieho kódu ktorejkoľvek decentralizovanej aplikácie.[10]

Bitcoin versus Ethereum

Kým Bitcoin je niekedy popisovaný ako celosvetová účtovná kniha, ktorá je však obmedzená len na zaznamenávanie transakcií len v určitej mene, tak Ethereum by sa dalo opísať ako celosvetový počítač – miesto, kam ktokoľvek môže nahrať svoj program a mať istotu, že jeho kód bude spustený presne v tej podobe, ako bol zamýšľaný a že bude spustený na platforme tvorenej tisíckami počítačov po celom svete, ktoré – v mene zdieľanej zhody – overia výsledok a nie je možné ich všetky vypnúť či napadnúť. Táto technológia, ktorá už siedmy rok poháňa Bitcoin, rovnaká bezpečnosť daná použitú kryptografie plus navyše schopnosť vykonávať výpočtové operácie je teraz dostupná všetkým a vývojárom sa tak otvárajú nové príležitosti.

Kryptomeny

Kryptomeny sú podskupinou digitálnych platidiel, ktoré v rámci zvyšovania bezpečnosti používajú na kódovanie transakcií pokročilú kryptografiu. Vo svojej najčistejšej forme je kryptomena peer-to-peer verzia elektronickej hotovosti, teda mena s transakciami typu klient-klient. Umožňuje online platby od jedného subjektu k druhému priamo, bez nutnosti finančnej inštitúcie. Sieť časovo označí danú transakciu použitím kryptografickej funkcie proof-of-work POW (systém potvrdenia práce). Tento koncept, ktorý slúži k odradeniu od servisných útokov a ďalšieho zneužívania služieb ako je napr. posielanie spamovej pošty, prvýkrát predstavili v roku 1993 Cynthia Dwork a Moni Naor a spočíva vo vyžadovaní splnenia práce od žiadateľa o službu. Kľúčom pre fungovanie POW je jeho asymetria: pre žiadateľa o službu musí byť práca dostatočne náročná, ale uskutočniteľná, naopak pre poskytovateľa služieb musí byť kontrola vykonania tejto práce veľmi ľahká. Konkrétne pre bežného používateľa je jednoduché poslať jeden e-mail, pretože práca je jednoduchá avšak ak by ten istý užívateľ chcel poslať spamový mail 10 000 ľuďom, musel by už vlastniť značný počítačový výkon, aby mohol zadanú prácu vykonať. Existujú 2 triedy POW protokolov:

a) Protokol typu výzva-odpoveď (challange - response) predpokladá priame interaktívne spojenie medzi klientom a poskytovateľom služby (serverom). Poskytovateľ služby zvolí zdanie úlohy (výzva) napr. hľadanie určitej položky s konkrétnymi vlastnosťami v celej sade položiek. Klient vyhľadá príslušnú odpoveď, ktorú odošle serveru a ten ju skontroluje.

b) Protokol typu riešenie-overenie (solution - verification) interaktívne spojenie medzi klientom a serverom nepredpokladá to znamená, že úloha sa zadá sama bez toho, aby ju predtým server vyriešil. Preto musí server overiť aj výber problému, aj jeho nájdené riešenie.[11]

---

[10] *List top cryptocurrencies analysis comparison*. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <http://www.businessinsider.com/list-top-cryptocurrencies-analysis-comparison>

[11] *Proof-of-work system.* In Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001. [online]. [cit. 2019-06-04]. Dostupné na: <https://en.wikipedia.org/wiki/Proof-of-work_system>

Bitcoin užíva proof-of-work funkciu s názvom Hashcash (challange - response) na tvorenie blokov transakcií. Jednoducho povedané ide v podstate o súťaž spočívajúcu v dekódovaní, ktorá motivuje tých ktorí sa jej zúčastnia. Konkrétne účastník, ktorému sa ako prvému podarí rozlúštiť kód, dostane za odmenu novo vytvorené Bitcoiny. Táto súťaž takto vytvorí záznam o uskutočnených transakciách. Ďalšie populárne kryptomeny ako napr. Peercoin alebo BlackCoin používajú metódu proof-of-stake (doklad o podiely), ktorej hlavnou úlohou je opäť zabrániť dvojitému utrácaniu. V proof-of-work systéme miner musí opakovane používať hashovacie algoritmy na overenie elektronických transakcií, zatiaľ čo v proof-of-stake systéme musia dokazovať vlastníctvo určitého počtu coinov. V systéme proof-of-work pravdepodobnosť vyťaženia bloku závisí na množstve práce, ktorú vykonal miner. V systéme proof-of-stake je podstatné koľko coinov miner vlastní - miner, ktorý vlastní 1% coinov môže vyťažiť 1% blokov. To znamená, že miner v tomto systéme musí vlastniť coiny, aby mohol ťažiť. Ďalším podstatným rozdielom medzi týmito systémami je energetická náročnosť, pričom proof-of-work je oproti proof-of-stake oveľa viac energeticky náročný.[12]

Vo viacerých prácach a komerčných článkoch sa píše, že bitcoin je prvá kryptomena na svete. To v skutočnosti nie je pravda. Prvou komerčne úspešnou kryptomenou je eCash, ktorého fungovanie popísal David Chaum v protokoloch z roku 1983 a 1992. eCash sa zrealizoval vďaka firme DigiCash, Inc. a použil sa ako systém pre mikroplatby (PayPal definuje ako platby < 12 $, Visa definuje ako platby < 20 $) v americkej banke medzi rokmi 1995 až 1998. V európskych krajinách eCash implementovali Credit Suisse vo Švajčiarsku, Deutsche Bank v Nemecku alebo aj Den norske Bank v Nórsku. Platobné transakcie sa uskutočňovali online alebo offline. Kryptografia sa použila na zamedzenie dvojitého utrácania a tiež sa pomocou nej chránili osobné údaje používateľa. eCash bol teda centralizovaný platobný systém patriaci firme DigiCash, Inc. Na konci 90. rokov bol systém predaný firme InfoSpace a nakoniec skrachoval.[13]

Pri vzostupe globálnej finančnej krízy v roku 2008 sa záujem o kryptomeny znova zvýšil. Americký programátor a kryptograf Nick Szabo na blogu[14] vysvetlil, ako môžu kryptomeny predísť problémom spájaným s peniazmi s núteným obehom a svetu predstavil myšlienku decentralizovanej digitálnej meny zvanej bit gold. Ako už naznačuje samotný názov, predpokladá sa existencia zlata určeného na ťažbu a jeho registrácia v digitálnom registri. Tento digitálny register obmedzil potrebu tretej strany pre transakcie. Jeho myšlienka bola v skutku jednoduchá. Navrhol jednoduchý protokol, ktorý požadoval od účastníkov vynaloženie prostriedkov na ťažbu tohto digitálneho zlata, pričom tieto prostriedky sa využili na overenie tohto verejne prístupného digitálneho registra. Prečo bol jeho nápad úspešnejší ako predošlé formy kryptomien? Jednoducho preto, že tieto myšlienky začal uverejňovať v čase vypuknutia finančnej krízy, kedy ľudia prestávali veriť zaužívanému finančnému systému a zároveň aj kvôli tomu, že ako prvý prišiel s myšlienkou voľne prístupného digitálneho registra. Prvou inováciou bolo navrhnutie odmeny pre minerov, druhou zas voľne prístupný register - blockachain. [15]Aj keď sa bit goldu nakoniec nepodarilo komerčne uspieť, je to bez pochýb priamy predchodca Bitcoinu ako ho poznáme dnes.

Už od vzniku Bitcoinu v roku 2009 sa mu vyčítali rôzne nedostatky a mnoho ľudí ho považovalo len za pokus, preto na seba vývojárska komunita nedala dlho čakať a snažila sa predstaviť nové algoritmy a riešiť aj sociálno-ekonomické problémy, ktoré Bitcoin priniesol.

[12] *Proof of Stake.* 2017. [online]. [cit. 2019-06-04]. Dostupné na: <https://en.bitcoin.it/wiki/Proof_of_Stake>

[13] LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Singapore: Elsevier, 2015.

[14] SZABO, N. 2008. *Bit gold*. [online]. [cit. 2019-06-04]. Dostupné na:<http://unenumerated.blogspot.cz/2005/12/bit-gold.html>

[15] LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Singapore: Elsevier, 2015.

Nové protokoly sa zverejňovali na internetových fórach a čakalo sa, či sa nazbiera dosť priaznivcov a stane sa z nej uznávaná kryptomena. Pre všetky nové kryptomeny však kľúčovým prvkom zostáva blockchain a kryptografia.[16]

Kryptomeny, ktoré vznikli vďaka sociálnym sieťam

Existovalo mnoho pokusov, ako k Altcoinom prilákať rôznorodé komunity ľudí, nie len programátorov a technokratov. Reddcoin je asi najlepším príkladom. Reddcoin vytvoril tzv. sociálnu peňaženku, ktorá jednoducho umožňuje transakcie na najpopulárnejšie mediálne platformy ako Twitter, YouTube alebo Reddit. Reddcoin bol špeciálne vyvinutý na posilnenie finančného dotovania obsahu - užívateľ má možnosť mikroplatbou podporiť autora článku, blogu, tweetu alebo komentára. Bitcoin sa v skutočnosti ukázal ako nevýhodný pre online príspevok, pretože transakcie menšie ako 0,01 BTC nechcú mineri overovať bez minimálneho poplatku 0,0001 BTC. Ďalšou kryptomenou, ktorá vznikla vďaka sociálnym sieťam je Dogecoin. Ten vznikol len tak pre zábavu ako reakcia na veľmi populárny internetový meme z roku 2013. Dogecoin sa stal tak populárny a používaný, že v období medzi decembrom 2013 a februárom 2014 mal najväčší počet transakcií a dokonca predbehol aj samotný Bitcoin. Dogecoin sa použil aj na rôzne fundraisingové účely - viac ako 26 miliónov Dogecoinov sa vyzbieralo na pomoc jamajskému bobovému tímu, aby mohol štartovať na zimných olympijských hrách v Soči v Rusku v roku 2014.

Charakteristiky jednotlivých virtuálnych mien

Dnes Bitcoin zďaleka nie je jedinou kryptomenou na trhu. Myšlienkou decentralizovaného digitálneho platidla sa inšpirovalo mnoho ďalších skupín, ktoré vytvorili celú paletu rôznych technológií. Medzi najväčšie kryptomeny patrí Ripple, platobný systém, ktorý umožňuje platbu v rôznych menách, podobne ako PayPal. Ripple ovláda jedna spoločnosť, ktorá zároveň vlastní viac než 60 percent Ripple kryptomincí. Naopak, medzi systémy spĺňajúce tradičnú definíciu kryptomeny patrí Litecoin, Ethereum, Monero, Dash či Zcash.

Litecoin (LTC)

Litecoin sa považuje za striebro, ak je bitcoin zlato. Lee ho vytvoril v roku 2011 a považuje sa za alternatívu bitcoinu. Lee sa v podstate zameral na zníženie času potrebného na potvrdenie nových transakcií a na vylepšenie spôsobu, akým sa ťažia bitcoiny, aby sa zabezpečilo, že by tak mohol robiť každý. "Moja vízia je, že ľudia budú používať Litecoin každý deň na nákup veci. Bola by to len voľba platobnej metódy," povedal dávnejšie Lee. Litecoin je tiež navrhnutý tak, aby produkoval viac mincí - 84 miliónov oproti 21 miliónom bitcoinov. V súčasnosti je v obehu okolo 54 miliónov mincí, v porovnaní so súčasnými 16,7 miliónmi bitcoinov.

Monero (XMR).

Prednosťou je anonymita. Podrobnosti každej transakcie, vrátane odosielateľa, prijímateľa a objemu, sú zaznamenané vo verejnej knihe, ale tak, že sa nedajú odhaliť. Teoreticky neexistuje žiadna možnosť, aby nikto iný pripojil medzi odosielateľa a prijímateľa, alebo aby videl veľkosť transakcie. Znie to atraktívne pre počítačových zločincv? Asi áno. Hackeri stojaci za globálnym útokom WannaCry, ktorý infikoval 230 000 počítačov so systémom Microsoft Windows, vyžadovali platby v Monero. Hovorí sa, že hackerov, ktorí požadujú bitcoiny je oveľa viac a podporovatelia Monera tvrdia, že najväčšie prípady využitia mincí nie sú nezákonné. Monero môže byť atraktívne pre spoločnosti, ktoré chcú presunúť

[16] LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data.* Singapore: Elsevier, 2015.

peniaze bez toho, aby o tom vedela konkurencia, alebo ktokoľvek, kto jednoducho nechce, aby boli transakcie zverejnené. Len nedávno sa medializovala správa, že 45 hudobníkov, vrátane Lana Del Ray, Sia a Dolly Parton, bude prijímať Monero. Mnohí dokonca ponúknu zľavy tým, ktorí s nimi platia. V obehu je asi 15,5 milióna XMR a na rozdiel od bitcoinu a Litecoinu, Monero nemá fixne daný konečný počet mincí.

Neo

Ak Čína uvoľní svoj postoj k ICO a bitcoinu, ethereum sa stane dvojkou hneď za bitcoinom, na základe trhovej kapitalizácie vo výške 61 miliárd dolárov. Takže Neo zrejme ešte má čo doháňať. Neo sa na trh dostal okolo roku 2014, vtedy ešte pod názvom "Antshares". Áno, je to odkaz na Matrix. V obehu je v súčasnosti 65 miliónov z celkového počtu 100 miliónov mincí.

Cardano (Ada)

Táto platforma ďalšej generácie má za sebou správny tím, odhodlanie a peniaze na vytvorenie skutočného kandidáta na ethereum. Cardano blockchain bol spustený len pred niekoľkými mesiacmi, ale už sa mu podarilo presadiť na scéne s obrovskými prírastkami. V novembri sa dostala do TOP 10 kryptomien, pokiaľ ide o trhovú kapitalizáciu. Neskôr sa prepadla na 13. miesto. Projekt sa začal v roku 2015 a považuje sa za prvý blockchain s vedecký pozadím, vybudovanú vedúcimi akademikmi a inžiniermi prostredníctvom odborného výskumu. Cardano je stále relatívne neznámy, ale už často využívaný v súkromných transakciách, čo je základ pre masové rozšírenie. Generálny riaditeľ Charles Hoskinson hovorí, že Cardano sa zaoberá otázkami "trvalej udržateľnosti, interoperability a škálovateľnosti", aby sa kryptomeny premenili zo "zábavnej novinky" na niečo, čo by mohli využiť miliardy ľudí a prepojiť sa s legálnym finančným systémom. Cardano sa ešte stále nachádza vo veľmi rannom štádiu pričom ďalšia fáza má začať niekedy v druhom štvrťroku roku 2018. To znamená, že ešte to môže chvíľu trvať, kým sa prepracuje k plnohodnotnej inteligentnej zmluvnej platforme. V súčasnosti je v obehu asi 26 miliárd z maximálne 45 miliárd mincí.

Ripple (XRP)

Bývalí vývojári bitcoinu si založili softvérovú spoločnosť Ripple v roku 2012 a jej digitálna mena, XRP, je považovaná za logického nástupcu bitcoinu. Nie je to len mena, ale systém, v ktorom sa dá obchodovať s akoukoľvek menou vrátane bitcoinu. Ripple spája banky, poskytovateľov platieb, burzy digitálnych aktív a korporátnu sféru prostredníctvom RippleNet, aby poskytla bezprecedentnú skúsenosť, ako posielať peniaze do celého sveta, vysvetľujú jej tvorcovia. Ripple získala licenciu vo viac ako 100 bankách. Objem XRP v obehu je v súčasnosti okolo 38,7 miliárd z maximálnej ponuky 100 miliárd, čo je oveľa viac ako je strop u zvyšku kryptomien v tomto zozname.

Iota (MIOTA)

Veľkou výhodou je, že nemá žiadne obchodné poplatky, žiadnych ťažiarov ani bloky. Pri každej transakcii, ktorú vykonávate, sa váš výpočtový výkon používa na overenie ďalších dvoch transakcií, takže každý majiteľ Iota je zároveň aj "ťažiarom". Iota sa v podstate zameriava na to, aby sa stala chrbticou bezpečných platieb medzi počítačmi v rámci technológie Internet vecí. Je unikátna v tom, že je považovaná za prvú kryptomenu vytvorenú bez použitia blockchainu. Namiesto toho je založená na rozloženej architektúre nazvanej "The Tangle". Táto inovácia umožnila Iote dosiahnuť tri hlavné míľniky: transakcie s nulovými nákladmi, transakcie offline a nekonečnú škálovateľnosť. Najnovšie partnerstvo so spoločnosťou Microsoft ju len podsunulo do najvyššej úrovne najcennejších kryptomien. Maximálny počet

mincí v obehu je tesne pod 2,8 miliardou, a takmer celá maximálna ponuka je už v súčasnosti v obehu.

Bitcoin Cash

Bitcoin Cash patrí medzi najnovšie kryptomeny, zrodil sa v auguste 2017 po tvrdom rozdelení bitcoinu, v podstate je to nová verzia bitcoinu, ktorý ale nie je kompatibilná s bitcoinom. Bitcoin Cash vznikol z dôvodu, že niektorí používatelia boli frustrovaní vysokými poplatkami a nekonečným časom potrebným pre spracovanie transakcií. Vzhľadom na to, že Bitcoin Cash má väčší limit veľkosti blokov, jeho tvorcovia tvrdia, že táto kryptomena má väčšiu kapacitu na spracovanie transakcií s nižšími poplatkami a za kratší čas. Na druhej strane sú však tí, čo tvrdia, že rast veľkosti blokov ohrozuje decentralizovanú podstatu kryptomeny. Najväčšou výzvou, ktorej čelí Bitcoin Cash, je masívnejšie prijatie. Musí presvedčiť firmy, aby akceptovali bitcoin aj túto konkurenčnú platobnú sieť. Rovnako musí presvedčiť ťažiarov, aby sa zúčastňovali na procese zúčtovania jednotlivých transakcií. V polovici novembra Bitcoin Cash na krátko prekročil trhovú kapitalizáciu etherea, aby sa dočasne stal druhou najcennejšou kryptomenou. Odvtedy ale spadol na tretie miesto. V obehu je v súčasnosti 16,8 milióna mincí, z maximálnej ponuky 21 miliónov.

Záver

Alternatívne kybermeny sú zaujímavým novým nástrojom a bude takisto zaujímavé sledovať ich ďalší vývoj. Či bude hodnota Bitcoinu naďalej stúpať alebo jeho hodnota nečakane klesne. Otázkou zostáva, či špekulanti, ktorí nakupujú veľké množstvo kryptomien sa rozhodnú v čase, kedy bude mať Bitcoin vysokú hodnotu, ho zbaviť a tak hodnota meny klesne alebo akým spôsobom sa bude vyvíjať vzhľadom na to, že Bitcoinov je limitované množstvo a akým spôsobom a v akej hodnote bude predávaný, ak sa vyťažia všetky Bitcoiny. Bezpečné využitie kryptomien ku kryptomenám začínajú zaujímať postoje ľudia, vlády i ekonomické systémy. Zatiaľ sú ich postoje skôr úsmevné a rozporuplné a pôsobia ako strach z neznáma. Predovšetkým sú označované za dobrý nástroj na nákup zbraní a drog pre teroristov. V skutočnosti sa už stali prípady, keď boli poskytnuté a vymenené vedome kryptomeny na nákup drog a nelegálneho tovaru a služieb, rovnako ako sa k tomu odjakživa zneužívajú bežné peniaze a komodity, zlato alebo ľudské životy. V skutočnosti ale za Bitcoinom stojí obrovská partia ľudí, veľmi schopných programátorov, vývojárov, inovátorov a cieľavedomých obchodníkov, ktorí podľa ich tvrdení majú s Bitcoinom len tie najlepšie úmysly.

Zoznam použitej literatúry:

1. BÖHME, R., CHRISTIN, N., EDELMAN B., TYLER MOORE, T. *"Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives,* 29(2): 213-38. DOI: 10.1257/jep.29.2.213. 2015.
2. BARBER, S., BOYEN, X., SHI, E., UZUN, E. Bitter to better – how to make Bitcoin a better currency. In *Keromytis,* A.D. (ed.) FC 2012. LNCS, vol. 7397, Springer, Heidelberg, 2012. s. 399–414.
3. BRIERE, M., OOSTERLINCK, K., SZAFARZ, A. Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins, SSRN working paper series, 2013.
4. BUCHHOLZ, M., DELANEY, J., WARREN, J., PARKER, J. 2012. *Bits and Bets, Information, Price Volatility, and Demand for BitCoin. Economics 312.* [online]. [cit. 2019-06-04]. Dostupné na: <http://www.bitcointrading.com/pdf/bitsandbets.pdf >
5. European Central Bank (ECB). 2012. *Virtual Currency Schemes.* [online]. [cit. 2019-06-04]. Dostupné na: <www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf >
6. GRINBERG, R. *Bitcoin: an innovative alternative digital currency. Hastings Sci*. Technol. Law J. 4, 2011. s. 159–208.

7. 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.
8. KORAUŠ, A., GOMBÁR, M., KELEMEN, P., BACKA, S. 2019. *Using quantitative methods to identify insecurity due to unusual business operations, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: < https://doi.org/10.9770/jesi.2019.6.3(3) >
9. KORDÍK, M., KURILOVSKÁ, L. 2019. *Content of a Intra Group Compliance Agreement as a risk mitigating factor, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.3(10) >
10. LEE KUO CHUEN, D. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Singapore: Elsevier, 2015. ISBN 978-0-12-802117-0.
11. POON, J., DRYJA, T. 2015. *The Bitcoin lightning network: scalable off-chain instant payments.* [online]. [cit. 2019-06-04]. Dostupné na: <https://lightning.network >
12. ROSENFELD, M. 2012. *Overview of colored coins. White paper*. [online]. [cit. 2019-06-04]. Dostupné na:<Dostupné z: bitcoil.co.il>
13. SCHIRRIFF, K. 2014. *Bitcoin mining the hard way: the algorithms, protocols, and bytes*. [online]. [cit. 2019-06-04]. Dostupné na: <http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html>
14. SZABO, N. 2008. *Bit gold*. [online]. [cit. 2019-06-04]. Dostupné na: <http://unenumerated.blogspot.cz/2005/12/bit-gold.html>
15. Wood, D.G. 2014. *Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum*. [online]. [cit. 2019-06-04]. Dostupné na: <https://securecdn.pymnts.com/wp-content/uploads>
16. *Finančný kompas.* [online]. [cit. 2019-06-04]. Dostupné na: <www.financnykompas.sk>
17. *Ethereum logo.* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://securecdn.pymnts.com/wp-content/uploads/2017/06/Ethereum.jpg>
18. *List top cryptocurrencies analysis comparison.* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <http://www.businessinsider.com/list-top-cryptocurrencies-analysis-comparison>
19. SLAVKOVSKÝ, *S.* 2017. *Čo je kryptomena?* [online]. [cit. 2019-06-04]. Dostupné na: <https://kryptomagazin.sk/co-je-kryptomena/>
20. *Aké má Bitcoin výhody a nevýhody?* 2016. [online]. [cit. 2019-06-04]. Dostupné na: <http://www.akoobchodovat.sk/ake-ma-bitcoin-vyhody-a-nevyhody/>
21. *Čo je to blockchain?* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <http://blockchainslovakia.sk/blockchain-ako-technologia-pravdy/>
22. *Proof of Stake.* 2017. [online]. [cit. 2019-06-04]. Dostupné na: <https://en.bitcoin.it/wiki/Proof_of_Stake>
23. Wikipedia: the free encyclopedia. 2001. *Proof-of-work system.* [online]. [cit. 2019-06-04]. Dostupné na: <https://en.wikipedia.org/wiki/Proof-of-work_system>

Kontaktné údaje:
doc. Ing. Antonín Korauš, PhD., LL.M, MBA
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
antonín.koraus@minv.sk

Mgr. Pavel Kelemen
Fakulta manažmentu
Prešovská univerzita v Prešove
kelemen.pavel@gmail.com

JUDr. Stanislav Backa
Fakulta manažmentu
Prešovská univerzita v Prešove
stanislav.backa@gmail.com

Ing. Jozef Polák
Fakulta manažmentu
Prešovská univerzita v Prešove
jozefpolak64@gmail.com

Riadenie rizika podvodu z pohľadu bezpečnosti a včasného odhalenia

Antonín Korauš, Pavel Kelemen, Štefan Zachar

Abstrakt:
Podvody môžu byť drahé odčerpanie finančných zdrojov spoločnosti. V dnešnom konkurenčnom podnikateľskom prostredí si žiadna spoločnosť nemôže dovoliť vyradiť časť svojich príjmov na pokrytie nákladov na podvody. Tie podniky, ktoré účinne identifikovali svoje najvýznamnejšie náklady na podvody, podnikli významné kroky v útokoch a minimalizácii týchto nákladov. Spoločnosti, ktoré nevidia a nešetria svoje náklady spojené s podvodmi, sú ohrozené konkurenciou, ktorá tak zníži svoje náklady.
Najčastejším druhom interných podvodov v slovenských podnikoch sú krádeže majetku a použitie prostriedkov na súkromné účely. Na druhej strane k najrozšírenejším externým podvodom patrí manipulácia pri výberovom konaní a vystavovanie falošných faktúr.
Kľúčové slová:
Úver, úverový podvod, riziková skupina úverových podvodov, prevencia úverových podvodov, schémy podvodov.

Abstract:
Fraud can be a costly drain on a company's financial resources. In today's competitive business environment, no company can afford to throw away part of its revenues to cover the costs of fraud. Those businesses which have effectively identified their most significant fraud costs have made significant steps in attacking and minimizing those costs. Companies which did not spot and tackle its fraud costs are vulnerable to competitors who lower their costs by doing so.
The most common type of internal fraud in Slovak enterprises is the theft of property and the use of funds for private purposes. On the other hand, the most widespread external fraud is manipulation in the selection process and the display of false invoices.
Key words:
Credit, credit fraud, credit fraud risk group, credit fraud prevention, fraud schemes.

Úvod

Jedným z kľúčových nástrojov prevencie, ktorými sa firmy môžu brániť výskytu podvodov, je analýza rizika vzniku podvodov (tzv. fraud risk assessment)[1]. Každá firma by mala vyhodnotiť riziko výskytu jednotlivých podvodných schém, identifikovať ich pravdepodobnosť a dopad, odhaliť slabá miesta kontrolného systému a eliminovať riziko zavedením chýbajúcich kontrol a opatrení.

- V prvom kroku je potrebné zmapovať aktuálnu situáciu, zistiť, aké podvody firme hrozia, na ktorom oddelení sa môžu vyskytovať a aká je ich pravdepodobnosť výskytu.
- Následne je potrebné si vybrať (napríklad 15-20) najvýznamnejších podvodných schém a otestovať, či je kontrolný systém schopný tieto podvody odhaliť.
- Potom by sa mala firma zamerať na zistenie konkrétnych slabých miest a navrhnúť také nástroje a kontroly, aby svoj rozpočet na prevenciu využila čo najlepšie – získať za čo najnižšie investície čo najviac informácií. Medzi takéto nástroje patrí napríklad dôkladne preverovať reputácie obchodných partnerov, odhaľovanie možných prepojení medzi nimi a zamestnancami, a vyhľadávanie neštandardných príznakov v obchodných transakciách a účtovných záznamoch.

Možností, ako zdokonaliť svoj prevenčný systém a zamedziť tak výskytu podvodov, je viac:

- Zaktivizovať vedenie – postoj vedenia firmy k podvodom je zásadným faktorom úspechu. Vedenie, ktoré i pri nedokonalom kontrolnom systéme firmy aktívne šíri etickú kultúru s nulovou toleranciou voči podvodom, propaguje odhaľovanie podvodov

[1] KALABIS, Z. *Boj bank proti praniu špinavých peňazí*. BIVŠ, 2009. s. 78.

a investuje do riadenia rizík a vzdelávania svojich zamestnancov, bude ďaleko úspešnejšie než vedenie s moderným preventívnym systémom ale len s pasívnym prístupom.

- Zaviesť preventívne a detekčné techniky – k tým efektívnym patria napríklad whistle-blowing (systém oznamovania, zberu a vyhodnotenia podnetov o existencii nekalého správania), ďalej preventívne preverovanie obchodných transakcií v účtovníctve, preverovanie obchodných partnerov a zákazníkov, overovanie informácií od záujemcov o zamestnanie umožňujúce neprijatie podvodníkov, dôkladný výber riadiacich pracovníkov, alebo odhalenie prepojenia medzi zamestnancami a tretími stranami.
- Vzdelávanie zamestnancov – firma by mala investovať taktiež do vzdelania svojich zamestnancov súvisiaceho s porozumením etického správania, stotožnenia sa s hodnotami spoločnosti, rozpoznávaním podvodov a reakciami na ich výskyt.

Včasné odhalenie podvodov

Vo vedeckých štúdiách (Feroz et al., 2000, Dobrovič et al., 2017, Korauš et al., 2017, Mura et al., 2017, Spathis et al., 2002; Ravisankar a kol., 2011) sú predmetom výskumu analýzy podvodov.[2,3,4,5,6,7]

Riziko podvodov bolo doposiaľ považované len za jedno z mnohých prevádzkových rizík podnikania. Firmy a finančné inštitúcie mu vzhľadom k nízkemu povedomiu nevenovali v Česku ani na Slovensku takú pozornosť, ako iným rizikám. V poslednej dobe však dochádza k výraznej zmene trendu. Vzhľadom k vysokým finančným stratám, škodám na reputácii a obchodných vzťahoch, resp. zániku niektorých spoločností, sa podvody dostali na úroveň hlavných podnikateľských rizík. Otázkou je či sú lokálne firmy pripravené na ich riadenie.

Dostupné štatistiky uvádzajú znepokojujúce čísla o dopadoch podvodov. Výskyt podvodov v Česku a na Slovensku uvádza takmer polovica firiem, ktoré ich odhalili a utrpeli stratu väčšiu než 50 000 EUR. Zahraničné prieskumy nie sú o nič optimistickejšie – podľa európskej verzie prieskumu Association of Certified Fraud Examiners (ACFE)[8] za rok 2017 dosiahla priemerná výška strát bežnej firmy 5 percent jej ročného obratu. Straty z podvodov sú už také obrovské, že sa firmám oplatí investovať do detekčných a preventívnych programov.

V súčasnej dobe sa zvyšuje úroveň povedomia a každý manažér môže získať o podvodoch množstvo užitočných informácií len tým, že bude sledovať média. Každý rok o podvodoch vychádzajú stovky článkov a desiatky káuz, v ktorých sú popísané rôzne

---

[2] FEROZ, E., H., KWON, T., M., PASTENA, V., S., PARK, K. *The efficacy of red flags in predicting the SEC's targets: an artificial neural networks approach. Intelligent Systems in Accounting*. Finance & Management 9, 2000. s. 145 – 157.

[3] DOBROVIČ, J., GOMBÁR, M., BENKOVÁ, E. *Sustainable development activities aimed at combating tax evasion in Slovakia*. Journal of Security and Sustainability Issues, Volume 6, Issue 4, 2017. s. 761-772.

[4] KORAUŠ, A., DOBROVIČ, J., POLÁK, J., BACKA, S. 2019. *Aspects of the security use of payment card pin code analysed by the methods of multidimensional statistics, Entrepreneurship and Sustainability Issues 6(4): 2017-2036.* [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.4(33)>

[5] MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. *Economic freedom – classification of its level and impact on the economic security.* AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157.

[6] RAVISANKAR, P., RAVI, V., RAGHAVA R., G., BOSE, I. *Detection of financial statement fraud and feature selection using data mining techniques.* Decision Support Systems, č. 50, 2011. s. 491 – 500.

[7] SPATHIS, CH., DOUMPOS, M., ZOPOUNIDIS, C. *Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques.* European Accounting Review, č.11, 2002. s. 509 – 535.

[8] *Association of Certified Fraud Examiners (ACFE).* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.acfe.com/>

podvodné schémy, ich príznaky, rovnako ako spôsoby ich odhalenia. Už len na základe týchto článkov si tak môže manažér vytvoriť určitou predstavu o tom, čo môže jeho spoločnosti hroziť. Týmto by to ale nemalo končiť.

Aby firmy mohli efektívne odhaľovať a vyšetrovať podvody, malo by byť ideálne splnených niekoľko základných faktorov.

Legislatívna podpora – tá by mala vytvoriť rámec ochrany a odmeňovania oznamovateľov nekalého správania, resp. firmy motivovať k vyšetrovaniu podvodov a k zavádzaniu preventívnych opatrení. Zákon o trestnej zodpovednosti právnických osôb jasne vymedzuje právnické osoby, ktoré nesú plnú trestnú zodpovednosť za rozhodovanie svojich vlastníkov, riadiacich a kontrolných orgánov, resp. zamestnancov. V zmysle tohto zákona ako aj Trestného zákona a Trestného poriadku môžu byť postihnutí za rôzne druhy podvodov a nekalého správania, za ktoré im bude hroziť nielen pomerne vysoká peňažná pokuta, ale tiež napríklad prepadnutie majetku, zákaz činnosti alebo zrušenie firmy. Zoznam trestných činov, za ktoré môže byť právnická osoba zodpovedná je uvedený v predmetnom ustanovení. Ide najmä o:

- niektoré majetkové trestné činy,
- trestné činy súvisiace s drogami a omamnými látkami,
- korupčné trestné činy,
- daňové trestné činy,
- trestné činy obchodovania s ľuďmi,
- neoprávnené zamestnávanie,
- trestné činy týkajúce sa životného prostredia a iné trestné činy.

Najprísnejším trestom bude trest zrušenia právnickej osoby, ktorý súd uloží právnickej osobe so sídlo na území Slovenskej republiky, ak jej činnosť bola úplne alebo prevažne využívaná na páchanie trestnej činnosti.

Ďalšími trestami sú trest prepadnutia majetku, trest prepadnutia veci, peňažný trest, trest zákazu činnosti, trest zákazu prijímať dotácie alebo subvencie, trest zákazu prijímať pomoc a podporu poskytovanú z fondov EÚ, trest zákazu účasti vo verejnom obstarávaní, trest zverejnenia odsudzujúceho rozsudku.

V prípade konkurzu alebo likvidácie spoločnosti zákon ustanovuje, že trestná zodpovednosť PO nezaniká vyhlásením konkurzu na takúto spoločnosť, jej vstupom do likvidácie, jej zrušením alebo zavedením nútenej správy.

Prístup vedenia a vlastníkov firmy – aby vedenie firmy uverilo prínosu investícií do detekčného a preventívneho programu, musí si byť predtým vedomé rozsahu hroziacich podvodov a výšky možných škôd. Pokiaľ si toto nebezpečenstvo nedokáže predstaviť, nebude naklonené realizácii prevencie a nákladom s ňou spojeným.

Znalosti – dôležitým faktorom je tiež úroveň znalostí, a to nielen špecialistov zodpovedných za odhaľovanie podvodov, ale tiež bežných zamestnancov firmy. Odhalenie je závislé na schopnosti identifikovať príznaky jeho výskytu, stanovení možných podvodných schém a vytvorení hypotéz priebehu podvodu a jeho možných páchateľov. Nízka úroveň znalostí v tomto procese znemožní odhaliť a dôkladne preveriť nekalé praktiky.

Existencia morálnych vzorov – aby sa firmy a najmä ich zamestnanci odhodlali aktívne postaviť proti podvodom, musí vidieť pozitívny prínos vo svojom správaní. Pre niekoho to bude otázka morálky a cti, postaviť sa jednoznačne proti negatívnemu konaniu. Pre iného racionálne odôvodnenie obavy z ďalšieho fungovania firmy alebo vlastného zamestnania. Stále však zostane veľká časť ľudí, ktorí nebudú mať osobný charakter, odvahu alebo záujem s podvodmi bojovať. V týchto prípadoch ale pomôžu silné vzory. Ľudia, ktorí sa neboja obetovať svoje súkromie a riskovať verejné poníženie. Príklady nebojácnych postojov, aj voči vysoko postaveným manažérom budú ďalších motivovať k nasledovaniu a k zaujatiu

rozhodného postoja proti podvodom. Tak isto aj verejné vystúpenia uznávaných osôb so silnou osobnou integritou a deklarovaním jasného postoja k etickému podnikaniu bude mať silný motivační impulz pre tých, ktorí sú stále ešte nerozhodní a váhajú.

Efektívny detekčný systém – firme by mal umožniť podvody zachytiť a preveriť. Aj v zdanlivo jednoduchom systéme pre zber podnetov o podvodoch sa môžu firmy dopustiť zásadnej chyby. Zavedenie anonymnej linky nemusí stačiť. Pokiaľ firmy nevedia, aké informácie majú od oznamovateľov zbierať a ako ich vyhodnocovať, môže sa stať, že nebudú schopné podvody rozpoznať a ani získať dôkazy o ich existencii. Nepreverovanie podnetov, resp. ich odkladanie, či nezahájenie vyšetrovania oznámených prípadov tak môže viesť k rezignácii vlastných zamestnancov a prestanú používať oznamovací systém. Firmy by sa mali zamerať na dôkladné a najmä pravidelné školenia svojich zamestnancov o spôsobe využívania oznamovacieho systému, deklarovať absolútnu ochranu oznamovateľa a pravidelne informovať o výsledkoch fungovania tohto systému.

Záver

Podvody existujú všade tam, kde sú ľudia, a preto možno konštatovať, že sú rizikom, ktoré sa dá riadiť. Bez obmedzenia na konkrétnu oblasť sa budú vyskytovať najmä tam, kde sa rozhoduje, jedná, pracuje alebo manipuluje s peniazmi, majetkom alebo tiež záväzkami firmy. Preto neprekvapí, že najčastejšou oblasťou výskytu podvodov sú obchod, nákup, zásobovanie, resp. finančné oddelenie spoločností.

K najčastejším externým podvodom vo firmách patrí falošná fakturačná schéma a podvody vychádzajúce z existencie stretu záujmov. Medzi tie interné naopak patrí zneužitie firemných prostriedkov na súkromné účely, resp. sprenevera hotovosti. Spoločnou črtou týchto schém je to nie sú to žiadne sofistikované podvody vyžadujúce zložité účtovné operácie alebo mafiánske spolčovanie mnohých osôb. Často sú spáchané tak, že niekto obíde nefunkčné kontrolné opatrenia, schvaľovacie pravidlá alebo nedokonalý preventívny systém.

Odhalenie vyššie uvedených schém umožňuje niekoľko nástrojov – či už je to whistle-blowing (už spomínaný systém oznamovania, vyhodnocovania podnetov o existencii nekalého správania), preventívne preverovanie obchodných transakcií v účtovníctve, preverovanie obchodných partnerov a zákazníkov, overovanie informácií od záujemcov o zamestnanie, alebo vykonávanie náhodných kontrol. Jednoznačne najčastejším spôsobom odhalenia a tiež najefektívnejším, je informácia od zamestnancov zachytená pomocou whistleblowing systému, čiernej skrinky, e-mailové schránky, prípadne prostredníctvom anonymnej linky. Firmy by sa preto mali zamerať na zavedení a rozvoj takého systému. Nemali by rezignovať na veľký počet vymyslených, nenávistných alebo šikanóznych oznámení, ktoré bude tento systém celkom určíte tiež zaznamenávať. Dôležitá bude schopnosť identifikovať podnety ukazujúce na skutočne závažné problémy vo firme. Zmeny v technickej oblasti, predovšetkým v oblasti informačných a komunikačných technológií kvalitatívne zmenili proces získavania, spracovávania a uchovávania informácií.[9]

Firmy by mali zmeniť svoj zavedený prístup z riešenia dopadov a následkov na ich prevenciu. A tým čo najviac odradiť tých, ktorí podvodné aktivity páchajú. Mali by zaviesť postupy a opatrenia k efektívnemu odhaľovaniu a vyšetrovaniu podvodov. Vedenie firiem, pokiaľ tak ešte neučinilo, by malo dbať na presadzovaní etického myslenia a správania sa vo svojich spoločnostiach a isť ostatným príkladom. Dôležité je tiež zoznamovať zamestnancov, manažérov a vlastníkov firiem s nebezpečím podvodov a možnostiach ich eliminácie.

Predpovede sú, že budúcnosť prinesie nárast výskytu podvodov. Firmy by sa preto mali na toto pripraviť zavedením aspoň základných detekčných a preventívnych postupov. Prevencia

[9] IVANČÍK, R., KAZANSKÝ, R. *Kybernetická vojna, útoky a terorizmus.* In Bezpečnostné fórum 2016, zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016. s. 11-18.

podvodov je určíte výhodnejšia, než riešenie ich následkov. Aj pri nedokonalom kontrolnom systéme, pokiaľ vedenie aktívne šíri etickú kultúru s nulovou toleranciu proti podvodom, propaguje odhaľovanie podvodov, investuje do riadenia rizika podvodov a vzdelávania zamestnancov, takáto spoločnosť bude ďaleko úspešnejšia ako firma s najmodernejším prevenčným systémom bez záujmu svojho vedenia o jeho výstupy. Aktivita a postoj vedenia firmy je v boji s podvodmi kľúčová.

Zoznam použitej literatúry:

1. DOBROVIČ, J., GOMBÁR, M., BENKOVÁ, E. *Sustainable development activities aimed at combating tax evasion in Slovakia, Journal of Security and Sustainability Issues,*Volume 6, Issue 4, 2017, s. 761-772. ISSN: 20297017.
2. FEROZ, E. H., KWON, T. M., PASTENA, V. S., PARK, K. *The efficacy of red flags in predicting the SEC's targets: an artificial neural networks approach.* Intelligent Systems in Accounting, Finance & Management, 9, 2000. s. 145 – 157.
3. Association of Certified Fraud Examiners (ACFE) [online]. [cit. 2019-06-04]. Dostupné na: <https://www.acfe.com/>
4. IVANČÍK, R., KAZANSKÝ, R. Kybernetická vojna, útoky a terorizmus. In *Bezpečnostné fórum 2016*, zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016, s. 11-18. ISBN 978-80-557-1093-8.
5. KALABIS, Z. *Boj bank proti praniu špinavých peňazí*. BIVŠ, 78, 2009. ISBN: 978-80-7265-147-4.
6. KORAUŠ, A., DOBROVIČ, J., POLÁK, J., BACKA, S. 2019. *Aspects of the security use of payment card pin code analysed by the methods of multidimensional statistics, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.4(33)>
7. KORAUŠ, A., DOBROVIČ, J., POLÁK, J., BACKA, S. 2019. *Security aspects: protection of people in connection with the use of personal identification numbers, Journal of Security and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jssi.2019.8.3(3)>
8. KORAUŠ, A., VESELOVSKÁ, S., KELEMEN P. Cyber security as part of the business environment. In Zborník z konferencie Medzinárodné vzťahy 2017: *Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice 30. novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 2017, 1113 s. ISBN 978-80-225-4488-7. ISSN 2585-9412.
9. KORDÍK, M., KURILOVSKÁ, L. 2019. *Content of a Intra Group Compliance Agreement as a risk mitigating factor, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na:<https://doi.org/10.9770/jesi.2019.6.3(10)>
10. MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. *Economic freedom – classification of its level and impact on the economic security.* AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157. ISSN 1804-7890.
11. RAVISANKAR, P., RAVI, V., RAGHAVA R., G., BOSE, I. *Detection of financial statement fraud and feature selection using data mining techniques.* Decision Support Systems, 50 , 2011. s. 491 – 500.
12. SEC - U.S.Security and Exchange Commission. 2013. Annual report to congress on the Dodd.
13. SPATHIS, CH., DOUMPOS, M., ZOPOUNIDIS, C. *Detecting falsified financial statements: a comparative study using multicriteria analysis and multivariate statistical techniques.* European Accounting Review, 11, 2002. s. 509 – 535.

Kontaktné údaje:
doc. Ing. Antonín Korauš, PhD., LL.M, MBA
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
antonín.koraus@minv.sk

Mgr. Pavel Kelemen
Katedra manažmentu
Prešovská univerzita v Prešove
kelemen.pavel@gmail.com

Mgr. Štefan Zachar
Katedra informatuiky a manažmentu
Akadémia PZ v Bratislave
stefan.zachar@minv.sk; stefan.zachar@akademiapz.sk

Procesné riadenie – firemný nástroj bezpečnosti, ochrany majetku a neželanej manipulácie s údajmi

Antonín Korauš, Jozef Polák, Jana Kuchtová

Abstrakt:
Implementácia procesného riadenia do organizácie je interdisciplinárna úloha, ktorá v sebe integruje problematiku ako procesného a projektového riadenia, tak aj zmenového manažmentu. Zvládnutie implementácie predpokladá mať správne nastavený projekt, silného koordinátora a kvalitne zvládnutú komunikáciu a podporu, tak aby sa procesné riadenie mohlo stať súčasťou organizácie aj z bezpečnostného hľadiska a hľadiska ochrany osôb a majetku.
Kľúčové slová:
Ochrana majetku, procesné riadenie, procesne riadená organizácia, administratívna bezpečnosť.

Abstract:
The implementation of process management in an organization is an interdisciplinary task that integrates issues such as process and project management as well as change management. Managing implementation requires a properly set up project, a strong coordinator, and well-communicated communication and support so that process management can be part of the organization, both from a security point of view and with regard to the protection of individuals and property.
Key words:
Property protection, process management, process-controlled organization, administrative security.

Úvod

Procesné riadenie je riadenie firmy takým spôsobom, pri ktorom kľúčovú rolu hrajú podnikové procesy. Riadenie organizácie je postavené na znalostiach procesov, ich meraní, monitoringu a vykonávaní ich neustáleho zlepšovania.[1]

Mládková[2] popisuje procesné riadenie ako systém manažmentu, založený na poznaní, optimalizácii a využití procesov organizácie pre tvorbu hodnôt.

Na procesné riadenie je možné nazerať ako na systémy, postupy, metódy a nástroje zabezpečuje trvalú maximálnu výkonnosť a neustále zlepšovanie podnikových a medzipodnikových procesov, ktoré vychádzajú z jasne formulovanej stratégie organizácie, ktorých cieľom je naplniť stanovené strategické ciele.[3]

Procesným prístupom k riadeniu organizácie dochádza k odkrývaniu procesov a ich následnému pozdvihnutiu nad rámec organizačných štruktúr. Tieto procesy sú vďaka optimalizácii postupne navrhované horizontálne a zároveň sú zbavované činností, ktoré neprinášajú pridanú hodnotu. Proces sa stáva stredobodom pozornosti[4]. Procesný prístup taktiež vytvára podnikovú infraštruktúru a kultúru, ktorá zabezpečuje vykonávanie a zlepšovanie existujúcich procesov a podporu pri tvorbe a zlepšovaní novo vznikajúcich procesov s dôrazom na ochranu a bezpečnosť.

Cieľom procesného riadenia je rozvíjať a optimalizovať jednotlivé činnosti organizácie tak, aby bola schopná čo najefektívnejšie, najúčelnejšie a bezpečne reagovať na požiadavky (rýchlo sa meniace požiadavky) zákazníka .

Podľa Drahotského[5] platia u procesného riadenia určité princípy, ktoré je potrebné aplikovať pri implementácii procesného riadenia do vybraného podniku.

---

[1] ŘEPA, V. *Procesně řízená organizace.* 1. vyd. Praha: Grada, 2012. 301 s.
[2] MLÁDKOVÁ, L., JEDINÁK, P. *Management.* Plzeň: Aleš Čeněk, 2009. 273 s.
[3] ŠMÍDA, F. *Zavádění a rozvoj procesního řízení ve firmě*. 1. vyd. Praha: Grada, 2007. 293 s.
[4] KORAUŠ, A., VESELOVSKÁ, S., KELEMEN P. *Cyber security as part of the business environment*. In Zborník z konferencie Medzinárodné vzťahy 2017: Aktuálne otázky svetovej ekonomiky a politiky, Smolenice 30. novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 2017. 1113 s.
[5] DRAHOTSKÝ, I., ŘEZNÍČEK, B. *Logistika - procesy a jejich řízení.* Brno: Computer Press, 2003. 334 s.

Princípy implementácie:

1. Integrácia a kompresia práce – samostatné práce sú integrované do logických celkov tak, aby boli vykonávané v procesnom tíme. Kompresia práce v tomto kontexte znamená vylúčenie zbytočných činností, doplnenie chýbajúcich a zlepšenie, či inováciu neefektívnych krokov.
2. Delinearizácia práce – práca sa vykonáva v prirodzenom slede a jednotlivé činnosti na seba logicky nadväzujú. Samotný tím rozhoduje o tejto postupnosti.
3. Najvhodnejšie miesto k práci – práca je vykonávaná na mieste, ktoré je najvýhodnejšie bez ohľadu na hranice funkčných celkov (útvarov alebo oddelení) ale s dôrazom na ochranu a bezpečnosť
4. Uplatnenie tímovej práce – realizácia procesov je zabezpečovaná procesnými tímami, ktoré však musia disponovať dostatočnými právomocami. Procesný tím nahradzuje klasickú funkčnú štruktúru organizácie a sústreďuje sa na zabezpečenie správneho priebehu procesu.
5. Procesne zamerané motivácia – motivácia procesného tímu je naviazaná na výsledok procesu a nie na jednotlivé činnosti. Odmeny pre procesný tím závisia od pridanej hodnoty procesu pre zákazníka.
6. Zodpovednosť za proces – v procesnom riadení hrá kľúčovú rolu procesný vlastník, ktorý zodpovedá za celkový priebeh procesu naprieč celou organizáciou.
7. Varianty poňatia procesu – každý proces má niekoľko variant riešení. Voľba príslušnej varianty záleží od typu požiadavky na vstupe, výstupe alebo dostupnosti zdrojov.
8. 3S – samo riadenie, samokontrola a samo organizácia charakterizujú absolútnu autonómiu procesného tímu. Tento princíp je založený na pridelení vysokej úrovne právomocí, ktoré sú späté so zodpovednosťou, kompetentnosťou a znalosťou jednotlivých členov tímu, ktorý takto vytvára priestor na vysokú efektivitu založenú na eliminácii rizík a akcentovaní bezpečnosti.
9. Pružná autonómia procesných tímov – tento princíp je založený na predpoklade, že štruktúra procesných tímov je zostavená tak, aby mohli pružne reagovať novým požiadavkám.
10. Znalostná a informačná bezbariérovosť a dodržiavanie ochrany a bezpečnosti – musí prísť k odstráneniu znalostných a informačných bariér, vytvoreniu ideálneho toku informácií bezpečným spôsobom vo vnútri organizácie. Databázu znalostí je potrebné zdieľať a informačné zdroje centralizovať so zachovaním požadovanej ochrany údajov a informačnej bezpečnosti. Vďaka tomuto princípu dochádza k tomu, že každý zamestnanec vie získať všetky informácie o organizácii a on sám určí, ktoré sú vhodné alebo potrebné pre výkon jeho práce. Toto je zásadný rozdiel oproti funkčnému spôsobu riadenia organizácie.

Procesné riadenie zároveň pomáha organizácii napĺňať legislatívne a auditné požiadavky a tak prispieť k zníženiu rizika[6] penalizácie alebo inej hrozby, ako napríklad úniku údajov, neželanej manipulácie s informáciami a podvodom.

Proces vo všeobecnosti vnímame ako určitý postup alebo priebeh a nadväznosť činností, či už vo výrobe, službách alebo každodenných činnostiach. V odbornej literatúre sa vyskytuje viacero definícii výrazu proces.

Proces je rad vzájomne ovplyvňujúcich sa činností, ktoré pridávajú hodnotu vstupom prostredníctvom využitia zdrojov a premenia ich na výstupy, ktoré sú určené zákazníkom daného procesu. Každý proces má vymedzený svoj začiatok a koniec, svoje rozhranie a väzby na ostatné procesy a činnosti.

[6] KORDÍK, M., KURILOVSKÁ, L. 2019. *Content of a Intra Group Compliance Agreement as a risk mitigating factor.* Entrepreneurship and Sustainability Issues 6(3): 1195-1204. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.3(10) >

V Cambridgskom slovníku je výraz proces vysvetlený ako séria aktivít, ktoré je potrebné vykonať v určitom poradí na dosiahnutie výsledku[7].

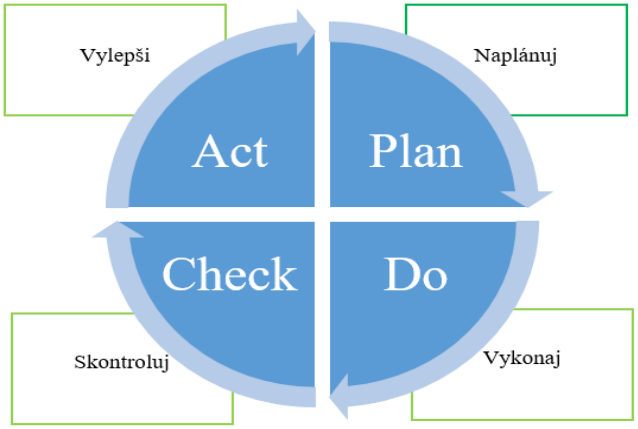
Podnikový proces chápeme ako súhrn činností, ktoré sú medzi sebou prepojené a za vzájomnej interakcie vedia vytvárať hodnotu pre zákazníka daného procesu. Zákazníkov ako používateľov hodnoty, ktorá sa zvýši alebo transformuje do inej podoby označujeme ako interných zákazníkov a zákazníci vystupujúci ako koneční užívatelia výstupu procesu, označujeme ako externých.

Systematické zlepšovanie procesov – DEMINGOV CYKLUS

Keď je proces zmapovaný a optimalizovaný, neznamená to, že sa životný cyklus jeho správy ukončil. Práve naopak, pokiaľ je proces využívaný v organizácii mal by sa systematicky vylepšovať. K tomu je možné vyžiť metódu Demingov cyklus P-D-C-A (Plan – Do – Check – Act), ktorá je vďaka svojej univerzálnosti uplatniteľná vo všetkých typoch organizácii.[8]

Půček[9] popisuje jednotlivé fázy cyklu nasledovne:

1. Fáza P (Plan): Čo a ako chceme zlepšiť. Kvantifikácia problému. Zostavenie plánu na zlepšenie.
2. Fáza D (Do): Realizácia naplánovaného. Transformácia plánovaného do praxe.
3. Fáza C (Check): Zostavenie kontrolného plánu, či sa nám podarilo dosiahnuť požadovaných výsledkov a vykonanie kontroly.
4. Fáza A (Act): V prípade ak kontrolou boli zistené nedostatky, vyhľadávame nové riešenie.



Obr. 1: Demingov cyklus - PDCA
Zdroj: Vlastné spracovanie

Riadenie rizík a bezpečnostná politika organizácie

Dôležitým aspektom bezpečného pôsobenia organizácie na trhu je identifikácia rizík a ich minimalizácia resp. eliminácia. Riziká výrazne ovplyvňujú bezpečnosť a ochranu osôb ale aj majetku. Na riadenie rôznych rizík sa v súčasnosti používa množstvo odlišných metód a techník. Smernice, normy a štandardy sú medzinárodne uznávané nástroje, ktoré môžu pomôcť organizáciám efektívnejšie implementovať tieto techniky.

---

[7] Cambridge dictionary. 2019. [online]. [cit. 2019-06-04]. Dostupné na:<https://dictionary.cambridge.org/dictionary/english/process>

[8] DŽUBÁKOVÁ, M., LICHNEROVÁ, L. *Procesný manažment*. 1. vyd. Bratislava: Ekonóm, 2013. 126 s.

[9] PŮČEK, M., KOCOUREK, S. *Řízení procesů výkonu státní správy: (případová studie Vsetín).* Vyd. 1. Praha: Ministerstvo vnitra České republiky, 2004. 160 s.

Riadenie rizík a bezpečnostná politika organizácie úzko spolu súvisia[10]. Bezpečnostná politika organizácie je základným a východiskovým dokumentom na procesné riadenie a projektovanie každého bezpečnostného systému (aj podniku)[11]. Predstavuje deklaráciu zodpovednosti subjektu bezpečnosti (podniku) za bezpečnosť osôb a ochranu majetku a informácií. Bezpečnostná politika definuje chránené záujmy subjektu a stanovuje systémové zásady alebo tieto záujmy chrániť. Bezpečnostná politika sa vypracováva na základe analýzy bezpečnostných rizík. Bezpečnostná politika vychádza z týchto faktorov (príčiny):

- platné právne normy a ich aplikácia prostredníctvom podnikových normatívnych aktov,
- špecifické bezpečnostné požiadavky na zaistenie bezpečnostných záujmov daného podniku,
- predstavy podniku o požadovanom spôsobe ochrany,
- ekonomické možnosti a ochota financovať zabezpečenie bezpečnosti.

Základné ciele bezpečnostnej politiky

- zabezpečenie ochrany bezpečnosti a aktív podniku,
- vytvoriť podmienky pre spoľahlivé fungovanie podniku,
- zabezpečenie trvalého rozvoja,
- efektívne využitie všetkých zdrojov vyčlenených na zaistenie bezpečnosti podniku,
- vytvorenie systému spoľahlivého a nepretržitého riadenia bezpečnosti podniku,
- stanovenie zodpovednosti za bezpečnosť podnikových aktív.

Vyhláška 453/2007 Z. z. Národného bezpečnostného úradu zo 17. septembra 2007 o administratívnej bezpečnosti podľa § 6 ods. 10 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov upravuje administratívnu bezpečnosť registratúrnych záznamov obsahujúcich utajované skutočnosti a utajovaných skutočností nelistinného charakteru, ak ich povaha dovoľuje nakladať s nimi ako s listinami a ustanovuje opatrenia administratívnej bezpečnosti pre ochranu utajovaných skutočností na hmotných nosičoch so záznamom informácií podľa § 2 písm. c) prvého bodu zákona.

Záver

V súčasnej dobe rýchlych zmien, náročnej legislatívy, globalizácie a silnej konkurencie, sa stále väčším trendom stáva implementácia rámcov procesného riadenia do štruktúr a kultúry organizácií.[12] Zmeny v technickej oblasti, predovšetkým v oblasti informačných a komunikačných technológií kvalitatívne zmenili proces získavania, spracovávania a uchovávania informácií[13]. Procesné riadenie chápe organizáciu ako súbor procesov, ktoré prekračujú hranice organizačných jednotiek v podniku a svoje výstupy dodáva externému alebo internému zákazníkovi. Procesný prístup je chápaný ako esenciálny nástroj pre kontinuálne zlepšovanie firemných procesov a svojou podstatou má pomôcť k získaniu vyššej konkurencieschopnosti, dosahovania vyššej produktivity a efektívnosti. Pre implementáciu týchto zmien je potrebné porozumieť princípom a zásadám procesného riadenia

[10] KORAUŠ, A., GOMBÁR, M., KELEMEN, P., BACKA, S. 2019. *Awareness of security risks associated with payment systems analyzed by the methods of multidimensional statistics*. Journal of Security and Sustainability Issues 8(4): 687-703. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jssi.2019.8.4(12) >

[11] KORAUŠ, A., GOMBÁR, M., KELEMEN, P., BACKA, S. 2019. *Using quantitative methods to identify insecurity due to unusual business operations*. Entrepreneurship and Sustainability Issues 6(3): 1101-1112. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.3(3)>

[12] MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. *Economic freedom – classification of its level and impact on the economic security.* AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157.

[13] IVANČÍK, R., KAZANSKÝ, R *Kybernetická vojna, útoky a terorizmus.* In Bezpečnostné fórum 2016, zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016. s. 11-18.

a zakomponovať ich do vybraného podniku spôsobom plnohodnotne rešpektujúcim bezpečnosť a ochranu osôb a majetku.

Zoznam použitej literatúry:

1. Cambridge dictionary. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://dictionary.cambridge.org/dictionary/english/process>
2. DRAHOTSKÝ, I., ŘEZNÍČEK, B. *Logistika - procesy a jejich řízení.* Brno: Computer Press, 2003. 334 s. ISBN 80-7226-521-0.
3. DŽUBÁKOVÁ, M.; LICHNEROVÁ, L. *Procesný manažment*. 1. vyd. Bratislava : Ekonóm, 2012. 126 s. ISBN 978-80-225-3379-9. .
4. IVANČÍK, R., KAZANSKÝ, R. Kybernetická vojna, útoky a terorizmus. In *Bezpečnostné fórum 2016*, zborník vedeckých prác z 9. medzinárodnej vedeckej konferencie. Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, zv. 1, 2016, s. 11-18. ISBN 978-80-557-1093-8.
5. KORAUŠ, A., VESELOVSKÁ, S., KELEMEN P. Cyber security as part of the business environment. In Zborník z konferencie Medzinárodné vzťahy 2017: *Aktuálne otázky svetovej ekonomiky a politiky*, Smolenice 30. novembra - 1. Decembra 2017, Vydavateľstvo Ekonóm, 2017, 1113 s. ISBN 978-80-225-4488-7. ISSN 2585-9412.
6. KORAUŠ, A., GOMBÁR, M., KELEMEN, P., BACKA, S. 2019. *Awareness of security risks associated with payment systems analyzed by the methods of multidimensional statistics*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jssi.2019.8.4(12) >
7. KORAUŠ, A., GOMBÁR, M., KELEMEN, P., BACKA, S. 2019. *Using quantitative methods to identify insecurity due to unusual business operations, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.3(3)>
8. KORDÍK, M., KURILOVSKÁ, L. 2019. *Content of a Intra Group Compliance Agreement as a risk mitigating factor, Entrepreneurship and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jesi.2019.6.3(10) >
9. MLÁDKOVÁ, L., JEDINÁK, P. *Management.* Plzeň: Aleš Čeněk, 2009. 273s. ISBN 978-807-3802-301.
10. MURA, L., DAŇOVÁ, M., VAVREK, R., DÚBRAVSKÁ, M. Economic freedom – classification of its level and impact on the economic security. AD ALTA-Journal of Interdisciplinary Research, Vol. 7, No. 2, 2017. s. 154 – 157. ISSN 1804-7890.
11. PŮČEK, M., KOCOUREK, S. *Řízení procesů výkonu státní správy: (případová studie Vsetín)*. Vyd. 1. Praha: Ministerstvo vnitra České republiky, 2004. 160 s. ISBN 80-239-4098-8.
12. ŘEPA, V. *Procesně řízená organizace.* 1. vyd. Praha: Grada, 2012. 301 s. ISBN 978-80-247-4128-4.
13. ŠMÍDA, F. *Zavádění a rozvoj procesního řízení ve firmě*. 1. vyd. Praha: Grada, 2007. 293 s. ISBN 978-80-247-1679-4.
14. Vyhláška 453/2007 Z. z. Národného bezpečnostného úradu zo 17. septembra 2007 o administratívnej bezpečnosti.

Kontaktné údaje:

doc. Ing. Antonín Korauš, PhD., LL.M, MBA
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
antonín.koraus@minv.sk

Ing. Jozef Polák
Fakulta manažmentu
Prešovská univerzita v Prešove
jozefpolak64@gmail.com

Mgr. Jana Kuchtová
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
jana.kuchtova@minv.sk

Ochrana osobných údajov

Výsledky výskumov vykonaných vo Francúzsku, na Slovensku a v Českej republike

Matej Kostrec

Abstrakt:
Ochrana osobných údajov a súkromia v informačných systémoch je vysoko aktuálna téma, pretože spracovanie informácií a využívanie Internetu je celosvetovou doménou, ktorá neberie ohľad na administratívne členenie štátov. Z tohto dôvodu je nevyhnutné prijať a zosúladiť legislatívne opatrenia, ktoré by zvýšili úroveň ochrany osobných údajov naprieč celou planétou. Jedným z takýchto opatrení je aj Európske nariadenie o ochrane osobných údajov – GDPR, ktorého znenie zaväzuje členské štáty EÚ a všetky inštitúcie a jednotlivcov, sídliacich na ich území, dodržiavať striktne pravidlá na ochranu dát zaznamenaných a spracúvaných v ich informačných systémoch, ktoré sú ustanovené týmto nariadením. Vzhľadom na skutočnosť, že už uplynul skoro rok od nadobudnutia účinnosti nariadenia GDPR, cieľom tohto príspevku je zmapovanie situácie v povedomí občanov EÚ o ochrane osobných údajov a rizikách spojených s ich neoprávneným získavaním a spracúvaním po zavedení GDPR do praxe. Formou on-line dotazníka, ktorý bol vypĺňaný respondentmi vo Francúzsku, v Slovenskej republike a v Českej republike, bol vykonaný výskum, ktorého výsledky sú v príspevku vyhodnotené za jednotlivé krajiny, ale aj porovnané navzájom medzi týmito krajinami.
Kľúčové slová:
GDPR – Európske nariadenie o ochrane osobných údajov; výskum; krajiny výskumu – Francúzsko, Česká republika, Slovenská republika; zneužitie osobných údajov; riziká; dôverné informácie; sociálne siete.

Abstract:
The protection of personal data and privacy in information systems is a highly topical issue, as the processing of information and the use of the Internet is a worldwide domain that does not respect the administrative division of states. For this reason, it is necessary to adopt and harmonize legislative measures to increase the level of protection of personal data across the planet. One of such measure is the General Data Protection Regulation - the GDPR, whose wording obliges EU Member States and all institutions and individuals residing in their territory to comply strictly with the rules on data protection recorded and processed in their information systems which are established by this Regulation. In view of the fact that nearly a year has passed since the entry into force of the GDPR Regulation, this contribution focuses on mapping EU citizens' awareness of the protection of personal data and the risks associated with their unauthorized acquisition and processing following the implementation of the GDPR. In the form of an on-line questionnaire, which was filled in by respondents in France, the Slovak Republic and the Czech Republic, research was carried out, the results of which are evaluated for each country as well as compared to each other.
Key words:
GDPR – General Data Protection Regulation; research; countries of research – France, Czech Republic, Slovak Republic; misuse of personal data; risks; confidential information; social networks.

Úvod

Európske nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation) nadobudlo účinnosť 25. mája 2018. Jeho cieľom je ochrana digitálneho práva všetkých občanov EÚ. Pretože ochrana fyzických osôb v súvislosti so spracovávaním osobných údajov patrí medzi základné ľudské práva, upravuje toto nariadenie rešpektovanie súkromného a rodinného života a uchovávanie citlivých informácií o každom občanovi EÚ. Nariadenie sa týka každého, kto zhromažďuje a spracováva osobné údaje Európanov, vrátane spoločností a inštitúcií mimo EÚ, ktoré pôsobia na našom trhu. Nariadenie je platné pre firmy, inštitúcie, jednotlivcov – zamestnancov, zákazníkov, klientov aj dodávateľov naprieč všetkými odvetviami. Rovnako sa týka aj tých, ktorí analyzujú chovanie užívateľov webov a aplikácií.[1] Ako ovplyvnilo nariadenie GDPR povedomie občanov o ochrane osobných údajov a ich právach a povinnostiach z neho vyplývajúcich? Odpoveď na túto otázku sme sa pokúsili zmapovať formou výskumu prostredníctvom on-line dotazníka v troch krajinách EÚ.

[1] *Čo je GDPR?* 2019. [online]. [cit. 2019-0-04]. Dostupné na: <https://gdpr-slovensko.sk/co-je-gdpr/>

Otázky položené respondentom výskumu:

1. Povedali by ste, že dnes ste viac alebo menej, alebo ani viac, ani menej citliví na otázku ochrany vašich osobných údajov ako v predchádzajúcich rokoch?
   (Osobné údaje sú údaje, ktoré priamo identifikujú osobu (napr. meno, priezvisko, telefónne číslo, adresa, bankové údaje, atď.) alebo nepriamo (z GPS súradníc pohybu príslušnej osoby, atď.))
2. Povedali by ste, že vo všeobecnosti je ochrana údajov, ktoré umožňujú identifikovať osobu dostatočná alebo nedostatočná?
3. Počuli ste už niekedy o GDPR, Európskom nariadení o ochrane osobných údajov?
4. Povedali by ste, že rozumiete dobre alebo nerozumiete tomu, čo GDPR zmenilo v oblasti ochrany osobných údajov, práv občanov a spotrebiteľov, povinnosti spoločností a inštitúcií?
   (Otázka bola položená len respondentom, ktorí na otázku č. 3 odpovedali kladne.)
5. Zaznamenali ste už niekedy akékoľvek zneužitie v používaní vašich osobných údajov?
6. Aké boli tieto zneužitia pri používaní vašich osobných údajov, ktoré ste zaznamenali?
   (Otázka bola položená len respondentom, ktorí na otázku č. 5 odpovedali kladne.)
   Výber z nasledujúcich možností:
   a) Prenos vašich osobných údajov (adresa, telefónne číslo, e-mail atď.) tretím stranám bez vášho súhlasu (na komerčné účely).
   b) Online publikovanie osobných údajov bez vášho súhlasu organizáciou alebo osobou.
   c) Publikovanie vašich osobných údajov v súbore, ktorý vás poškodzuje (napr. neplatiči, exekúcie, policajné záznamy, spravodajské súbory, atď.)
   d) Nadmerný dohľad na pracovisku (napr. monitorovanie videokamerou, geolokácia vášho vozidla, zaznamenávanie vašich telefonických rozhovorov, atď.)
   e) Iný druh zneužitia.
7. Pre každý z nasledujúcich prvkov povedzte, či vás znepokojuje viac, menej alebo ani viac, ani menej ako pred niekoľkými rokmi?
   a) Riziko zneužitia vašich bankových údajov.
   b) Riziko vidieť dôverné informácie o vašom živote zverejnené na internete v dôsledku chyby alebo zneužitia (intímnych fotografií, choroby, súkromnej konverzácie, atď.)
   c) Používanie vašich osobných údajov prostredníctvom sociálnych sietí.
   d) Skutočnosť, že informácie, ktoré poškodzujú vašu povesť, sú zámerne rozširované jednotlivcom alebo organizáciou.
   e) Skutočnosť, že vaše údaje budú používané politickými stranami, zvolenými zástupcami alebo kandidátmi.
   f) Skutočnosť, že vám boli poskytnuté personalizované informácie podľa vášho správania na sociálnych sieťach, napr.: na Facebooku.
   g) Prítomnosť cielených reklám na vami navštevovaných webových stránkach (podľa histórie vášho vyhľadávania, podľa vami navštívených stránok, atď.).
   h) Tvorba štátnych policajných súborov pre bezpečnostné účely.

Výskum vykonaný vo Francúzsku

Výskum bol vykonaný na vzorke 1003 osôb, reprezentujúcich populáciu vo veku 18 rokov a viac. Reprezentatívnosť vzorky bola zabezpečená metódou kvót (pohlavie, vek, zamestnanie respondenta) po stratifikácii podľa regiónu a kategórie aglomerácie. Výskum prebiehal v termíne od 30. do 31. októbra 2018 formou on-line dotazníka. Predmetom výskumu je povedomie o ochrane osobných údajov, to znamená o údajoch, ktoré priamo identifikujú

osobu (napr. meno, priezvisko, telefónne číslo, adresa, bankové údaje, atď. .) alebo ju identifikujú nepriamo (z GPS súradníc pohybu príslušnej osoby, a pod.).

Výskum vykonaný na Slovensku

Výskum bol vykonaný na vzorke 105 osôb, ktoré rovnako ako vo Francúzsku reprezentujú populáciu vo veku od 18 do 50 rokov. Reprezentatívnosť vzorky bola taktiež zabezpečená metódou kvót (pohlavie, vek, zamestnanie respondenta) po stratifikácii podľa regiónu a kategórie aglomerácie. Výskum prebiehal v termíne od 11. do 15. marca 2019 formou on-line dotazníka. Predmet výskumu bol rovnaký ako vo Francúzsku, t. j. zistenie povedomia respondentov o ochrane osobných údajov, pričom zámerom výskumu je porovnanie stavu vo Francúzsku, na Slovensku (SR) a v Českej republike (ČR). Počet respondentov výskumu 105 osôb na Slovensku bol zvolený proporcionálne k vzorke 1003 osôb výskumu, vykonaného vo Francúzsku, aby bol pomer počtu kompatibilný vzhľadom na celkový počet obyvateľov v jednotlivých krajinách. Počet respondentov vo Francúzsku predstavuje 10-násobok počtu respondentov na Slovensku, rovnako ako počet obyvateľov vo Francúzsku (cca 63 miliónov)[2] predstavuje 10-násobok počtu obyvateľov na Slovensku (cca 5,47 miliónov)[3]. Percentuálne vyjadrenie odpovedí na jednotlivé otázky je teda jednoznačne porovnateľné.

Výskum vykonaný v Českej republike

Výskum bol vykonaný na vzorke 211 osôb, ktoré rovnako ako vo Francúzsku a na Slovensku reprezentujú populáciu vo veku 18 a viac rokov. Reprezentatívnosť vzorky bola taktiež zabezpečená metódou kvót (pohlavie, vek, zamestnanie respondenta) po stratifikácii podľa regiónu a kategórie aglomerácie. Výskum prebiehal v termíne od 18. do 20. marca 2019 formou on-line dotazníka. Predmet výskumu bol rovnaký ako vo vyššie uvedených dvoch krajinách, t. j. zistenie povedomia respondentov o ochrane osobných údajov. Počet respondentov výskumu 211 osôb v Českej republike bol zvolený proporcionálne k vzorke 1003 osôb výskumu vykonaného vo Francúzsku, a k vzorke 105 osôb výskumu zrealizovaného na Slovensku tak, aby bol pomer počtu kompatibilný vzhľadom na celkový počet obyvateľov v jednotlivých krajinách. Počet respondentov v Českej republike predstavuje dvojnásobok počtu respondentov na Slovensku a 5-násobok počtu respondentov vo Francúzsku, čo je približne rovnaký pomer medzi počtami obyvateľov v jednotlivých krajinách.[4] Percentuálne vyjadrenie odpovedí na jednotlivé otázky je teda jednoznačne porovnateľné.

[2] *Európska únia*. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://sk.wikipedia.org/wiki/Európska_únia>

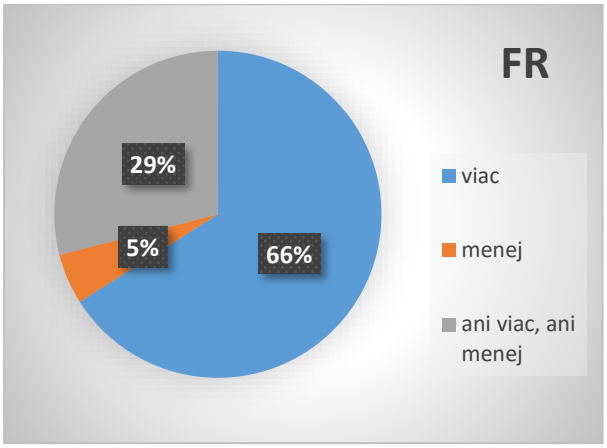
[3] *Európska únia*. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://sk.wikipedia.org/wiki/Európska_únia>

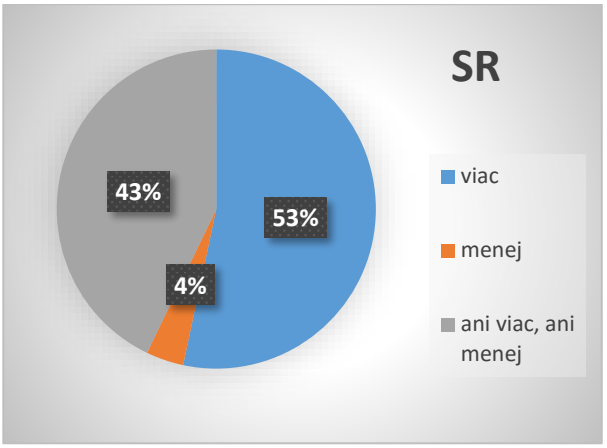
[4] Počet obyvateľov Francúzska je cca 63 miliónov, Slovenskej republiky cca 5,5 milióna a Českej republiky cca 10,5 milióna. Pomer obyvateľov medzi jednotlivými krajinami je teda daný nasledujúcimi vzťahmi:
Francúzsko – Slovensko = 10:1,
Francúzsko – Česká republika = 5:1,
Česká republika – Slovensko = 2:1.

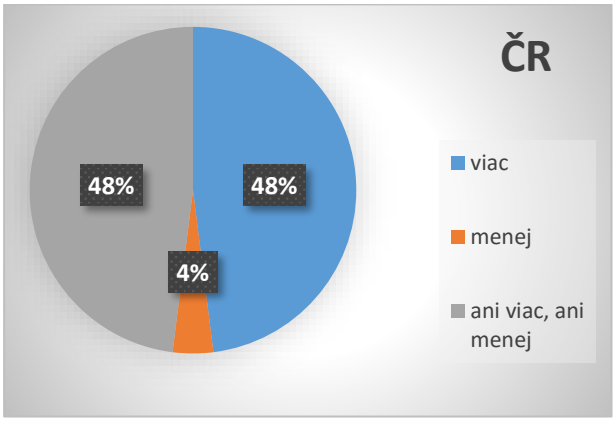
Hodnotenie výskumu

Otázka č. 1

Povedali by ste, že dnes ste viac alebo menej, alebo ani viac, ani menej citliví na otázku ochrany vašich osobných údajov ako v predchádzajúcich rokoch?







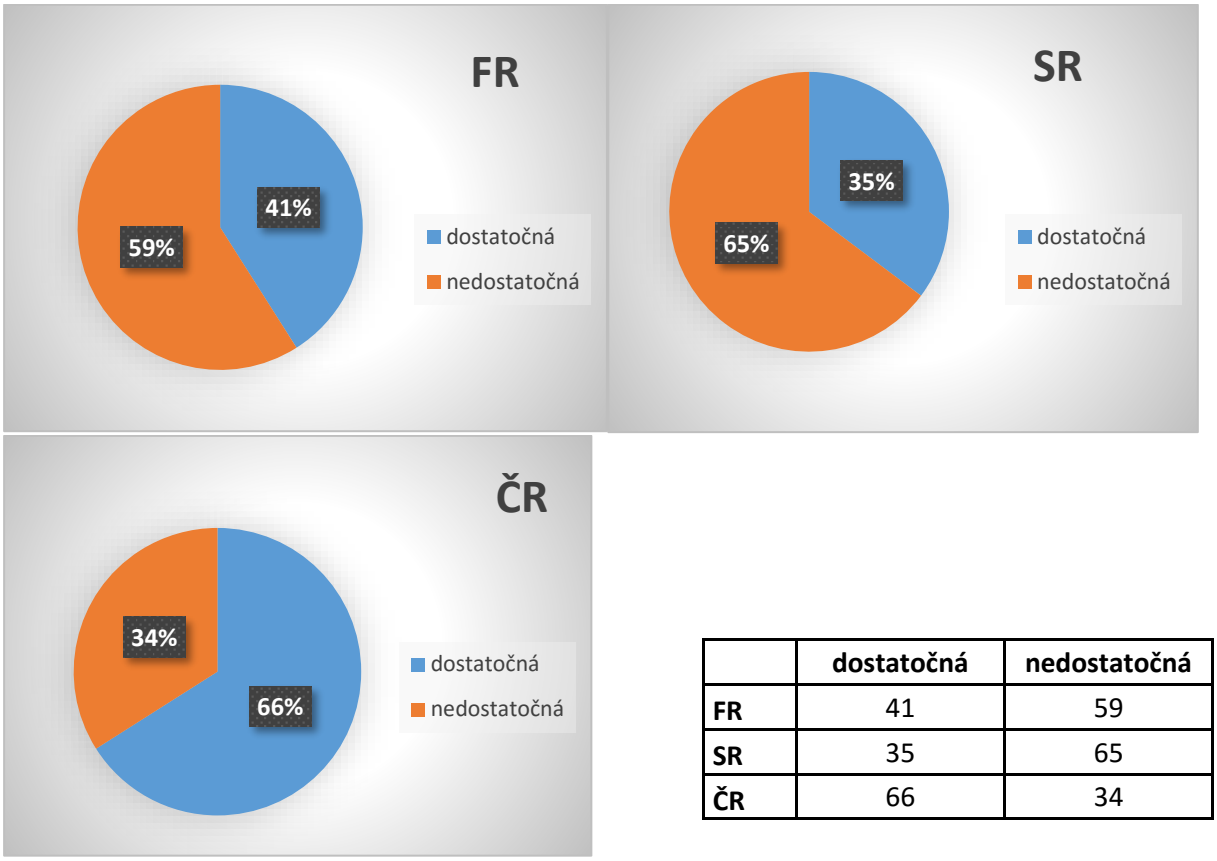
	viac	menej	ani viac, ani menej
FR	66	5	29
SR	53	4	43
ČR	48	4	48

Obr. 1: Grafy a tabuľka s vyhodnotením otázky č.1
Zdroj: vlastné spracovanie

Po nadobudnutí účinnosti Európskeho nariadenia o ochrane osobných údajov GDPR sa zdá, že až 2/3 respondentov výskumu vo Francúzsku je citlivejších a viac sa zaujíma o výskyt a spracúvanie svojich osobných údajov v rôznych informačných systémoch. Ich podiel k respondentom v ČR je až o 13% vyšší a v SR dokonca o 18% vyšší. Francúzi teda reagujú citlivejšie na práva, ktoré im umožňujú lepšie si chrániť svoje súkromie, prípadne dožadovať sa ochrany svojich osobných údajov aj formou súdnych sporov vedených voči firmám a inštitúciám, ktoré porušujú tieto ich práva. Naopak v SR si viac ako polovica respondentov a v ČR skoro polovica respondentov myslí, že nariadenie GDPR nemá náležitý dopad na zvýšenie ochrany osobných údajov.

Otázka č. 2

Povedali by ste, že vo všeobecnosti je ochrana údajov, ktoré umožňujú identifikovať osobu dostatočná alebo nedostatočná?



	dostatočná	nedostatočná
FR	41	59
SR	35	65
ČR	66	34

Obr. 2: Grafy a tabuľka s vyhodnotením otázky č.2
Zdroj: vlastné spracovanie

Aj napriek implementácii GDPR do praxe vo všetkých členských štátoch EÚ už viac ako polroka pred realizáciou výskumu, si viac ako polovica respondentov vo Francúzsku a až 2/3 respondentov v SR myslí, že ochrana osobných údajov je nedostatočná. Nedôvera občanov voči účinnosti nových pravidiel pre firmy a inštitúcie vyplýva aj zo skutočnosti, že napríklad napriek početným hláseniam o porušení týchto pravidiel príslušnému zodpovednému orgánu vo Francúzsku - CNIL[5], doposiaľ neboli uložené žiadne postihy, pretože náročnosť

[5] CNIL - Národná komisia pre informatiku a slobody, vo Francúzsku. Komisia CNIL je zodpovedná za zabezpečenie toho, aby informačné technológie slúžili občanovi a neporušovali ľudskú identitu, ľudské práva, súkromie, individuálne ani verejné slobody. CNIL dostala 742 oznámení o porušeniach už za prvé štyri mesiace od nadobudnutia účinnosti GDPR (od 25. mája do 1. októbra), ktoré sa týkajú údajov 33 727 384 osôb nachádzajúcich sa vo Francúzsku alebo v iných krajinách EÚ.
Tieto porušenia sa týkajú:
porušenia dôvernosti údajov (695),
a/alebo zníženia dostupnosti (71),
a/alebo narušenia integrity (50),
pričom je zrejmé, že niektoré oznámenia sa týkali súčasne viacerých z vyššie uvedených alternatív.
Zdroj: CNIL. *Infographie Bilan: 4 mois de RGPD en chiffres - Notification de violation des données.* 2018. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.cnil.fr/fr/infographie-bilan-4-mois-de-rgpd-en-chiffres notification-de-violation-des-donnees>

vyšetrovania týchto hlásení a priebeh konania voči predmetným firmám, ktorým bolo dokázané porušenie GDPR, je veľmi zdĺhavý a náročný proces. Zdá sa, že v SR je situácia ešte komplikovanejšia a dôvera občanov v oblasti domáhania sa svojich práv a dlhotrvajúce súdne konania ich odrádzajú od procesu podávania sťažností v oblasti porušovania ochrany osobných údajov. Zaujímavým výsledkom výskumu sú odpovede respondentov v ČR, kde až 66% respondentov si myslí, že ochrana osobných údajov v informačných systémoch je dostatočná.

Otázka č. 3

Počuli ste už niekedy o GDPR, Európskom nariadení o ochrane osobných údajov?

	áno	nie
FR	65	35
SR	76	24
ČR	96	4

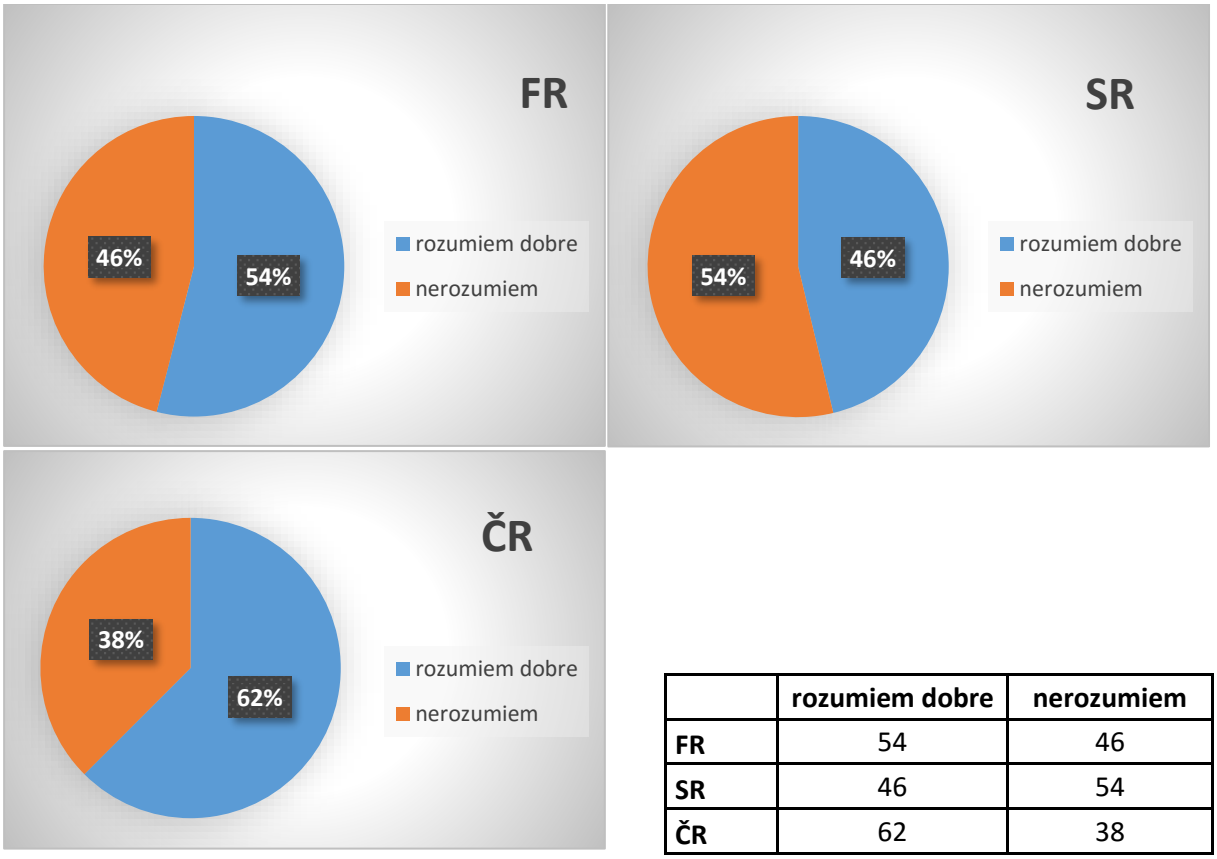
Obr. 3: Grafy a tabuľka s vyhodnotením otázky č.3
Zdroj: vlastné spracovanie

Prekvapujúce je vysoké percento (až 96%) respondentov v ČR, ktorí už počuli, resp. sú oboznámení s GDPR. Je zrejmé, že záujem občanov o oboznámenie sa s legislatívnymi úpravami je v ČR o 20%, resp. 30% vyšší ako v SR, resp. vo Francúzsku. Aké je však reálne chápanie obsahu a dosahu týchto legislatívnych textov si uvedieme v reakcii na odpovede na nasledujúcu otázku výskumu.

Otázka č. 4

Povedali by ste, že rozumiete dobre alebo nerozumiete tomu, čo GDPR zmenilo v oblasti ochrany osobných údajov, práv občanov a spotrebiteľov, povinnosti spoločností a inštitúcií?

(Otázka bola položená len respondentom, ktorí na otázku č. 3 odpovedali kladne.)



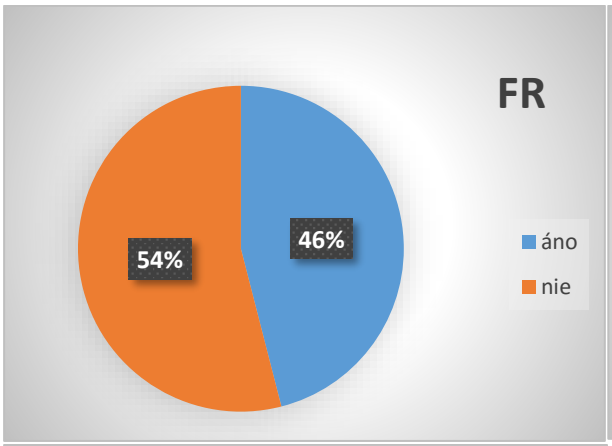
	rozumiem dobre	nerozumiem
FR	54	46
SR	46	54
ČR	62	38

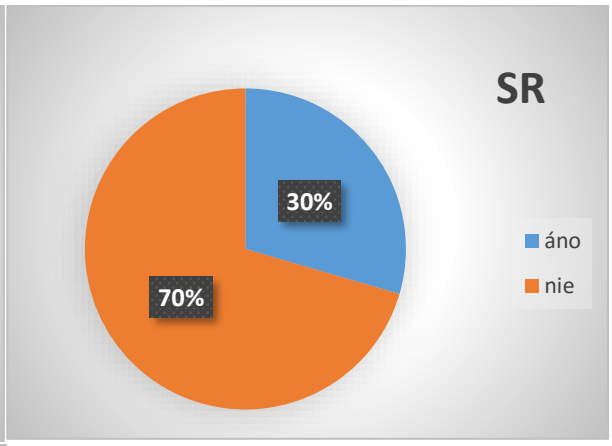
Obr. 4: Grafy a tabuľka s vyhodnotením otázky č.4
Zdroj: vlastné spracovanie

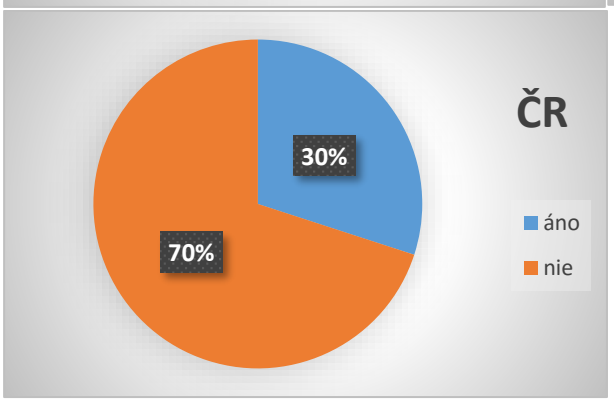
Na túto otázku odpovedali len respondenti, ktorí na predchádzajúcu otázku, či už niekedy počuli o GDPR, odpovedali kladne. Aj napriek vysokému percentu respondentov v ČR, ktorí už počuli o Európskom nariadení o ochrane osobných údajov, až viac ako 1/3 ich nerozumie obsahu GDPR a právam a povinnostiam, ktoré z tohto nariadenia vyplývajú. Približne polovica respondentov výskumu v SR a vo Francúzsku sa taktiež vyjadrila, že obsahu a dosahu GDPR pre firmy i jednotlivcov nerozumie. Z výsledkov odpovedí na túto otázku je zrejmé, že je nevyhnutné zabezpečiť lepšiu informovanosť a osvetu obyvateľov všetkých troch krajín o zmenách vyplývajúcich z GDPR v oblasti ochrany osobných údajov, práv občanov a spotrebiteľov a povinností spoločností a inštitúcií.

Otázka č. 5

Zaznamenali ste už niekedy akékoľvek zneužitie v používaní vašich osobných údajov?







	áno	nie
FR	46	54
SR	30	70
ČR	30	70

Obr. 5: Grafy a tabuľka s vyhodnotením otázky č.5
Zdroj: vlastné spracovanie

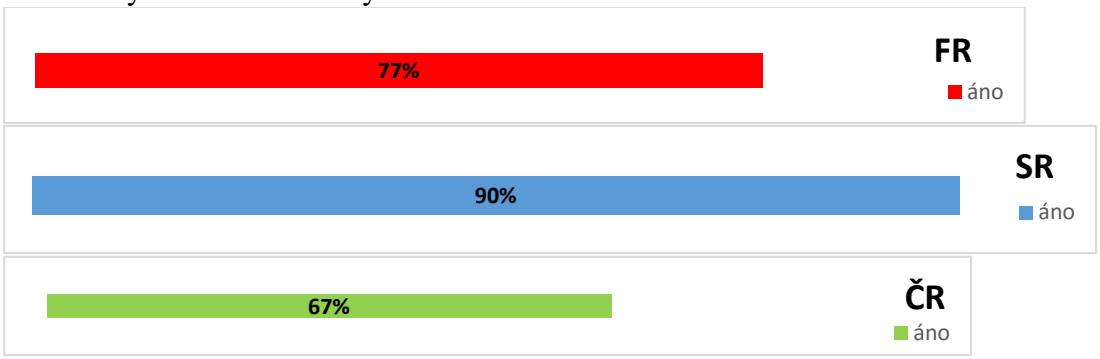
V reakcii na odpovede na túto otázku je nevyhnutné poznamenať, že viac ako 2/3 respondentov zo SR a ČR a viac ako polovica respondentov výskumu vo Francúzsku si neuvedomuje, kde všade sú ich osobné údaje spracúvané, aj napriek tomu, že elektronizácia obchodu, bankových operácií, rezervačných informačných systémov, komunikácia prostredníctvom sociálnych sietí a iných komunikačných nástrojov Internetu, atď., je už samozrejmosťou pre väčšinu občanov vo všetkých troch krajinách. Ich informovanosť o spôsobe získania a spracúvania ich osobných údajov, ako aj nevyhnutnosti poskytovania ich súhlasu udeleného vopred pred spracúvaním ich údajov, je zdá sa veľmi nízka. Na túto otázku kladne, t. j. zaznamenali zneužitie svojich osobných údajov, odpovedala len asi polovica respondentov vo Francúzsku a asi 1/3 respondentov v SR a ČR. V nasledujúcej otázke si detailnejšie rozoberieme spôsoby zneužití zaznamenaných výhradne týmito respondentmi.

Otázka č. 6

Aké boli tieto zneužitia pri používaní vašich osobných údajov, ktoré ste zaznamenali? (Otázka bola položená len respondentom, ktorí na otázku č. 5 odpovedali kladne.)

a) Prenos vašich osobných údajov (adresa, telefónne číslo, e-mail atď.) tretím stranám bez vášho súhlasu (na komerčné účely).

Graf 1: Vyhodnotenie otázky č.6a

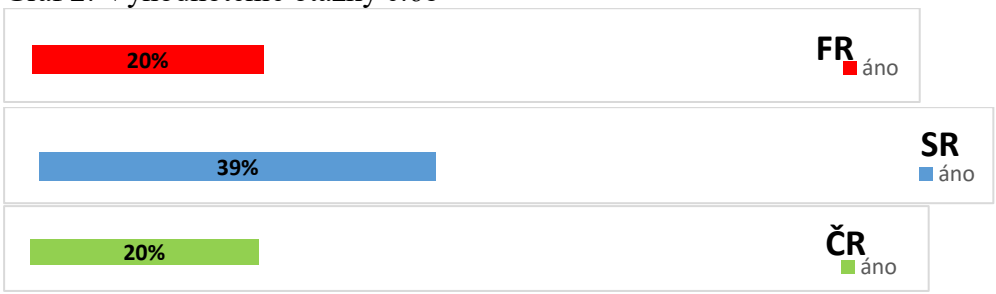


Zdroj: vlastné spracovanie

Táto oblasť zneužitia pri používaní osobných údajov je indikovaná najvyšším percentom vo všetkých troch krajinách. Je to pravdepodobné aj z toho dôvodu, že sú ľudia čoraz častejšie obťažovaní rôznymi nevyžiadanými komerčnými telefonátmi, reklamami, vernostnými kartami, a pod. Je teda najviditeľnejšia, resp. najrozšírenejšia.

b) Online publikovanie osobných údajov bez vášho súhlasu organizáciou alebo osobou.

Graf 2: Vyhodnotenie otázky č.6b

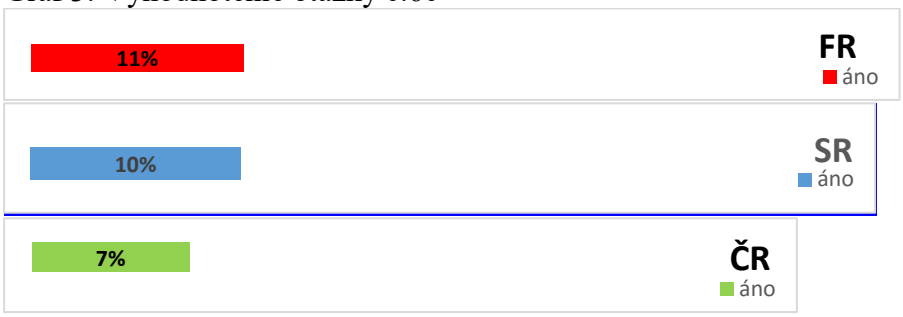


Zdroj: vlastné spracovanie

Táto oblasť tvorí tiež dosť rozšírenú obchodnú a komunikačnú prezentáciu osobných údajov, najmä pri používaní nechránených profilov na sociálnych sieťach, ale aj pri rôznych súťažiach organizovaných najmä pre reklamné a propagačné účely.

c) Publikovanie vašich osobných údajov v súbore, ktorý vás poškodzuje (napr. neplatiči, exekúcie, policajné záznamy, spravodajské súbory, atď.)

Graf 3: Vyhodnotenie otázky č.6c

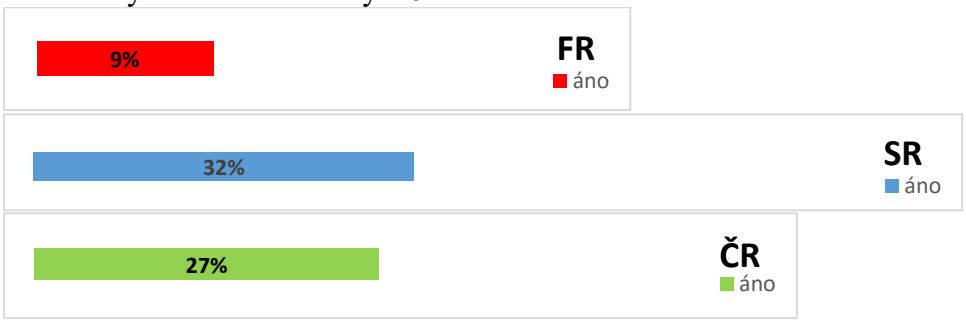


Zdroj: vlastné spracovanie

Táto oblasť publikovania osobných údajov je špecifickou oblasťou, a to z dôvodu evidencie nekalých, resp. problematických situácií a aktivít konkrétnych subjektov, za účelom predchádzania ďalším takýmto skutkom. Slúži najmä pre informovanosť verejnosti. Samozrejme vedenie takýchto registrov a databáz prináleží výhradne do kompetencie k tomu relevantných inštitúcií. Inými, k tomu neurčenými, subjektami je toto publikovanie nelegálne.

d) Nadmerný dohľad na pracovisku (napr. monitorovanie videokamerou, geolokácia vášho vozidla, zaznamenávanie vašich telefonických rozhovorov, atď.)

Graf 4: Vyhodnotenie otázky č.6d

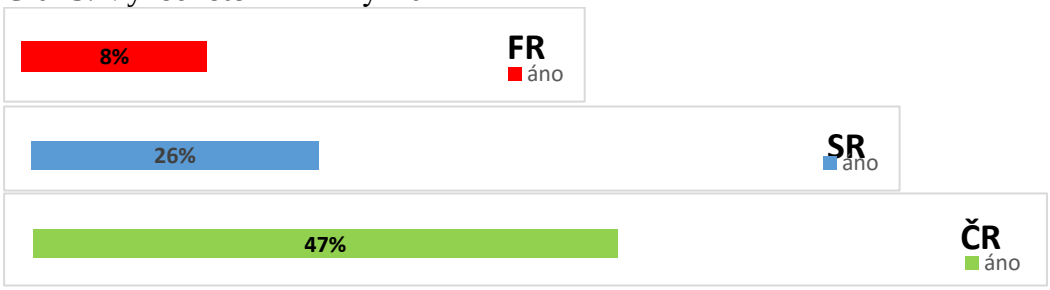


Zdroj: vlastné spracovanie

Nadmerné monitorovanie na pracovisku zaznamenávajú hlavne respondenti výskumu v SR a ČR (približne 1/3). Bližšie príčiny neboli predmetom výskumu, ale je možné, že táto obava respondentov v oboch post-komunistických krajinách je daná napríklad aj dedičstvom postupov praktikovaných v minulosti.

e) Iný druh zneužitia.

Graf 5: Vyhodnotenie otázky č.6e



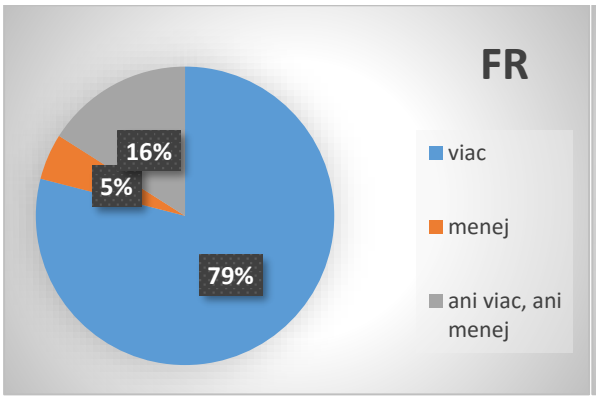
Zdroj: vlastné spracovanie

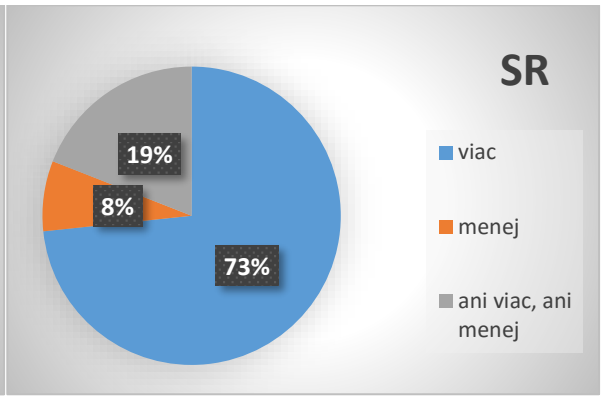
Zarážajúce je vysoké percento (až 47%) respondentov výskumu v SR, ktorí síce uvádzajú, že zaznamenali zneužitie osobných údajov, ale nešpecifikujú konkrétny spôsob. Je možné, že sa v niektorých prípadoch jedná skôr o domnienku, ako o skutočne zaznamenané zneužitie.

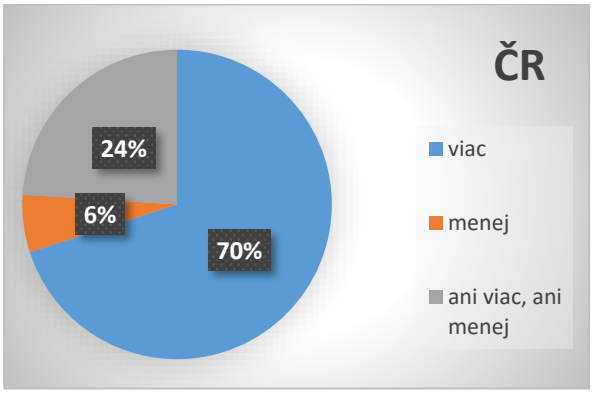
Otázka č. 7

Pre každý z nasledujúcich prvkov by ste povedali, že vás znepokojuje viac, menej alebo ani viac, ani menej ako pred niekoľkými rokmi?

a) Riziko zneužitia vašich bankových údajov.





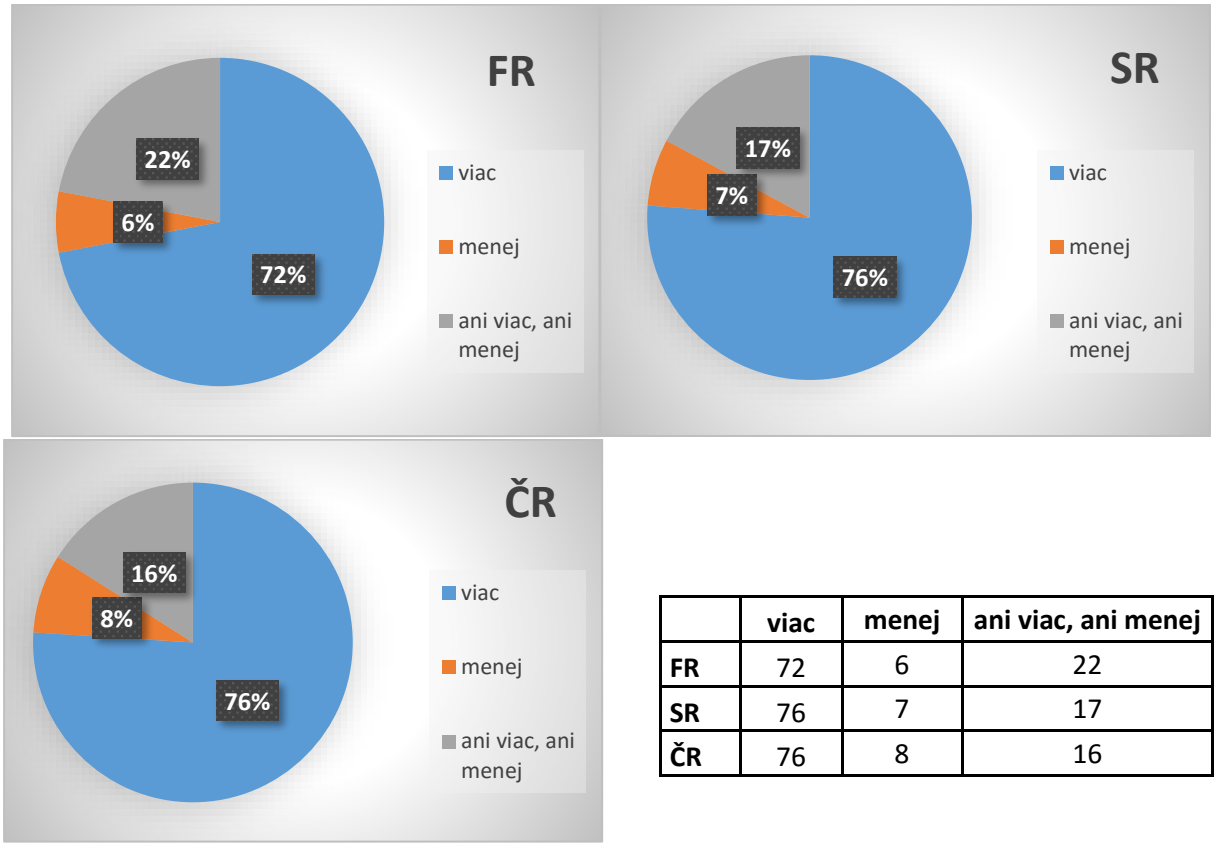


	viac	menej	ani viac, ani menej
FR	79	5	16
SR	73	8	19
ČR	70	6	24

Obr. 6: Grafy a tabuľka s vyhodnotením otázky č.7a
Zdroj: vlastné spracovanie

Najčastejšia obava respondentov (až 2/3) vo všetkých troch krajinách je možnosť existencie rizika zneužitia bankových údajov. Je to naozaj kritická oblasť, pretože v bankových inštitúciách majú ľudia uložené svoje finančné prostriedky, na ktorých sú životne závislí. Preto je oblasť ochrany osobných/bankových údajov pre nich existenčne dôležitá.

b) Riziko vidieť dôverné informácie o vašom živote zverejnené na internete v dôsledku chyby alebo zneužitia (intímnych fotografií, choroby, súkromnej konverzácie, atď.)

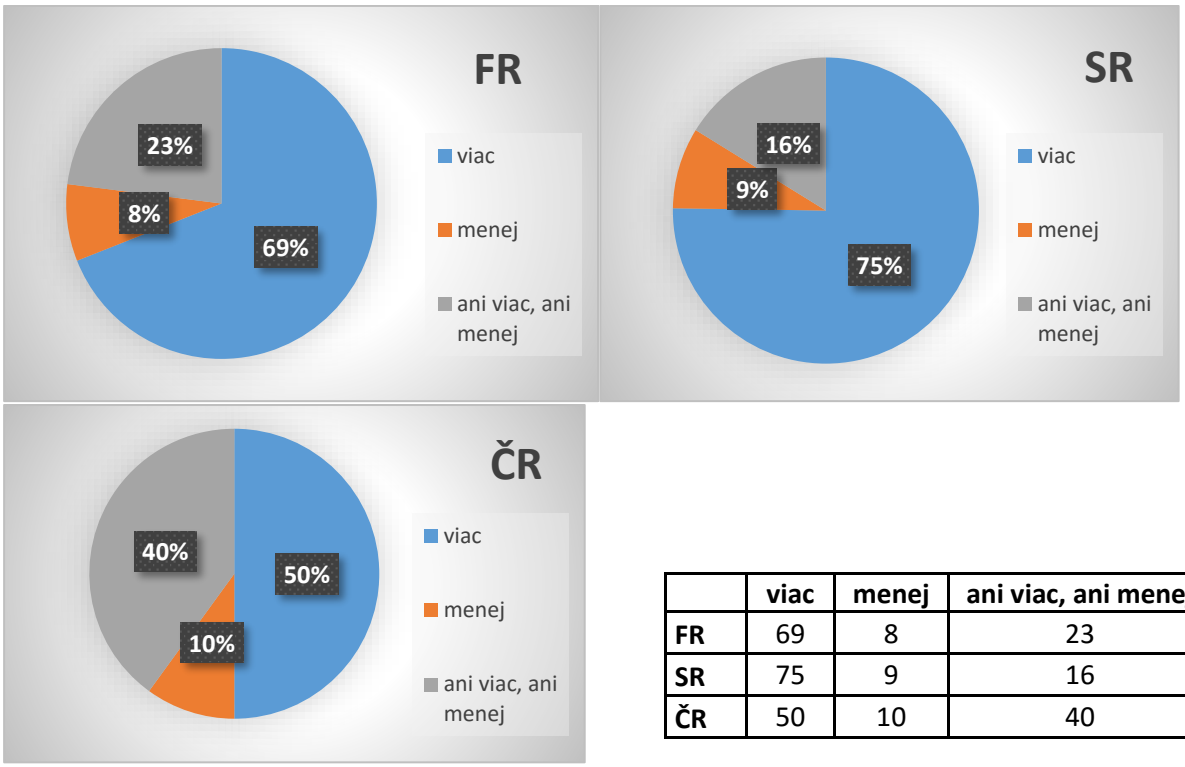


	viac	menej	ani viac, ani menej
FR	72	6	22
SR	76	7	17
ČR	76	8	16

Obr. 7: Grafy a tabuľka s vyhodnotením otázky č.7b
Zdroj: vlastné spracovanie

Obdobne, ako v predchádzajúcom prípade, je obava zo straty súkromia prostredníctvom uverejnenia dôverných osobných informácií na Internete, veľmi vysoká. Až 2/3 respondentov vo všetkých troch krajinách ju považuje za ešte rizikovejšiu ako zneužitie bankových údajov. Je to pochopiteľné, pretože oblasť zdravia, sexuálnej orientácie, vierovyznania, politickej príslušnosti, fotografií a rodinných a sociálnych pomerov, a pod., ľudia považujú za intímnu oblasť svojej identity.

c) Používanie vašich osobných údajov prostredníctvom sociálnych sietí.



	viac	menej	ani viac, ani menej
FR	69	8	23
SR	75	9	16
ČR	50	10	40

Obr. 8: Grafy a tabuľka s vyhodnotením otázky č.7c
Zdroj: vlastné spracovanie

Používanie sociálnych sietí pre komunikáciu medzi rodinou, priateľmi a známymi sa stalo nevyhnutným fenoménom elektronizácie našej spoločnosti. Najobľúbenejšou oblasťou je zdieľanie fotografií a noviniek, ale aj spoznávanie nových ľudí (priateľov našich priateľov, známych našich známych, atď.). Aj ľudia, ktorí nemajú veľké informatické znalosti, tu uverejňujú svoje osobné a citlivé údaje a fotografie. Nevedia si zabezpečiť ochranu svojich profilov, a tak riziko zneužitia týchto dát nepovolanými osobami je vysoké. Najväčšie obavy z ich zneužitia má viac ako 2/3 respondentov v SR a vo Francúzsku. Z výskumu je zrejmé, že informatické znalosti respondentov v ČR sú na takej úrovni, aby si užívatelia sociálnych sietí dokázali sami nastaviť ochranu svojich profilov, a tak len polovicu respondentov znepokojuje riziko neoprávneného zneužitia ich osobných dát.

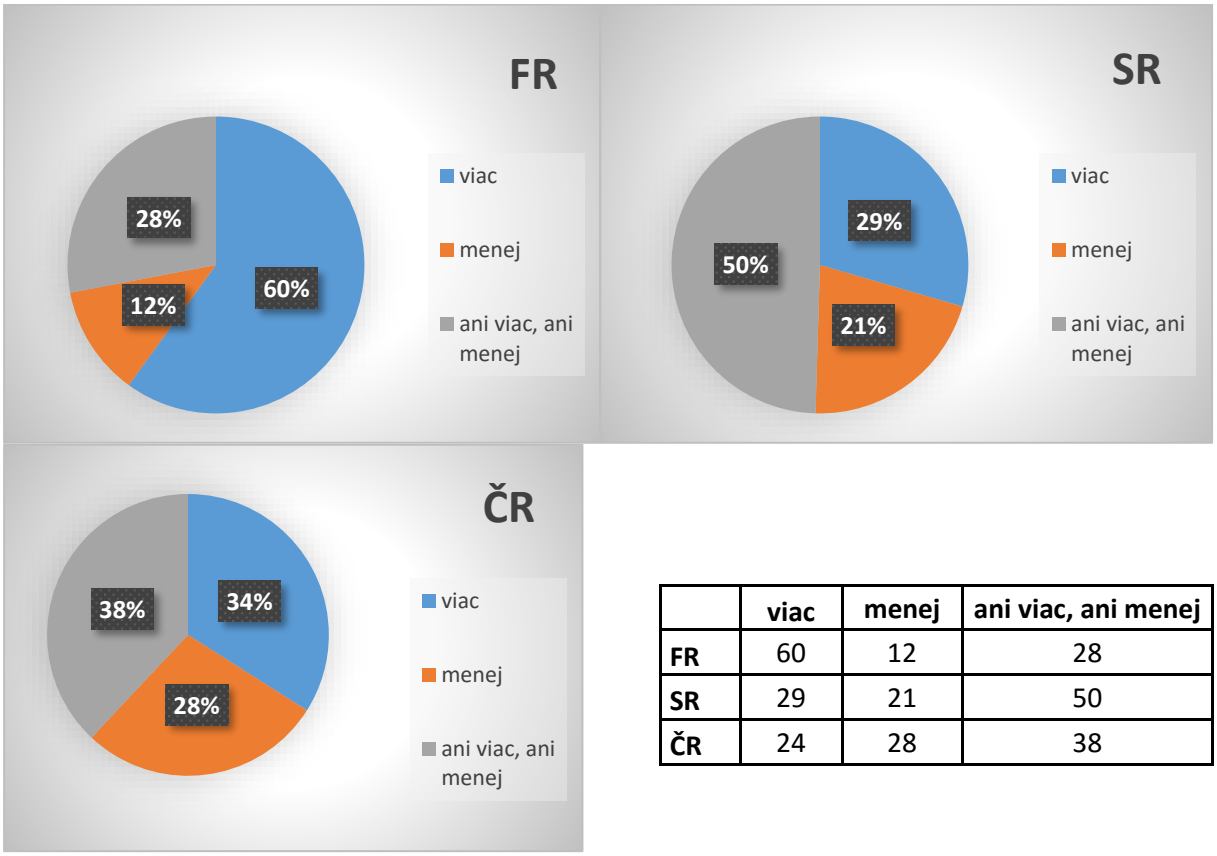
d) Skutočnosť, že informácie, ktoré poškodzujú vašu povesť, sú zámerne rozširované jednotlivcom alebo organizáciou.

	viac	menej	ani viac, ani menej
FR	68	8	24
SR	67	7	26
ČR	42	8	50

Obr. 9: Grafy a tabuľka s vyhodnotením otázky č.7d
Zdroj: vlastné spracovanie

Obavy zo šírenia negatívnych informácií majú opäť až 2/3 respondentov v SR a vo Francúzsku. Aj bez využívania elektronických médií boli a sú klebety veľkou živnou pôdou najmä pre závistlivcov a nepriateľov, ktorých hladným cieľom je ublížiť, minimálne slovne, svojim obetiam. Takže tieto obavy sú opodstatnené. Zaujímavý je však postoj respondentov v ČR, kde iba menej ako polovica má zo šírenia negatívnych informácií väčšiu obavu, avšak až 50% z nich uvádza, že situácia sa nadobudnutím účinnosti nariadenia GDPR nemení, čím priznávajú obavy z takejto aktivity zo strany iných osôb.

e) Skutočnosť, že vaše údaje budú používané politickými stranami, zvolenými zástupcami alebo kandidátmi.

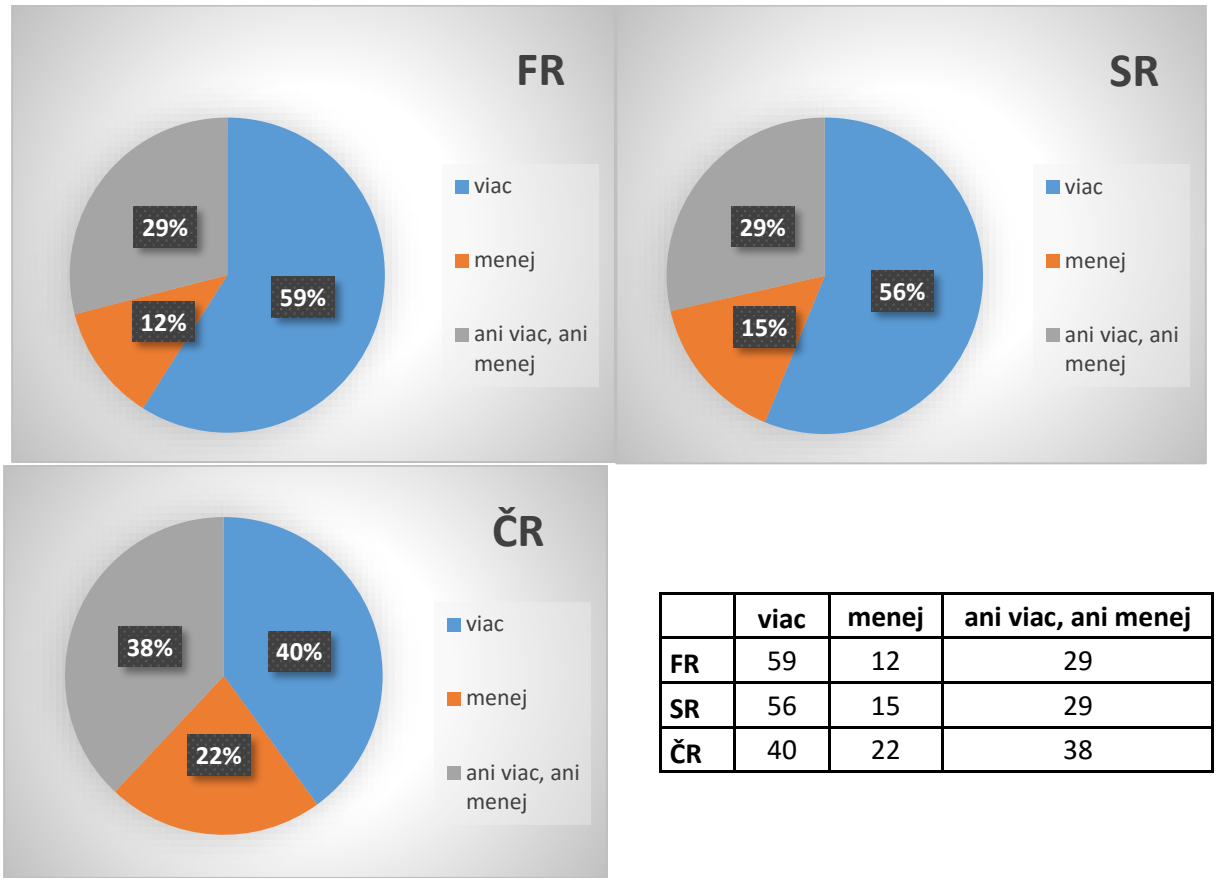


	viac	menej	ani viac, ani menej
FR	60	12	28
SR	29	21	50
ČR	24	28	38

Obr. 10: Grafy a tabuľka s vyhodnotením otázky č.7e
Zdroj: vlastné spracovanie

Obavy zo zneužívania osobných údajov politickými stranami alebo zvolenými zástupcami občanov majú až 2/3 respondentov vo Francúzsku, ale iba asi 1/3 respondentov v SR a ČR. Táto situácia je daná vo Francúzsku skúsenosťami z minulosti, kde politické strany majú dlhú existenciu a najmä v predvolebných obdobiach využívajú rôzne zdroje dát na získanie volebných preferencií. Naopak v post-komunistických krajinách vznikajú nové politické strany a ich zvolení predstavitelia majú zatiaľ iné priority, než získavať údaje voličov pre potreby ich priameho oslovovania za účelom podpory konkrétnej politickej strany.

f) Skutočnosť, že vám boli poskytnuté personalizované informácie podľa vášho správania na sociálnych sieťach, napr.: na Facebooku.



	viac	menej	ani viac, ani menej
FR	59	12	29
SR	56	15	29
ČR	40	22	38

Obr. 11: Grafy a tabuľka s vyhodnotením otázky č.7f
Zdroj: vlastné spracovanie

Komerčný trend využívania vernostných kariet a programov, ktoré najmä obchodné organizácie a firmy používajú pre sledovanie správania sa svojich zákazníkov, začína znepokojovať aj samotných zákazníkov. Títo si uvedomujú, že prostredníctvom týchto prostriedkov je sledované ich súkromie a podľa odpovedí respondentov výskumu, až približne polovica z nich začína mať z tejto aktivity čím ďalej, tým väčšie obavy.

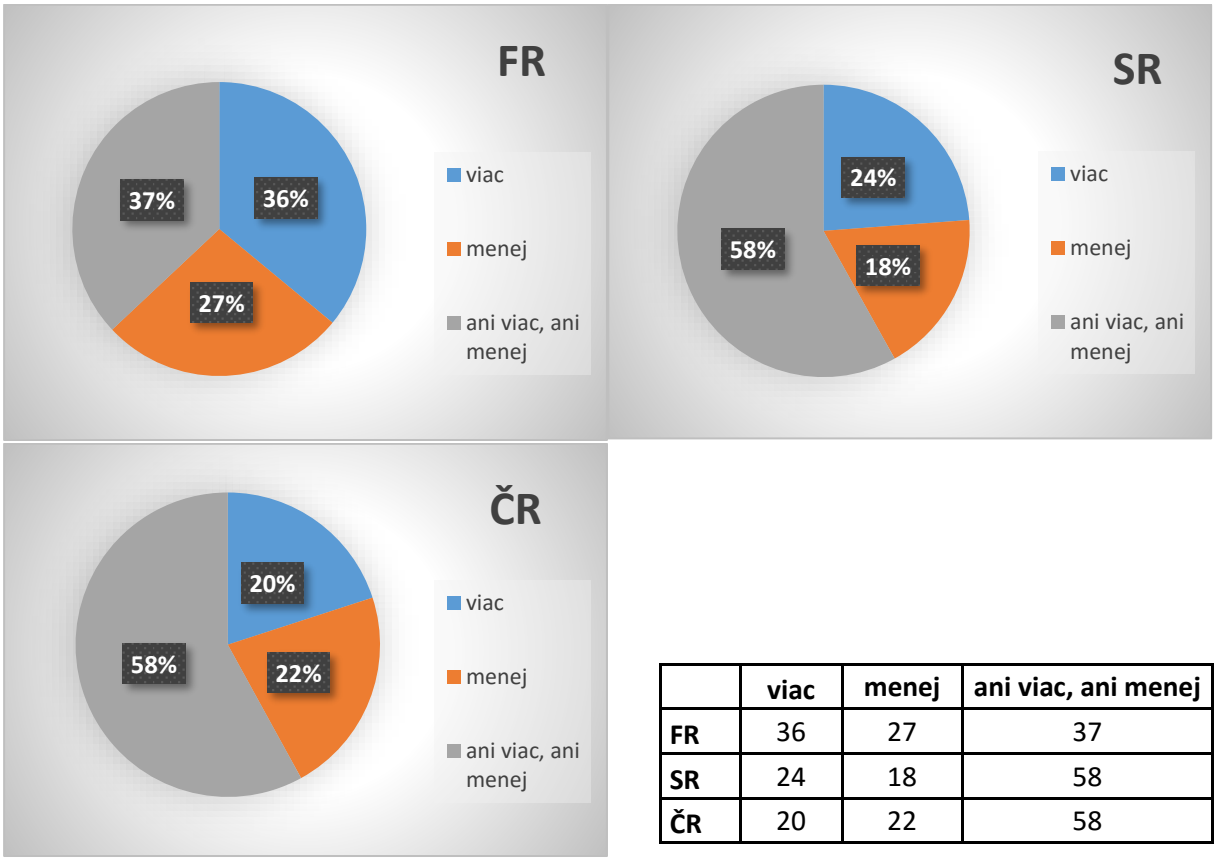
g) Prítomnosť cielených reklám na vami navštevovaných webových stránkach (podľa histórie vášho vyhľadávania, podľa vami navštívených stránok, atď.).

	viac	menej	ani viac, ani menej
FR	55	16	29
SR	67	14	19
ČR	44	24	32

Obr. 12: Grafy a tabuľka s vyhodnotením otázky č.7g
Zdroj: vlastné spracovanie

Zvyšuje sa aj podiel odpovedí respondentov vo všetkých troch krajinách, ktorí začínajú pociťovať väčšie riziko zo zneužívania ich osobných údajov prostredníctvom elektronických médií, medzi ktoré patrí aj sledovanie ich návštevnosti webových stránok. Výber cielenej reklamy, ktorá sa im zobrazuje v banneroch pri návštevách obľúbených stránok, predstavuje narušovanie ich súkromia.

h) Tvorba štátnych policajných súborov pre bezpečnostné účely.



	viac	menej	ani viac, ani menej
FR	36	27	37
SR	24	18	58
ČR	20	22	58

Obr. 13: Grafy a tabuľka s vyhodnotením otázky č.7h
Zdroj: vlastné spracovanie

Využívanie osobných údajov pre tvorbu štátnych policajných súborov pre bezpečnostné účely nepovažuje väčšina respondentov vo všetkých troch krajinách za riziko pre ich osobu. Vzhľadom na zhoršujúcu sa bezpečnostnú situáciu na celom svete, je to aj pochopiteľné, pretože vzájomná výmena údajov z databáz bezpečnostných zložiek medzi rôznymi štátmi, môže napomôcť k predvídaniu negatívnych bezpečnostných udalostí a prijatiu príslušných opatrení pre ich zamedzenie, resp. zmiernenie ich dopadov.

Záver

Z výskumu o povedomí o dôležitosti ochrany osobných údajov, ktorý bol zrealizovaný až v troch krajinách EÚ, je možné vyvodiť závery, že napriek prijímaniu celoeurópskych legislatívnych textov, ktoré upravujú oblasť ochrany osobných údajov na nadnárodnej úrovni, povedomie obyvateľov EÚ o nebezpečenstvách a rizikách vyplývajúcich zo straty súkromia, prípadne zneužitia ich osobných dát, je i naďalej nízke. Ľudia síce vnímajú prijatie príslušných opatrení zo strany kompetentných orgánov, ale buď im nevenujú dostatočnú pozornosť, alebo im nerozumejú. Preto považujeme za nevyhnuté venovať sa vysvetľovaniu obsahu týchto textov formou publikovania základných princípov, ktoré z nich vyplývajú spolu s uvedením názorných prípadov zneužitia súkromia alebo osobných dát, ale aj príkladov, pomocou ktorých je možné riziká zneužitia znížiť. Ale hovorí sa, že počuté slovo má lepší dopad na pochopenie ako písané, preto odporúčame organizovanie prednášok a vzdelávacích kurzov z oblasti ochrany osobných údajov a súkromia v elektronickom prostredí.

Zoznam použitej literatúry:

1. ŠÍMA, J. *Kvalita služeb sportovních zařízení a možnosti jejího hodnocení*. Univerzita Karlova v Praze, Karolinum, 2016. ISBN 978-80-246-3326-8.
2. *Les Français et la protection des données personnelles.* 2018. [online]. [cit. 2019-06-04]. Dostupné na:<https://www.cnil.fr/sites/default/files/atoms/files/barometre_ifop_rgpd-2018.pdf>
3. *Čo je GDPR?* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://gdpr-slovensko.sk/co-je-gdpr/>
4. Európska únia. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://sk.wikipedia.org/wiki/Európska_únia>
5. [Infographie] Bilan : 4 mois de RGPD en chiffres - Notification de violation des données. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.cnil.fr/fr/infographie-bilan-4-mois-de-rgpd-en-chiffres-notification-de-violation-des-donnees>
6. 6. *Nariadenie GDPR*. 2019. [online]. [cit. 2019-06-04]. Dostupné na:<https://dataprotection.gov.sk/uoou/sk/main-content/nariadenie-gdpr>
7. *Úřad pro ochranu osobních údajů.* 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.uoou.cz/>

Kontaktné údaje:

JUDr. Matej Kostrec, PhD.
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
matej.kostrec@minv.sk

Digitálna stopa ako základ kybernetickej bezpečnosti

Jana Kuchtová

Abstrakt:
Autorka príspevku sa snaží poukázať na problematiku kybernetickej kriminality prostredníctvom vymedzenia digitálnej stopy, ktorá je zanechávaná každým používateľom digitálneho zariadenia. Z tohto pohľadu je digitálna stopa základom kybernetickej bezpečnosti a dôležitým faktorom pri odhaľovaní a objasňovaní trestnej činnosti. Používatelia digitálnych zariadení zverejňujú na internete informácie, ktorých zhromažďovanie a zneužívanie páchateľmi môže viesť k bezpečnostným rizikám ohrozujúcim spoločnosť.
Kľúčové slová:
Kybernetická bezpečnosť, počítačová kriminalita, informatika, digitálna stopa, sociálne inžinierstvo.

Abstract:
Author of this paper tries to point out the issue of cybercrime by defining the digital footprint left by every digital device user. From this point of view, the digital footprint is the foundation of cyber security and an important factor in detecting and clarifying crime. Digital device users publish information on the Internet whose collection and abuse by perpetrators can lead to security risks to society.
Key words:
Cyber security, cybercrime, informatics, digital footprint, social engineering.

Úvod

Kybernetická kriminalita je, dá sa poveda, pojmom 21. storočia. Ide o fenomén modernej doby, spájajúci sa s kybernetickým priestorom a kriminalitou spojenou s jeho užívaním. Nie len že ide o aktuálnu tému, ale hlavne o problematiku vyžadujúcu si hlbokú analýzu, rozbor a nutnosť zaujatia jednotného postoja voči negatívnym vplyvom na ľudí. Na jednej strane je kybernetický priestor atraktívna oblasť spájajúca sa s technologickým napredovaním a informačným rastom populácie, čo je pozitívne, keďže k údajom sa v dnešnej dobe dostáva veľmi jednoducho. Ceny zariadení ktoré umožňujú prístup do kybernetického priestoru sú cenovo oproti minulosti oveľa dostupnejšie a zároveň požiadavkami zamestnávateľov na základné počítačové znalosti stúpol aj všeobecný záujem ľudí o nadobúdanie zručností v oblasti technológií. Tie majú slúžiť najmä na uľahčenie každodenných úloh a aktivít, teda možno hovoriť o tom, že majú slúžiť človeku v pozitívnom zmysle. Avšak tak ako aj v iných oblastiach, aj v kybernetickom priestore existuje veľká motivácia k páchaniu nelegálnej trestnej činnosti, vedúcej k osobným výhodám, zisku alebo inému obohateniu sa (motívy páchateľov môžu byť rôzne). Aby štát mohol efektívne bojovať s takouto formou kriminality, je nutné začať od vzdelávania špecialistov v danom obore, ktorých je v súčasnosti veľmi málo. Hlavným problémom získavania takýchto odborníkov, ktorý majú absolvované potrebné vzdelanie, je ich vysoké finančné ohodnotenie v súkromnej sfére, ktoré je niekoľko násobne vyššie ako by im vedel ponúknuť štát. Preto je nutné, aby štát zabezpečoval vzdelávanie ľudí, ktoré by ich dostatočne pripravilo na boj s kybernetickou trestnou činnosťou, v oblasti ktorej by sa stali odborníkmi. Motiváciou absolventov by mohla byť záruka ich okamžitého uplatnenia, vzhľadom na vyššie požiadavky a náročnosť ich dostatočné finančné ohodnotenie s možnosťou nadobúdania ďalších certifikátov a osvedčení. Samotné vzdelávanie kybernetickej bezpečnosti sa týka mnohých okruhov, vzhľadom na široké spektrum trestnej činnosti vykonávanej v kybernetickom priestore. Ďalšou náročnou úlohou je zabezpečovanie najnovšej techniky, schopnej vyrovnať sa zariadeniam používanými páchateľmi. Pri boji s týmto druhom trestnej činnosti je jednou z najnáročnejších bariér ich vysoká latentnosť, pričom keď sa spätne zistí spáchanie takého skutku, je len veľmi ťažko zistiteľný páchateľ – práve preto je nevyhnutné za základ objasňovania kybernetickej kriminality považovať digitálnu stopu, ktorú páchateľ zanecháva a na základe ktorej je možné získavať dôkazy vedúce k jeho úspešnému usvedčeniu.

Digitálna stopa

Digitálna stopa je tzv. odtlačok/ stopa používateľa, zanechávaná každým, kto používa digitálne zariadenie. Sú to také údaje, ktoré sú vytvárané používateľom pri využívaní internetu a jeho služieb. Medzi najčastejšie príklady patrí návšteva web stránok, sociálne siete, aplikácie, e-maily a mnoho ďalšieho. Ide o unikátny súbor aktivít digitálneho charakteru, akcií a komunikácií zanechávajúcich stopy na internete alebo v digitálnom zariadení, umožňujúci identifikáciu konkrétneho používateľa alebo zariadenia.[1] Ide o informácie o osobách alebo organizáciách, ktoré je možné získať z internetu, teda informácie o konkrétnej osobe existujúcej na internete v dôsledku jej online aktivity. Digitálna stopa je úzko prepojená s pojmom digitálna identita, ide o akúkoľvek online aktivitu, ktorá je súčasťou identity a jej obrazu pre ostatných. Rozšíreným pojmom digitálnej stopy je aj následná analýza a využitie nazbieraných a uložených dát.

Digitálnu stopu je možné deliť z viacerých hľadísk:

1. Podľa spôsobu vytvorenia digitálnej stopy
    - Aktívna
    - Pasívna[2]

2. Podľa vedomosti používateľa o vytvorení digitálnej stopy
    - Vedomá
    - Nevedomá

3. Podľa nosiča digitálnej stopy
    - Web
    - Digitálne zariadenie

Pasívna digitálna stopa je vytváraná bez zámerného úmyslu používateľa, za prehliadania a používania internetových služieb. Ide o IP adresy, vyhľadávané výrazy na internete, cookies, poskytovateľov pripojenia a lokalizáciu. Pri bežnej používateľskej úrovni nie je možné zabrániť vytváraniu pasívnej digitálnej stopy počas pripojenia k internetu. Každé zariadenie pripojené k internetu má jedinečnú adresu internetového protokolu, ktorá je buď statická alebo sa mení každým prihlásením. Na základe IP adresy zariadenia v sieti môže webový server poslať obsah stránky do prehliadača. Nosičom osobných informácií je prepojenie IP adresy poskytovateľom pripojenia s osobnými údajmi. Súbor cookie je uložený textový súbor ktorý webová lokalita pri prehliadaní internetu ukladá v zariadení, na základe čoho si webová lokalita uchováva informácie o prihlasovacom mene, hesle, jazyku a ďalších nastavení. Ďalším využitím cookie je zber anonymných štatistických údajov.[3] Úmyslom súborov cookie je na jednej strane zjednodušiť prehliadanie webových stránok – súbory cookie prvej strany (first-party cookie) a na strane druhej sú využívané pri pomoci inzerentov – súbory cookie tretej strany (third-party cookie) , ktorí na ich základe dokážu prispôsobiť svoje osobné preferencie. V prípade súborov cookie tretích strán môže dochádzať k nekontrolovateľnému zhromažďovaniu informácií

[1] Dictionary. 2019. *Digital footprint*. [online]. [cit. 2019-06-04]. Dostupné na:<https://www.dictionary.com/browse/digital-footprint>

[2] PEW Research

[3] *Čo sú súbory Cookie?* [online]. [cit. 2019-06-04]. Dostupné na: <https://ec.europa.eu/info/cookies_sk>

tretími osobami.[4] Zablokovaním týchto súborov dochádza k zvyšovaniu bezpečnosti používateľov.

Aktívna digitálna stopa je vytváraná používateľom vedome, za účelom vytvárania určitého obsahu. Používateľ zverejňuje údaje s vedomím dostupnosti takéhoto obsahu ostatným používateľom. Medzi najpopulárnejšie spôsoby vytvárania aktívnej digitálnej stopy patria sociálne siete, e-maily, blogy a ďalšie elektronické komunikačné systémy, kde sú dobrovoľné zverejňované informácie vo webovom priestore, telefonáty a rozhovory.

Vedomé a nevedomé digitálne stopy sú vytvárané inou osobou akou je používateľ, pričom o tom buď vie, v prípade čoho ide o vedomú digitálnu stopu, alebo nevie že sú o nej zverejňované údaje čo znamená, že ide o pasívnu digitálnu stopu.

Digitálnu stopu možno považovať za základ, ktorý by odborník na kybernetickú bezpečnosť mal ovládať ako východiskový poznatok nadväzujúci na čokoľvek, čo sa týka kybernetickej bezpečnosti. Nie je možné zadefinovať digitálnu stopu len ako súčasť informatiky, pretože ide o multidisciplinárnu problematiku týkajúcu sa aj ďalších oblastí, napríklad kriminalistiky, ekonómie, kriminológie a iných. Digitálna stopa sa týka každej oblasti v ktorej sú vytvárané digitálne odtlačky. Vo všeobecnosti prevláda názor, že digitálna stopa sa nachádza takmer na každom mieste činu.

Okrem iného, zaisťovanie digitálnych stôp je špecifický, systematický a častokrát náročný postup, ktorý si vyžaduje technické znalosti a dodržiavanie presných úkonov, aby tak nedošlo k znehodnoteniu tohto špecifického typu stopy. Vzdelávanie odborníkov v danej oblasti by mohlo viesť k zlepšeniu celého procesu od vyhľadávania, cez zaisťovanie až po analýzu a interpretáciu výsledkov digitálnych stôp súvisiacich s trestnou činnosťou. Protiprávne konanie môže byť spáchané za využitia digitálneho zariadenia, môže byť spáchané smerom k digitálnemu zariadeniu alebo v ňom digitálne zariadenie vystupuje ako vedľajší prvok. V dnešnej dobe už nemožno hovoriť len o počítači, keďže technologicky rozvoj umožňuje páchať trestnú činnosť s oveľa širším spektrom zariadení a proti mnohým iným zariadeniam, akým je počítač – napríklad čoraz populárnejšie sa rozvíjajúca oblasť Internet of Things (Internet veci), ktorý možno chápať ako prepojenie akéhokoľvek elektrického zariadenia s internetom alebo navzájom, nad rámec bežných zariadení akými sú stolné počítače, notebooky, smartphony a tablety.[5]

Digitálna stopa a sociálne inžinierstvo

Sociálne inžinierstvo je pojem označujúci podvody, podvádzanie a manipuláciu s obeťami, za účelom získavania, spracovávania a distribúcie dôverných informácií a finančných prostriedkov. Páchatelia zneužívajú digitálnu stopu obete, prostredníctvom ktorej môžu získavať heslá, bankové údaje a iné citlivé informácie. Najčastejšie ide o e-maily a sociálne siete. „Základným stavebným kameňom sociálneho inžinierstva je dôvera. Útočník podnikne kroky na to, aby si ju u budúcej obeti vybudoval a následne túto dôveru prehlbuje. Pred samotným útokom si útočník zistí informácie potrebné o obeti alebo o organizácii prostredníctvom OSINT (Open-source intelligence) – čo je získavanie spravodajských informácií z verejne dostupných zdrojov (médiá, webové komunity, sociálne siete, blogy, vládne reporty, rozpočty, tlačové konferencie, šedá literatúra a iné).“[6]

---

[4] ROOS, D. How to Surf the Web Anonymously? [online]. [cit. 2019-06-04]. Dostupné na: <https://electronics.howstuffworks.com/how-to-tech/how-to-surf-the-web-anonymously1.htm>

[5] KUCHTOVÁ, J. Aktuálne trendy súvisiace s využívaním moderných technológií, *In Aktuálne výzvy prevencie počítačovej kriminality: Zborník z medzinárodnej vedeckej konferencie konanej dňa 21. 3.* 2018. Bratislava: Akadémia Policajného zboru v Bratislave, 2018. s. 90 - 98.

[6] *Bezpečnostný system*. 2019. [online]. [cit.2019-06-04]. Dostupné na: <http://www.minv.sk/?Bezpecnostny_systemhttps://www.csirt.gov.sk/socialne-inzinierstvo-812.html>

Sociálne inžinierstvo je možné klasifikovať:

- Podľa rozsahu na:
  - masové podvody zamerané na veľký počet ľudí,
  - cielené podvody zamerané na konkrétnych jednotlivcov.[7]

- Podľa techniky:
  - Trashing,
  - Fishing,
  - Pharming,
  - Vishing,
  - HOAX a SPAM,
  - rôzne internetové lotérie.[8]

Zneužívanie digitálnej stopy na sociálne inžinierstvo v praxi môže byť uskutočňované vďaka trendu sociálnych sietí oveľa jednoduchšie ako v minulosti. „Útoky pomocou sociálneho inžinierstva sú rôznorodé - od hromadných phishingových emailov až po cielené, viacvrstvové a sofistikované útoky s využitím viacerých techník.“[9] Útočník si na základe digitálnej stopy vyhľadá osoby, ktoré majú vzťah k obeti. Na základe získaných informácií o rodinných väzbách môže rozposielať falošné e-maily s menom rodinných príslušníkov obeti a získavať tak citlivé informácie. V rámci sociálnych sietí je v mnohých prípadoch verejne dostupný dátum narodenia, dosiahnuté vzdelanie, rodinné väzby, obľúbené navštevované miesta – telocvične, obchody, kiná atď. Zdrojom dôležitých informácií pre páchateľa sú aj fotografie, z ktorých môže páchateľ zistiť veľa podstatných informácií.

Záver

Kybernetická kriminalita je oblasť, ktorú je potrebné neustále analyzovať, skúmať a v boji proti ktorej je nutné vynaložiť všetky prostriedky, keďže veľmi rýchlo napreduje tak, ako sa technologicky rozvíja spoločnosť. Zaisťovanie bezpečnosti v tejto oblasti je náročná úloha, ktorá si vyžaduje zavedenie vzdelávacieho systému, zabezpečenie technického vybavenia a dostatočnej prevencie. Bezpečný vývoj sa v dnešnej dobe stal v mnohých krajinách sveta skutočnou a naliehavou záležitosťou.[10] V rámci kybernetickej bezpečnosti je na mieste výskum samotnej digitálnej stopy, ktorá tvorí jej akýsi základ, ktorej zanechávanie, jej nezmazateľnosť a zraniteľnosť si v súčasnosti spoločnosť dostatočne neuvedomuje.

Zoznam použitej literatúry:

1. KORAUŠ, A., DOBROVIČ, J., RAJNOHA, R., BREZINA, I. 2017. *The safety risks related to bank cards and cyber attacks, Journal of Security and Sustainability Issues*. [online]. [cit. 2019-06-04]. Dostupné na: <https://doi.org/10.9770/jssi.2017.6.4>
2. KUCHTOVÁ, J. Aktuálne trendy súvisiace s využívaním moderných technológií, In *Aktuálne výzvy prevencie počítačovej kriminality*: Zborník z medzinárodnej vedeckej

[7] Interpol. 2019. *Types of social engineering*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud>

[8] PAULUS, T. 2013. *Techniky sociálneho inžinierstva*. [online]. [cit. 2019-06-04]. Dostupné na: <http://preventista.sk/info/techniky-socialneho-inzinierstva/>

[9] CSIRT.SK. *Sociálne inžinierstvo*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.csirt.gov.sk/socialne-inzinierstvo-812.html>

[10] KORAUŠ, A., et al. *The safety risks related to bank cards and cyber attacks*. 2017.

konferencie konanej dňa 21. 3. 2018. Bratislava: Akadémia Policajného zboru v Bratislave, 2018, 235 s. ISBN 978-80-8054-774-5.
3. Dictionary. 2019. *Digital footprint*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.dictionary.com/browse/digital-footprint>
4. *Čo sú súbory Cookie?* [online]. [cit. 2019-06-04]. Dostupné na: <https://ec.europa.eu/info/cookies_sk>
5. ROOS, D. *How to Surf the Web Anonymously*. [online]. [cit. 2019-06-04]. Dostupné na: <https://electronics.howstuffworks.com/how-to-tech/how-to-surf-the-web-anonymously1.htm>
6. CSIRT.SK. *Sociálne inžinierstvo*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.csirt.gov.sk/socialne-inzinierstvo-812.html>
7. Interpol. 2019. *Types of social engineering*. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.interpol.int/Crime-areas/Financial-crime/Social-engineering-fraud/Types-of-social-engineering-fraud>
8. PAULUS, T. *Techniky sociálneho inžinierstva*. [online]. [cit. 2019-06-04]. Dostupné na: <http://preventista.sk/info/techniky-socialneho-inzinierstva/>
9. *Bezpečnostný system*. 2019. [online]. [cit.2019-6-6]. Dostupné na: <http://www.minv.sk/?Bezpecnostny_systemhttps://www.csirt.gov.sk/socialne-inzinierstvo-812.html>

Kontaktné údaje:
Mgr. Jana Kuchtová
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
jana.kuchtova@minv.sk

Vybrané aspekty vzdelávania v oblasti kybernetickej bezpečnosti na základných školách

Filip Lenko

Abstrakt:
Dynamický rozvoj informačných technológií so sebou prináša aj nové spoločensky škodlivé javy. V oblasti kybernetickej bezpečnosti sa stáva výrazným fenoménom kyberšikanovanie. Častými obeťami kyberšikanovania sú deti a dospievajúci jedinci, ktorí nedokážu rozpoznať rôzne formy nebezpečia, ktoré im hrozia. Táto neschopnosť zhodnotiť situáciu môže mať vo výsledku vážny dopad na ich ďalší rozvoj. Príspevok sa zaoberá návrhom preventívnych opatrení a aktivít pre ochranu žiakov základných škôl pred kyberšikanovaním. Návrh opatrení je realizovaný základe vyhodnotenia dotazníkového výskumu zameraného na vnímanie kyberšikanovania žiakmi základných škôl. Cieľom príspevku je poukázanie na potrebu zvýšenia informovanosti žiakov v oblasti kyberšikanovania.
Kľúčové slová:
Kyberšikana, vzdelávanie, základné školy, prevencia, žiaci.

Abstract:
The dynamic development of information technologies also brings new socially dangerous phenomena. Cyberbullying is becoming a significant phenomenon in the field of cyber security. Frequent victims of cyberbullying are children and adolescents who are unable to recognize the various forms of danger they face. As a result, this inability to assess the situation can have a serious impact on their further development. The article deals with the design of preventive measures and activities to protect primary school pupils from cyberbullying. The proposal of measures is based on the evaluation of a questionnaire research focused on the perception of cyberbullying by primary school pupils. The aim of this article is to raise awareness of cyberbullying among pupils.
Key words:
Cyberbullying, education, primary schools, prevention, pupils.

Úvod

Bezpečnosť každej osoby je dôležitá, avšak veľký význam tvorí najmä bezpečnosť v spojení s deťmi a dospievajúcimi jedincami, ktorí ešte nedokážu kriminalite ako takej sami čeliť. Z toho dôvodu prevencia kriminality u deti zohráva dôležitú úlohu. Kyberšikanovanie je jednou z foriem šikanovania a bez znalostí samotnej problematiky šikanovania sa ním nedá zaoberať.

Šikanovanie, ktoré prebieha v školách sa často presúva aj do kyberpriestoru. Kyberšikanovanie sa často vyskytuje mimo školy, prevažne v domovoch obetí, čo naznačuje vážnosť tohoto ohrozenia. Pred šikanovaním obete utekajú do svojich domovov alebo tam, kde sa cítia bezpečne. Ukryť sa pred kyberšikanovaním je takmer nemožné. Nakoľko sa stávajú najčastejšími obeťami kyberšikanovania práve deti a dospievajúci jedinci, rozhodli sme sa vykonať dotazníkový výskum na základných školách v ktorom sme sa zamerali na vedomosti o kyberšikanovaní, formy kybernetického šikanovania a na skúsenosti s kyberšikanovaním.

Kyberšikanovanie

Kyberšikanovanie ako fenomén súčasnosti a zároveň nová forma agresie je spájaná s využitím informačných a komunikačných prostriedkov – internetu, e-mailu a predovšetkým sociálnych sieti. Pojem kyberšikanovanie pochádza z anglického cyberbullying a označuje spoločensky nežiaduce správanie či sociálno-patologický jav.[1]

Definície a charakteristika kybernetického šikanovania nie sú jednoznačné ani jednotné. Príčinou je snaha popísať a uchopiť kybernetický priestor, ktorý sa vďaka vývoju nových informačných a komunikačných technológií neustále mení. Všeobecne sa ale jedná

[1] HOLLÁ, K. *Kyber-šikana*. Bratislava: Iris, 2013. s. 20.

o šikanovanie, pri ktorom sa využívajú prostriedky elektronickej komunikácie. Kyberšikanovanie sa vyskytuje predovšetkým medzi dospievajúcimi jedincami a je čoraz intenzívnejšie. Pod tento pojem spadá napríklad ohováranie, vyhrážanie, sexuálne poznámky, šírenie osobných údajov obete, pejoratívne poznámky a prezývky – keď sú šírené prostriedkami elektronickej komunikácie. Patrí sem aj obťažovanie cez e-mail, sociálne siete či SMS[2].

Základné znaky kyberšikanovania

Rozpoznanie šikanovania nikdy nebolo veľmi jednoduché, ale pri kyberšikanovaní narážame na tento problém dvojnásobne. Kyberšikanovanie môže mať omnoho väčšie dôsledky ako bežné šikanovanie, tzv. šikanovanie tvárou v tvár. Základné znaky kyberšikanovania sú rovnaké ako u klasického šikanovania. Sú to predovšetkým periodicita, mocenská nerovnosť, zámer agresívneho obsahu a nepríjemné, zraňujúce správanie voči obeti. Základný rozdiel predstavuje iba prostredie, v ktorom sa oba typy šikanovania odohrávajú[3].

Pri porovnávaní oboch druhov šikanovania, môžeme zaznamenať faktory, ktoré robia kyberšikanovanie do istej miery nebezpečnejším. Zatiaľ čo pri šikanovaní sa agresor s obeťou stretávajú tvárou v tvár, realizáciu kyberšikanovania umožňujú informačné a komunikačné technológie. Agresor teda nemusí byť vybavený fyzickou silou, ale stačí mu bežná znalosť v oblasti informačných technológií. V jeho prospech hrá aj skutočnosť, že sa v kyberpriestore môže stať anonymnou osobou. Pri šikanovaní vie obeť presne, kto jej spôsobuje telesne či psychické utrpenie, pretože sa s tyranom reálne stretáva. Útočník, ktorý uskutočňuje kyberšikanovanie môže ukrývať svoju identitu a nechať obeť v pochybnostiach[4].

Ďalším znakom, ktorý robí kyberšikanovanie obzvlášť závažným, je jeho neobmedzenosť. Tým rozumieme neobmedzenosť z hľadiska času a priestoru. Na rozdiel od tradičného šikanovania môže kyberšikanovanie prebiehať sedem dni v týždni, dvadsaťštyri hodín denne. Je možné povedať, že dieťa sa pri tradičnom šikanovaní vie pred protivníkom skryť doma, no šikanovaniu prostredníctvom internetu sa však človek neschová nikdy a nikde. Zastrašujúce správy v kyberpriestore sa nedajú nijako odstrániť, takže sa s nimi obeť stretáva stále dookola. Navyše pri ich úniku či krádeži profilu si ich môže prečítať obrovské množstvo ľudí, čo znásobuje pocit bezmocnosti a utrpenia[5].

Typy kyberšikanovania

Kyberšikanovanie väčšinou začína ako tradičné šikanovanie, prípadne je jej sprievodným javom. Šikanovanie odohrávajúce sa v kyberpriestore má dve podoby. A to priamu (obeť je zainteresovaná v procese šikanovania) a nepriamu, teda kyberšikanu v zastúpení (bez okamžitého vedomia obete)[6].

Priame kyberšikanovanie - agresor útočí na obeť priamo, bezprostredne. Začne napríklad dehonestovať obeť, založí o nej falošný profil, zverejní jej fotografie či video a podobne[7].

Nepriame kyberšikanovanie – agresor na útok využíva inú osobu, ktorá často nevie o tom, že sa stala nástrojom útoku – napríklad pomsty[7]. Typický príklad predstavuje situáciu, kedy útočník prenikne na účet obete (napríklad na účet založený na sociálnej sieti), prostredníctvom tohto účtu začne znevažovať ostatných užívateľov, ktorí začnú reagovať.

---

[2] HANULOVÁ, L. *Internetová kriminalita páchaná na dětech psychologie internetové oběti, pachatele a kriminality.* Praha: Triton, 2012. s. 60.

[3] KYRIACOU, Ch. *Řešení výchovných problémů ve škole.* Praha: Portál, 2005. s. 89.

[4] VAŠUTOVÁ, M. *Proměny šikany ve světě nových médií.* Ostrava: Ostravská univerzita v Ostravě, 2010. s. 120.

[5] BURDOVÁ, E. a TRAXLER, J. *Bezpečně na internetu.* Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. s. 21.

[6] TRUKSOVÁ, L. *Analýza kyberšikany u adolescentov.* Praha: Institut sociologických studií Univerzita Karlova v Praze, 2010. s. 32.

[7] ČERNÁ, A. a kol. *Kyberšikana: Průvodce novým fenoménem.* Praha: Grada, 2013. s. 87.

Za online urážky sa budú chcieť pomstiť práve majiteľovi účtu, z ktorého boli dehonestujúce správy odosielané. Majiteľ účtu sa o tom dozvie až s časovým oneskorením[8].

Charakteristika účastníkov kyberšikany

Účastníci kyberšikanovania sa veľmi nelíšia od účastníkov bežného šikanovania. V oboch prípadoch sa hovorí o agresorovi, obeti a publiku. Všetky tri skupiny zohrávajú pri kyberšikanovaní významnú úlohu. Je jasné, že bez obete a agresora by sa incident vôbec nemohol odohrať, ale dôležitú úlohu má i na prvý pohľad nenápadné publikum. Kebyže agresor žiadne obecenstvo nemá, útok by ho čoskoro prestal baviť[7].

Agresor - býva pri tradičnom šikanovaní fyzicky alebo aspoň sociálne silnejší a obeť teda slabšia. Pri kyberšikanovaní to nemusí byť fyzicky silný jedinec, stačí, aby sa aspoň na základnej úrovni vyznal v informačných a komunikačných technológiách. Môže sa jednať o jednotlivca, ale tiež o celú skupinu. Kyberpriestor sa tak môže pre jedincov, ktorí sú v reálnom svete fyzicky slabší, hanbliví alebo nepriebojní, stať svetom, v ktorom sa premenia na človeka aktívneho niekedy až agresívneho[9].

Obeť - môže sa ňou stať niekto, kto nie je dobre oboznámený s rizikami kyberpriestoru a zverejňuje o sebe príliš osobných informácii. Taktiež podceňuje nástrahy kyberpriestoru alebo sa chová neopatrne a príliš dôveruje ľuďom, u ktorých pozná iba ich „online prezývku“. Kyberšikanovanie sa môže na obeti prejavovať ako psychologické šikanovanie, nakoľko sa jedná o rovnakú záležitosť. Obeť môže byť náladová, utiahnutá, môže začať používať komunikačné technológie oveľa frekventovanejšie alebo sa ich naopak strániť, môže mať problémy so spaním a nechutenstvom. Obete kyberšikanovania sa delia rovnako ako obete tradičného šikanovania. Na pasívne obete a obete – provokáterov. Pasívnymi obeťami sú práve plaché, hanblivé, citlivé deti, ktoré majú nižšie sebavedomie a nie sú tak fyzicky zdatné či atraktívne. Obete – provokatéri sa naopak vyznačujú hyperaktivitou, agresivitou, impulzívnosťou a spravidla nemajú žiadnych priateľov. Kolektív ich nemá príliš v obľube a ich šikanovanie vnímajú tak, že si ho skrátka zaslúžia[10].

Svedkovia, publikum - kyberšikanovanie sa uskutočňuje v kyberpriestore, v ktorom sa nachádza veľký počet svedkov. Publikum, teda prizerajúca skupina ľudí sa delí:

- prizerajúci, ktorí majú strach zasiahnuť,
- prizerajúci, teda priaznivci, ktorí sa na útoku zabávajú.[11]

Prizerajúci svedkovia sa delia aj na aktívnych a pasívnych. Keďže prejavy kyberšikanovania vidí v kyberpriestore množstvo ľudí, pasívny svedkovia predpokladajú, že niekto iný už obeti pomohol a tak nezasahujú do kyberšikanovania. Na druhej strane, aktívny svedok sa stáva buď obrancom alebo sympatizantom s agresorom. Obrancom vtedy, ak zasiahne do priebehu kyberšikanovania, ohlási ju a uteší obeť a sympatizantom s agresorom sa stáva vtedy, keď sa zabáva na jeho útokoch. Niektorí členovia publika nezasahujú, pretože si nie sú istí závažnosťou situácie.[12]

[8] SZOTKOWSKI, R. a KOPECKÝ, R. *Kyberšikana a ďalší druhy online agrese zaměřené na učitele.* Olomouc: Pedagogická fakulta Univerzita Palackého v Olomouci, 2018. s. 98.

[9] BLÁHOVÁ, R., ŠALŠOVÁ, L. *Problémy se třídou? Tipy a náměty pro třídní učitele.* Praha: Raabe, 2012. s. 47.

[10] KOPECKÝ, K. a kol. *Rizikové formy chování českých a slovenských dětí v prostrědí internetu*. Praha: Triton, 2015. s. 129.

[11] HOLLÁ, K. *Kyber-šikana*. Bratislava: Iris, 2013. s. 20.

[12] HOLLÁ, K. *Kyber-šikana*. Bratislava: Iris, 2013. s. 20.

Formy kyberšikanovania - vyjadrujú konkrétne prejavy, teda jednotlivé variácie online správania. Nasledujúce druhy správania, ktoré sú klasifikované ako kyberšikanovanie bez ohľadu na špecifické prostriedky komunikácie:

- flaming (vzplanutie),
- obťažovanie (harassment),
- ohováranie (denigration),
- zneužívanie identity (impersonation),
- odhalenie a podvod (outing and trickery),
- vylúčenie (exclusion),
- kyber-prenasledovanie (cyberstalking),
- veselé fackovanie (happy slapping)[13].

Výsledky a zistenia vyplývajúce z dotazníkového výskumu

Výskum bol realizovaný na dvoch základných školách v okrese Čadca a zúčastnilo sa ho celkovo 100 respondentov z oboch škôl. V príspevku použijeme výsledky len niekoľkých najdôležitejších otázok z hľadiska rozsahu.

Cieľom prvej otázky dotazníka bolo zistiť, aké množstvo žiakov sa stretlo s pojmom kyberšikanovanie. Výsledkom bolo zistenie, že 59 % žiakov sa s týmto pojmom stretlo a vedelo ho definovať resp. vysvetliť. Z dôvodu pomerne nízkych znalostí o kyberšikanovaní bolo potrebné žiakom vysvetliť, čo kyberšikanovanie znamená, aké má formy, kým môžu byť obete a páchatelia a ako sa jej brániť. Následne sme mohli pokračovať vo vypĺňaní dotazníka.

Ďalšia otázka bola zameraná na subjektívne vnímanie kyberšikanovania a otázka znela „Je podľa teba kyberšikanovanie závažný druh šikanovania?“. Pri tejto otázke sa 46 % žiakov vyjadrilo, že kyberšikanovanie nevnímajú ako závažný druh šikanovania, nakoľko v ich okolí nie je rozšírený. Zvyšných 54 % považovalo kyberšikanovanie za závažný druh šikanovania.

Cieľom ďalšej otázky bolo zistiť či sa žiaci vybraných základných škôl stali obeťami kyberšikanovania. Po vyhodnotení tejto otázky sme zistili, že 64 % žiakov sa doposiaľ nestalo terčom kyberšikanovania a zvyšných 36 % už malo skúsenosť s kyberšikanou. Môžeme povedať, že 36 % je pomerne vysoké percento vzhľadom na to, že účastníkmi výskumu boli deti vo veku od 10 do 15 rokov. Taktiež môžeme predpokladať, že v niektorých prípadoch sa nemuselo jednať o kyberšikanovanie nakoľko je tento dotazník založený na subjektívnom vnímaní danej problematiky žiakmi základných škôl.

Následne sme sa zaujímali o to, prostredníctvom akej formy sa stali obeťou kyberšikanovania. Žiaci najčastejšie uvádzali, že sa stali obeťami kyberšikanovania na sociálnych sieťach, ďalej formou urážajúcich a posmešných SMS správ a uverejňovania ich zosmiešňujúcich fotografií a videí na internet.

Z hľadiska prevencie šikanovania nás zaujímalo, či žiaci základných škôl boli poučení o šikanovaní a kyberšikanovaní, pred vypĺňaním tohto dotazníka. Vyhodnotenie tejto otázky dopadlo nasledovne: takmer 70 % žiakov bolo poučených o šikanovaní, 15 % žiakov bolo poučených o kyberšikanovaní a 15 % nebolo poučených žiadnym spôsobom. Zistili sme teda, že žiaci majú pomerne veľké rezervy a neuvedomujú si možné riziká, ktoré im hrozia. Na záver sme položili otázku či chcú byť a ak áno akou formou by chceli byť poučení o kyberšikanovaní, kde mohli označiť viac možností.

Výsledkom je, že 90 % respondentov chce byť dodatočne poučených o kyberšikanovaní a to formou: prednášok s učiteľmi (62 %), pozeraním náučných videí (22%), prednáška s policajtmi (preventistami) (70%) a prednáškami so školským psychológom (16 %).

[13] CHLEBCOVÁ, J. *Kyberšikana na sociálních sítích u žáků střědních škol.* Brno: Fakulta humanitních studií Univerzita Tomáše Bati ve Zlíně, 2013. s. 34.

Zhodnotenie dotazníkového výskumu

Z výsledkov dotazníkového výskumu je zrejmé, že kyberšikanovanie, ktoré patrí k novodobým fenoménom, väčšina žiakov už na základných školách vníma. Množstvo respondentov počula o kyberšikanovaní zo svojho okolia a časť z nich sa už aj stala obeťou kyberšikanovania. Z výsledkov dotazníkového výskumu vyplýva, že ženské pohlavie je častejšou obeťou kyberšikanovania a naopak u mužské pohlavie sa častejšie stáva obeťou šikanovania. Z oslovených respondentov oboch škôl takmer všetci trávia istú čas dňa vo virtuálnom svete. Priemerný čas, ktorý trávia deti zúčastnené výskumu, používaním mobilov, tabletov a iných technológií sú 2 – 4 hodiny denne.

Medzi činnosti, ktoré deti na internete vykonávajú najčastejšie sú online komunikácia a hranie online hier. Práve online komunikácia je prostriedkom na páchanie kyberšikanovania. Zistili sme, že najčastejšie dochádza ku kyberšikanovaniu formou zverejnenia posmešných fotografií a videí. Častokrát publikum sympatizuje s agresorom, čo celú situáciu pre obeť veľmi komplikuje a vzniknutá situácia môže na psychickom stave obete zanechať vážne následky. Samotnému kyberšikanovaniu častokrát predchádza šikanovanie, ktoré je v súčasnosti u mladých ľudí a na školách často riešené.

Dotazníkový výskum poukázal na to, že žiaci majú o kyberšikanovaní nedostatok informácií avšak majú záujem sa v tejto oblasti vzdelávať. Častokrát sa o kyberšikanovaní dozvedajú práve od svojich kamarátov a od učiteľov počas výučby alebo od svojich rodičov.

Záver

Vyjadrenia žiakov v rámci dotazníkového výskumu poukazujú na skutočnosť, že kyberšikanovanie sa na základných školách vyskytuje a stretávajú sa s ním už deti vo veku 10 rokov. Povedomie žiakov o formách páchania kyberšikanovania je častokrát na nízkej úrovni a nepovažujú ju za určitý druh ohrozenia. Tieto skutočnosti resp. nevedomosť môže mať však zásadný vplyv na ďalší vývoj žiakov ak sa stanú obeťami kyberšikanovania. Z tohto dôvodu je potrebné zvýšiť mieru informovanosti u mladistvých o šikanovaní a kyberšikanovaní ako aj ďalších oblastiach, ktorými sa zaoberajú preventívne aktivity.

Takmer 90 % respondentov vo veku od 10 do 15 rokov vyslovene chcelo mať prednášku a byť tak poučení o kyberšikanovaní resp. o možnostiach ako jej predchádzať alebo ju riešiť ak sa stanu obeťou takéhoto útoku. Respondentov najviac zaujala možnosť prednášky s príslušníkmi Policajného zboru a prednáškami s ich učiteľmi. Obe aktivity na školách priebežne prebiehajú, avšak pravdepodobne nie v dostatočnej miere. U žiakov základných škôl, resp. u detí a maloletých osôb je potrebné brať do úvahy nové riziká, ktoré so sebou prináša dnešná doba. Je potrebné aby preventívne aktivity zamerané na prevenciu v oblasti šikanovania a kyberšikanovania napredovali súčasne s dnešnou dobou a rozmachom rôznych nových rizík. Jedine týmto spôsobom dokážeme ochrániť resp. zabezpečiť bezproblémový psychický vývoj detí.

Zoznam použitej literatúry:

1. BLÁHOVÁ, R. a ŠALŠOVÁ, L. *Problémy se třídou? Tipy a náměty pro třídní učitele.* Praha: Raabe, 2012. 92 s. ISBN 80-87553-40-4.
2. BURDOVÁ, E. a TRAXLER, J. *Bezpečně na internetu.* První vydaní. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. 42 s. ISBN 80-904864-9-2.
3. ČERNÁ, A. a kol. *Kyberšikana: Průvodce novým fenoménem.* 1. vyd. Praha: Grada, 2013. 152 s. ISBN 80-247-4577-0.
4. CHLEBCOVÁ, J. *Kyberšikana na sociálních sítích u žáků střědních škol.* Brno: Fakulta humanitních studií Univerzita Tomáše Bati ve Zlíně, 2013. 70 s.

5. HOLLÁ, K. *KYBER-ŠIKANA.* Prvé vydanie. Bratislava: Iris, 2013. 111 s. ISBN 80-8153-011-1.
6. HULANOVÁ, L. *Internetová kriminalita páchaná na dětech psychologie internetové oběti, pachatele a kriminality.* 1. vyd.. Praha: Triton, 2012. 217 s. ISBN 80-7387-545-9.
7. KOPECKÝ, K. a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Centrum prevence rizikové virtuální komunikace Univerzita Palackého v Olomouci, 2015. 170 s. ISBN 978-80-244-4868-8.
8. KYRIACOU, Ch. *Řešení výchovných problémů ve škole.* Praha: Portál, 2005. 152 s. ISBN 80-7178-945-3.
9. SZOTKOWSKI, R. a KOPECKÝ, R. *Kyberšikana a ďalší druhy online agrese zaměřené na učitele.* 1. vydání. Olomouc: Pedagogická fakulta Univerzita Palackého v Olomouci, 2018. 129 s. ISBN 80-244-5335-4.
10. TRUKSOVÁ L. *Analýza kyberšikany u adolescentov.* Diplomová práca. Praha: Institut sociologických studií Univerzita Karlova v Praze, 2010. 103 s.
11. VAŠUTOVÁ, M. *Proměny šikany ve světě nových médií.* První vydaní. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. 225 s. ISBN 80-7368-858-5.

Kontaktné údaje:
Ing. Filip Lenko
Fakulta bezpečnostného inžinierstva
Katedra bezpečnostného manažmentu
Žilinská univerzita v Žiline
filip.lenko@fbi.uniza.sk

Príprava bezpečnostných manažérov v oblasti kybernetickej bezpečnosti - výsledky testovania

Ladislav Mariš, Viktor Šoltés

Abstrakt:
Vysokoškolské vzdelávanie bezpečnostných manažérov je zamerané na rôzne odborné predmety v oblasti ochrany osôb a majetku. Na Fakulte bezpečnostného inžinierstva, Žilinskej univerzity v Žiline sa obsah výučby predmetu aplikovaná informatika zameriava aj na otázky kybernetickej bezpečnosti. V rámci výučby bola realizovaná pilotná príprava a preskúšanie študentov formou phishingového testu. S odstupom 7 dní po prvom testovaní sa vykonal retest. V článku prezentujeme výsledky z prípravy a testovania študentov.
Kľúčové slová:
Phishing, test, študenti, csirt.sk, bezpečnosť.

Abstract:
University education of security managers is focused on various professional subjects in the field of personal and property protection. At the Faculty of Security Engineering, University of Žilina, the subject of applied informatics is also focused on cyber security issues. As part of the teaching, a pilot preparation and testing of students through a phishing test was carried out. Retest was performed 7 days after the first testing. The article presents the results of the preparation and testing of students.
Key words:
Phishing, test, students, csirt.sk, security.

Úvod

Phishing je forma kybernetického útoku s využitím foriem sociálneho inžinierstva. Koncept phishingu prvýkrát popísali Jerry Felix and Chris Hauck v roku 1987 v štúdii s názvom „*System Security: A Hacker's Perspective*“. Táto publikácia opisovala techniky, pri ktorých sa útočník vydáva za inštitúciu alebo službu. Samotný termín „*phishing*“ je podobný anglickému slovu „*fishing*“, čo v preklade znamená chytanie rýb, a nabáda k podobnému významu chytania obete na návnadu. Tiež sa môžeme stretnúť s významom začiatočných písmen „*ph-*“, ktoré sa odkazujú na “*phreaks*”, skupinu hackerov, ktorí v deväťdesiatych rokoch 20. storočia pri experimentovaní s možnosťami telekomunikačných systémov zašli za hranice zákona.

Najviac používanou technikou phishingu je vydávať sa za bankovú inštitúciu alebo správcu emailového konta, prostredníctvom falošného e-mailu. Tento e-mail (skrytá návnada) má obeť priviesť k tomu, aby najčastejšie klikla na niektorý hypertextový odkaz v správe či vyplnila formulár uvedený v tele správy alebo sa nachádza pod niektorým odkazom či v prílohe správy. Formulár najčastejšie nabáda na vyplnenie niektorých osobných údajov, napr. prihlasovacie údaje a pod.

V minulosti sa na tento účel používali najmä nie správne napísané názvy domén, napr. písmeno *m* sa podobá *rn*, čo si bežný človek nemusí rýchlo všimnúť a vo dobrej domnienke klikne na falošnú stránku. V súčasnosti útočníci využívajú sofistikovanejšie metódy, takže odkazy a falošné webové stránky sa svojim legitímnym náprotivkom skutočne veľmi podobajú.

Testovanie študentov bezpečnostného inžinierstva

Vysokoškolské vzdelávanie bezpečnostných manažérov je zamerané na rôzne odborné predmety v oblasti ochrany osôb a majetku. Na Fakulte bezpečnostného inžinierstva, Žilinskej univerzity v Žiline sa v rámci predmetu *aplikovaná informatika* obsah výučby zameriava aj na otázky kybernetickej bezpečnosti.

Cieľom praktickej časti výučby predmetu je o. i. vykonávať testovanie znalostí a zručností na oblasť kybernetickej bezpečnosti. Potreba poznania tejto oblasti je nevyhnutným predpokladom manažérskej činnosti v súkromnej či štátnej sfére, o to viac v problematike bezpečnostného manažérstva. Testovaniu študentov predchádzala príprava vo forme odbornej

prednášky na tému kybernetická bezpečnosť, zameraná na phishing. Po prednáške sme vykonali testovanie študentov vo forme tzv. *phishingového testu*. V nasledujúcom týždni sme vykonali opätovné testovanie, rovnakého phishingového testu.

Testovacia metóda

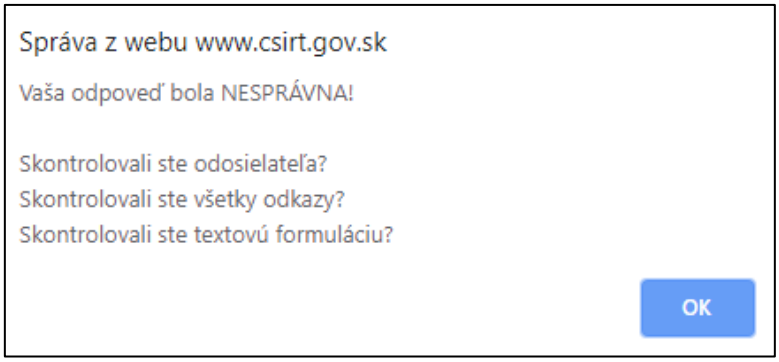
Na vykonanie phishingového testu sme zvoli odporúčaný test jednotky CSIRT na Úrade podpredsedu vlády SR pre investície a informatizáciu, ktorý je dostupný na stránke csirt.sk[1]. Test je zložený zo 17 testovacích otázok.

Úlohou testovaného študenta bolo rozhodnúť o tom, ktorá správa (prijatý email) je legitímny alebo je podvrhnutý kybernetickým útočníkom. Príklad otázky je na nasledujúcom obrázku (Obrázok 1). Po zobrazení otázky, študent overí všetky náležitosti správy a klikne buď na tlačidlo *Podvrhnutý* alebo *Legitímny.* Ak označí správnu odpoveď, tak prejde na ďalšiu otázku. Ak študent odklikane klikne na falošný odkaz v správe, tak sa na stránke zobrazí informácia, že študent spravil chybu a v reálnom svete mohol ohroziť svoj počítač (Obrázok 2). Ak študent označí nesprávnu odpoveď, stránku mu zobrazí upozornenie (Obrázok 3). Na zodpovedaní poslednej testovacej otázky sa zobrazí informácia o počte správnych a nesprávnych odpovedí (Obrázok 4). Zároveň testovaná osoba má možnosť pozrieť si návody ako odhaľovať podvodné správy alebo sa vrátiť k obsahu testovaných otázok s vysvetlením každej testovacej otázky.

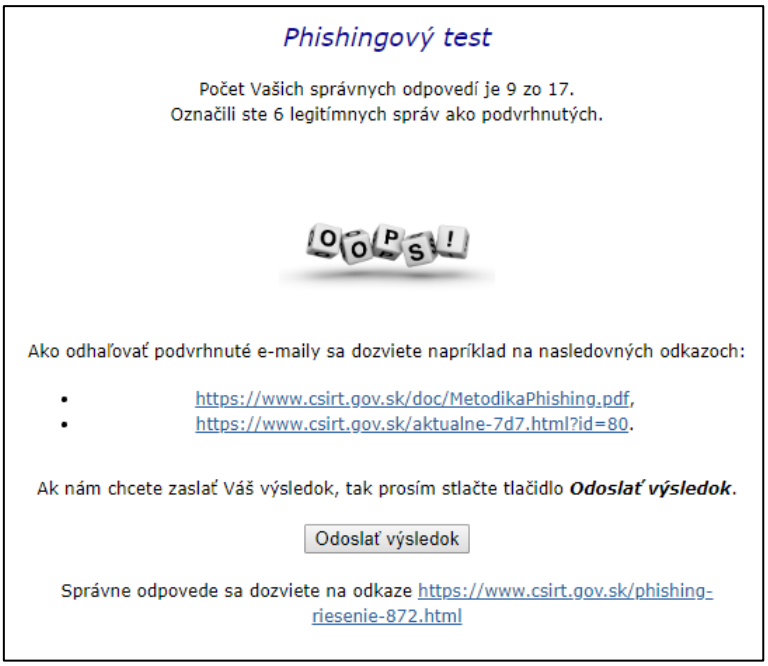
Obr. 1: Príklad testovacej otázky phishingového testu.
Zdroj: https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html

[1] CSIRT.SK - Úrad podpredsedu vlády SR pre investície a informatizáciu. 2019. *Phishingový test.* [online]. [cit. 2019-06-04]. Dostupné na: <https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html>

Obr. 2: Informáciu po kliknutí na falošný odkaz v správe
Zdroj: https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html



Obr. 3: Informácia po označení nesprávnej odpovede
Zdroj: https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html



Obr. 4: Zobrazenie výsledku testu
Zdroj: https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html

Výsledky testovania

Výsledky testovania sme si zapisovali ku každej testovanej osobe za účelom porovnania výsledkov. V nasledujúcej tabuľke (Tabuľka 1) zverejňujeme detailné výsledky testovania z oboch týždňov. Konkrétne mená študentov sme nahradili ID kódom pre zachovanie anonymity. v tabuľke uvádzame aj rozdiel v testovaní študentov. Pokiaľ je v hodnote rozdiel kladné číslo, tak sa študent zlepšil, pokiaľ je záporné číslo, tak sa zhoršil a pokiaľ je hodnota 0, počet správnych odpovedí je rovnaký. V tabuľke sú aj testované osoby, ktoré sa zúčastnili testu len raz, označené pomlčkou. V tom prípade sme rozdiel nezaznamenali.

Z výsledkov vyplýva, že sme spolu otestovali 78 študentov, z toho retest vykonalo 69 študentov. Priemerný výsledok prvého testovania bol 10,2 bodu. Priemerný výsledok druhého testovania bol 12 bodov. Priemerné zlepšenie bolo o 1,8 bodu.

45 (65,2 %) študentov sa zlepšilo, 18 (26,1 %) študentov malo rovnaký výsledok a 6 (8,7 %) študentov sa zhoršilo oproti prvému testovaniu.

Z hľadiska analýzy chybných odpovedí konštatujeme, že študenti robili chyby najmä pri kontrole skutočného odosielateľa a kontrole URL odkazov priamo z e-mailu. Zo skúseností z prvotného testovania, študenti v druhom testovaní boli viac kritickí k testovacím otázkam. To zapríčinilo najmä chybné označenie *Podrvhnutý*, napriek tomu, že sa jednalo o legitímne správy. Doplňujúce otázky zo strany učiteľa boli cielené na tému phishingu a kládol sa vyšší dôraz na osobné skúsenosti. Ako príklady je vhodné uvádzať negatívne skúsenosti či už osobné, alebo vybraného študenta.

Tabuľka 1: Výsledky testovania

ID	Počet správnych odpovedí		Rozdiel	ID	Počet správnych odpovedí		Rozdiel
	Testovanie 1	Testovanie 2			Testovanie 1	Testovanie 2	
1	10	12	2	40	10	12	2
2	11	10	-1	41	7	16	9
3	15	14	-1	42	9	11	2
4	12	13	1	43	10	10	0
5	10	11	1	44	10	12	2
6	9	10	1	45	9	14	5
7	6	11	5	46	12	-	-
8	10	12	2	47	11	12	1
9	12	-	-	48	12	11	-1
10	11	13	2	49	10	12	2
11	10	12	2	50	12	12	0
12	9	10	1	51	14	14	0
13	7	12	5	52	9	15	6
14	13	14	1	53	6	12	6
15	14	15	1	54	12	11	-1
16	12	12	0	55	10	10	0
17	10	11	1	56	12	12	0
18	9	10	1	57	8	13	5
19	8	12	4	58	9	13	4
20	12	13	1	59	10	15	5
21	13	13	0	60	12	-	-
22	14	15	1	61	10	10	0
23	12	11	-1	62	10	10	0
24	10	11	1	63	9	9	0
25	9	14	5	64	10	10	0
26	6	10	4	65	8	8	0
27	5	11	6	66	9	9	0
28	14	-	-	67	14	14	0
29	12	13	1	68	10	10	0
30	11	10	-1	69	10	10	0
31	12	14	2	70	6	6	0
32	13	14	1	71	10	12	2
33	7	14	7	72	9	-	-
34	10	13	3	73	10	15	5
35	5	8	3	74	11	12	1
36	12	15	3	75	-	11	-
37	9	16	7	76	-	10	-
38	10	10	0	77	-	12	-
39	12	17	5	78	-	13	-

Záver

Záujmom školstva by malo byť o. i. aj pripravovať študentov stredných a vysokých škôl na prácu s počítačov, čo sa do značnej mieri napĺňa. Treba však jedným dychom povedať, že práca s počítačom je nielen ho vedieť používať na rôzne účely, ale aj vedieť sa chrániť pred kybernetickými hrozbami. Je potrebné dodržiavať zásady bezpečnej práce na počítači, používať vierohodný a aktualizovaný softvér, a aktualizovaný antivírový program.

Snahou Fakulty bezpečnostného inžinierstva je okrem tradičných manažérskych a technických predmetov pripravovať študentov aj na kybernetické hrozby. Jednou z prvých aktivít, je prispôsobenie predmetov na tieto hrozby, pokiaľ je to možné.

Zaradením odborných prednášok a cvičení na tému kybernetickej bezpečnosti v konkrétnom prípade, napr. problematika phishingu, prispejeme k lepšej pripravenosti budúcich štátnych a súkromných zamestnancov.

Poďakovanie

Príspevok bol spracovaný v rámci riešenia projektu VEGA 1/0768/19.

Zoznam použitej literatúry:

1. *Phishingový test, Csirt.sk* - Úrad podpredsedu vlády SR pre investície a informatizáciu. 2019. [online]. [cit. 2019-06-04]. Dostupné na: <https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html>

Kontaktné údaje:

Ing. Ladislav Mariš, PhD.
Fakulta bezpečnostného inžinierstva
Katedra bezpečnostného manažmentu
Žilinská univerzita v Žiline
ladislav.maris@fbi.uniza.sk

Ing. Viktor Šoltés, PhD
Fakulta bezpečnostného inžinierstva
Katedra bezpečnostného manažmentu
Žilinská univerzita v Žiline
viktor.soltes@fbi.uniza.sk

Úloha sociológie v rozvoji digitálnych kompetencií študentov Akadémie PZ v Bratislave

Karol Murdza

Abstrakt:
Digitálne kompetencie sú kľúčovou zručnosťou 21. storočia a ich rozvíjanie sa týka takisto študentov Akadémie PZ v Bratislave. Významnú rolu v tomto edukačnom procese zohráva aj sociológia. Sociológia, ako spoločenská veda, umožňuje študentom lepšie pochopiť zložité spoločenské javy a procesy, podporuje schopnosti ich kritického myslenia vo vyhľadávaní sociálnych informácií a overovaní sociálnych faktov. Učí študentov hľadať pravdu a zároveň ju odlišovať od rôznych dezinformácií, ktoré ovplyvňujú kybernetickú bezpečnosť spoločnosti.
Kľúčové slová:
Digitálne kompetencie, sociológia, študent Akadémie Policajného zboru v Bratislave.

Abstract:
Digital competences are a key skill of the 21st century and their development also applies to students of the Academy of the Police Force in Bratislava. Sociology also plays an important role in this educational process. Sociology, as a social science, allows students to better understand the complex social phenomena and processes, supports their critical thinking skills in finding social information and validating social facts. It teaches students to seek the truth and at the same time to distinguish it from various misinformation that affect the company's cyber security.
Key words:
Digital competence, sociology, student of Academy of the Police Force in Bratislava.

Úvod

Služobná činnosť policajta je v súčasnej informačnej spoločnosti vo veľkej miere založená na práci s informáciami, ktorá zároveň vyžaduje získanie adekvátnych, špecificky zameraných spôsobilostí. Digitálne kompetencie nie sú iba elementárnou počítačovou gramotnosťou, ale zahŕňajú komplexný systém vedomostí a zručností, ktoré umožňujú policajtom aktívne vyhľadávať, zhromažďovať a správne vyhodnocovať bezpečnostné informácie, porozumieť ich kriminogénnemu, sociálno-patologickému a bezpečnostno-právnemu obsahu, v kontexte konkrétnej individuálnej, celospoločenskej i medzinárodno-bezpečnostnej situácie. Významnú rolu v rozvíjaní digitálnych kompetencií zohráva sociológia, ktorá podporuje schopnosti kritického myslenia študentov, učí ich hľadať pravdu, odlišovať ju od rôznych dezinformácií, efektívne komunikovať s občanmi, poskytovať im dôležité informácie a zároveň prijímať od nich podnety na boj proti kriminalite.

Sociologický pohľad na informačnú spoločnosť a jej vplyv na fungovanie bezpečnostného systému

Vznik pojmu „informačná spoločnosť“ súvisí s pokusmi charakterizovať relatívne novú vývojovú fázu západnej spoločnosti v 60-tých rokoch. V danom období vznikli tri významné vedecké koncepcie: „teória industriálnej spoločnosti“ (D. Bell, A. Toraine), „teória technotrónnej spoločnosti“ (Z. Brzezinski) a „teória informačnej spoločnosti“ (Y. Masuda). Spoločným menovateľom vzniku všetkých týchto teórií bola snaha analyzovať vplyv nových počítačových technológií na človeka a spoločnosť. Zaujímavou osobnou skúsenosťou pre autora tohto článku bola prednáška D. Bella v Bratislave, ktorá sa konala na pôde Sociologického ústavu SAV v marci 1988. Dnes, s odstupom času chápem pre mňa vtedy nepochopiteľné nadšenie D. Bella, s akým prezentoval svoju víziu fungovania globálnej sieťovej komunikácie, ktorá je dnes v podstate už realitou. V tom čase na Slovensku neboli k dispozícii žiadne osobné počítače a neexistovali ani sociálne siete, takže takto abstraktne formulovaná vízia sa pochopiteľne stretla skôr s úsmevom publika, než ocenením.

Na kvalitatívne zmeny v tzv. „technotrónnej spoločnosti“ založenej na nových technológiách upozornil Z. Brzezinski[1]. Niektoré z jeho tvrdení sa splnili, napr. závažné presuny pracovných síl z poľnohospodárstva do oblasti služieb, zmeny v oblasti vzdelávania, rozvoja masových prostriedkov atď. Iné, týkajúce sa napr. optimistických perspektív vnímania nezamestnanosti a sociálnych konfliktov sa nepotvrdili, ale naopak nové technológie priniesli iné, ešte radikálnejšie formy sociálnych konfliktov. Na niektoré novovzniknuté sociálne problémy v dôsledku rozvoja digitálnych technológií sa pokúša Z. Brzezinski aj upozorniť. Ide najmä o vytvorenie tzv. „globálneho gheta“[2], ktorého vznik môže byť zapríčinený nerovnomerným technologickým vývojom v rôznych častiach sveta.

Do spomínaných sociologických konceptov spoločnosti zaujímavým spôsobom vstupuje japonský vizionár Y. Masuda, označovaný aj ako priekopník tzv. „informačnej spoločnosti“. Y. Masuda, veľmi výstižne formuloval sociologickú charakteristiku informačnej spoločnosti. Pri koncipovaní svojej teórie vychádzal z toho, že dejiny ľudskej spoločnosti doteraz ovplyvnili najmä tieto tri faktory: poľovníctvo, poľnohospodárstvo a priemysel. Dnes sú to podľa Masuda informačné technológie, ktoré spôsobili vznik tzv. informačnej spoločnosti. Jej charakteristické znaky Masuda formuloval nasledovne: [3]

- technologický vývoj spoločnosti bude určovaný „informačnými technológiami,“
- extrémny nárast informačných produktov a technológii založených na vedení spôsobí „informačnú revolúciu,“
- vznik nových sociálnych symbolov,
- verejná infraštruktúra bude tvorená počítačovou základňou,
- rozbitie tradičných byrokratických štruktúr a vytvorenie „matricového modelu“ riadenia,
- lokálne komunity ľudskej pospolitosti budú nahradené informačnými komunitami, v ktorých budú uskutočňované všetky sociálne aktivity,
- tieto komunity budú odrážať vysoký stupeň autonomizácie,
- v súvislosti s novou infraštruktúrou spoločnosti vzniká participatívna demokracia, kedy každý, kto bude napojený na siete, bude môcť zasahovať do riadenia spoločnosti,
- nová spoločnosť prinesie krízu kontrolných mechanizmov a do popredia vystúpia také kategórie, ako je sebadisciplína a sebakontrola indivídua, ktoré budú vo vzájomnej harmónii.

Okrem pozitívnych Masudových vízií o vplyve informačných technológií na tzv. participatívnu demokraciu je zaujímavý jeho postreh týkajúci sa „krízy kontrolných mechanizmov“. Polícia je nástrojom sociálnej kontroly spoločnosti, nástrojom kontroly dodržiavania sociálnych (právnych) noriem, nástrojom kontroly kriminality v tom najširšom slova zmysle. V tejto súvislosti vzniká viacero otázok týkajúcich sa najmä vplyvu informácií na fungovanie a činnosť policajnej organizácie, ako aj na samotnú spoločenskú kontrolu kriminality.

Jeden z kritikov informačnej spoločnosti M. Crozier poukázal na negatívny vplyv informácií v byrokraticko-administratívnej činnosti modernej organizácie, čo sa bezprostredne dotýka mechanizmu fungovania celého bezpečnostného systému štátu. Bezpečnostný systém štátu totiž existuje a funguje ako byrokratický systém. V tomto konštatovaní nie je nič impertinentné. Je to jednoducho reálny fakt. Byrokracia zasahuje do všetkých oblastí života

[1] BRZEZINSKI, Z. *Between Two Ages. American’s Role in the Technetronic Era.* New York: Basic Books. 1970. s. 9-14.
[2] BRZEZINSKI, Z. *Between Two Ages. American’s Role in the Technetronic Era.* New York: Basic Books. 1970. s. 44-46.
[3] MASUDA, Y. *The Information Society and Post-Industrial Society*. Washington: World Future Society, 1980. s. 29–33.

modernej spoločnosti, bezpečnostnú oblasť nevynímajúc. Riadenie bezpečnosti, tak ako riadenie spoločnosti vyžaduje určitú štandardizáciu a unifikáciu postupov.

Riadenie bezpečnostného systému je v podstate riadením byrokratického systému. Byrokratický systém neosobných pravidiel moderného štátu sa stal neodmysliteľnou súčasťou výkonu jeho moci a administratívnej kontroly ľudí aj v bezpečnostnej oblasti. Byrokracia, tak ako v iných oblastiach riadenia, aj v procese riadenia bezpečnosti znižuje riziko svojvôle, improvizácie zamestnancov danej bezpečnostnej organizácie a vytvára normatívny systém konkrétnych úloh, postupov a krokov pri realizácií konkrétnej bezpečnostnej činnosti.

Byrokratické riadenie spoločnosti na jednej strane podľa Webera umožňuje účinnú verejnú správu, ale na strane druhej vytvára tzv. „železnú klietku racionalizácie". Mnohí členovia spoločnosti sa cítia byť obmedzení prísnymi byrokratickými pravidlami a hierarchiou neosobných inštitúcií so štandardizovanými postupmi, ktoré obmedzili slobodu jednotlivca. Byrokracia je nevyhnutná, ale kvôli administratívnej náročnosti, nezmyselnosti a samoúčelnosti prijímaných opatrení sa stáva terčom častej spoločenskej kritiky.

Kým Weber považoval byrokraciu za výraz účinnosti M. Crozier[4] spája byrokraciu s jej najdôležitejšou funkciou, špecifickou ochranou samotných byrokratov. Jej zmyslom je v podstate chrániť podriadených pred nadriadenými, nadriadených pred dôsledkami ich rozhodnutí a v konečnom dôsledku všetkých spoločne pred zodpovednosťou. Všetky informácie, hlásenia a obežníky slúžia skôr na vlastnú ochranu, než na informáciu iných. Vytvárajú nepreniknuteľnú vrstvu alibisticko-byrokratickej ochrany, ktorá v konečnom dôsledku blokuje akcieschopnosť organizácie. M. Crozier na to používa priliehavý názor: hovorí o „zablokovanej administratíve". Riadiaci pracovníci sú závislí na informáciách od svojich podriadených. Títo podriadení spravidla prispôsobujú informácie svojim záujmom a potrebe presvedčiť svojich nadriadených o vlastnej dôležitosti a opodstatnenosti svojej existencie. Riadiaci pracovníci preto rozhodujú tak, aby z ich rozhodnutí vyplynulo čo najmenšie riziko v prípade mylných informácií.

Byrokratický manažment v demokratickej spoločnosti znamená riadenie v súlade so zákonom a na základe relevantných, pravdivých a overených informácií. Význam informácií v procese riadenia je významný až do tej miery, že môžeme hovoriť o špecifickom informačnom manažmente, ako manažmente informačných zdrojov organizácie pre dosiahnutie jej stanovených cieľov. Informačný manažment sa stal samostatnou oblasťou manažmentu, ktorej obsahom je zber, spracovanie, riadenie a distribúcia informácií[5]. Informačný manažment v byrokratickom systéme nevyhnutne zápasí s administratívou informácií. Úloha prijímateľa a spracovávateľa informácií v tomto systéme riadenia je značne obmedzená, čo je v určitých situáciách dobre, v iných je to problém. Obzvlášť je to v prípadoch výskytu nepredvídateľných bezpečnostných hrozieb a práce s bezpečnostnými informáciami. Nie všetky scenáre krízového riadenia dokážu v súčasnej rizikovej spoločnosti vyčerpávajúcim spôsobom štandardizovať postupy bezpečnostných zložiek, resp. záchranných tímov. Nie každá bezpečnostná hrozba je „pokrytá" dostatočným množstvom informácií. Informačná spoločnosť v jednej oblasti poskytuje nepreberné množstvo informácií a zároveň v inej vytvára ich deficit. Nie vždy je bezpečnostnej oblasti dobré iba čakať na informácie z hora. Riziková spoločnosť vyžaduje výrazne zmeny aj v spôsobilosti bezpečnostných pracovníkov aktívne vyhľadávať, overovať a pracovať s bezpečnostnými informáciami.

Digitálne kompetencie v informačnej spoločnosti

Digitálne kompetencie sú štandardne označované za jednu z tzv. ôsmich kľúčových kompetencií pre celoživotné vzdelávanie, ktorými by mali disponovať všetci občania EÚ a ku

[4] CROZIER, M. *La société bloquée.* Paris: Seuil. 1970. s. 162-163.

[5] Podrobnejšie: VÁŇA, J. *Informačný manažment (Informácie – fenomén evolúcie ľudstva).* Bratislava: APZ, 2017. s. 240.

ktorým dospela EÚ v roku 2006. Kľúčové kompetencie pre uvedený rámec boli definované ako sebaisté a kritické využívanie digitálnych technológii, ktoré sú kombináciou nasledujúcich znalostí, zručností a prístupov, ktoré občania potrebujú v digitálnej spoločnosti: [6]

1. komunikácia v materinskom jazyku,
2. komunikácia v cudzích jazykoch,
3. matematická kompetencia a základné kompetencie v oblasti vedy a techniky,
4. digitálna kompetencia,
5. naučiť sa učiť,
6. spoločenské a občianske kompetencie,
7. iniciatívnosť a podnikavosť,
8. kultúrne povedomie a vyjadrovanie.

Digitálna kompetencia v uvedenom zozname patrí k tzv. „prierezovým" kompetenciám, tzn. k tým kompetenciám, ktoré napomáhajú zvládať aj iné kľúčové kompetencie. Ich charakteristickou črtou je prenositeľnosť, *tzn. možnosť ich synergického využitia v spojení s inými kompetenciami v nových a nepredvídaných situáciách. Typickými príkladmi takýchto prierezových kompetencií sú napr.*[7]*:*

- metodologické kompetencie *(riešenie problémov, používanie informačných a komunikačných technológií)*,
- komunikatívne kompetencie *(cudzie jazyky, písomné a ústne vyjadrovanie)*
- osobnostné kompetencie *(kritické myslenie, schopnosť tímovej práce, schopnosť učiť sa, sebariadenie, sebakontrola).*

Vývoj digitálnych kompetencií v EÚ je podrobne mapovaný na rôznych stránkach, ktoré ponúkajú podrobný prehľad o situácií v jednotlivých krajinách. Európska komisia vypracovala Európsky rámec digitálnych kompetencií pre občanov (DigComp)[8] je rozdelený do piatich oblastí:

1. Informačná a dátová gramotnosť (súvisí s prehľadávaním, vyhľadávaním, filtrovaním údajov a informácií, ich hodnotením a spracovávaním);
2. Komunikácia a spolupráca (využívanie údajov a informácií na interakciu, zdieľanie a zapojenie do občianskeho života a riadenia digitálnej identity);
3. Tvorba digitálneho obsahu (rozvoj digitálneho obsahu, jeho upravovanie, vylepšovanie, zdokonaľovanie a integrovanie do existujúceho súboru poznatkov, s cieľom vytvoriť nový, originálny a relevantný obsah);
4. Bezpečnosť (ochrana zariadení, osobných údajov, súkromia, zdravia, pohody a prostredia)
5. Riešenie problémov (riešenie technických problémov, identifikácia potrieb, tvorivé využívanie digitálnych technológií, identifikácia medzier v digitálnych kompetenciách ap.)

Spoločne obsahujú 21 kompetencií, ktoré sú skôr definované pre širokú občiansku verejnosť a pre všeobecné vzdelávanie. Uvedené kompetencie mapujú celý cyklus práce s informáciami, od ich vyhľadávania, cez ich spracovávanie, až po využívanie relevantných informácií v praktickom živote. Vo všeobecnosti takto definované kompetencie vymedzujú rámec aj pre vzdelávanie študentov bezpečnostno-právnych štúdií, ale nezohľadňujú niektoré

[6] Odporúčanie Európskeho parlamentu a Rady z 18. decembra 2006 o kľúčových kompetenciách pre celoživotné vzdelávanie (2006/962/ES). 2006. [online]. [cit. 2019-06-04]. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32006H0962&from=SK>

[7] Podrobnejšie viď.: Stratégia rozvoja slovenskej spoločnosti. 2010. [online]. [cit. 2019-06-04]. Dostupné na: <*http://archiv.vlada.gov.sk/old.uv/data/files/5613.pdf*>

[8] DIGCOMP 2.0. 2016. *The Digital Competence Framework for Citizens*. [online]. [cit. 2019-06-04]. Dostupné na: <https://ec.europa.eu/jrc/sites/jrcsh/files/DIGCOMP-FINAL-%20UPDATED%2002-06-2016.pdf>

špecifické kvality očakávané od príslušníkov bezpečnostných služieb. Ľ. Baričičová[9] vo svojom podnetnom príspevku upozorňuje na komplex faktorov, ktoré ovplyvňujú potrebu rozvoja informačnej kompetentnosti policajných manažérov v špecifickom prostredí polície. Okrem všeobecných faktorov, ktoré sa vzťahujú na informačnú podstatu samotného manažmentu, trendov v jeho vývoji, tvorbe a kultivácií informačných systémov, efektívnosti fungovania a využívania informačných systémov, autorka poukazuje aj na špecifické faktory vyplývajúce z informačnej podstaty policajnej práce.[10] Veľmi cenné na jej chápaní je to, že v popredí nevidí len odborné vedomosti, ale hlavné také kompetencie „ako sú myslenie v súvislostiach, riešenie problémov, hodnotenie rizika, ochota a schopnosť učiť sa, samostatnosť, komunikatívna a emocionálna inteligencia, zručnosť v informačno-komunikačných technológiách, ale tiež osobná flexibilita, čo predstavuje obsiahlu tvorivosť podporenú vysokou úrovňou vlastnej motivácie"[11].

Vplyv sociológie na rozvoj diagnosticko-poznávacej a analytickej spôsobilosti policajtov

Vzťah medzi sociológiou a rozvojom digitálnych kompetencií sa mnohým javí ako vzťah, ktorý je príliš abstraktný a veľmi vzdialený. Poniektorí jeho existenciu pripúšťajú nanajvýš s ironickým odôvodnením, „prečo nie veď napokon všetko so všetkým súvisí." Uvedený postoj žiaľ charakterizuje veľmi rozšírenú predstavu budúcich príslušníkov PZ o tom, že vo svojej budúcej policajnej praxi budú potrebovať iba praktické návody a právne normy. Ak chceme pochopiť v čom môže sociológia, ako veda o spoločnosti, napomôcť rozvíjať digitálne kompetencie budúcich príslušníkov PZ, v prvom rade si musíme uvedomiť v čom spočíva podstata policajnej práce a samotnej polície.

Zo sociologického hľadiska je polícia nástrojom udržiavania vnútorného poriadku, stability a sociálnej kontroly. Plní predovšetkým zákonom vymedzené úlohy vo veciach vnútorného poriadku, bezpečnosti a boja proti zločinnosti. Plnenie uvedených úloh je nemysliteľné bez existencie relevantných informácií, ktoré rozhodujúcim spôsobom determinujú akékoľvek bezpečnostné opatrenia zo strany polície. Bez adekvátnych, opodstatnených, overených a relevantných informácií, obsiahnutých napríklad v trestnom oznámení, nemôžu policajné orgány vykonávať svojvoľne žiadne úkony súvisiace s tzv. predsúdnym konaním. Ľ. Baričičová v tejto súvislosti dokonca hovorí o informačnej podstate polície a policajnej práce. Zdôrazňuje, že podstatou policajnej práce je predovšetkým práca s informáciami, ktoré sú podľa nej „pre prácu polície dôležitejšie ako čokoľvek iné."[12]

Informácie sa prelínajú všetkými úlohami a povinnosťami polície. Sú podnetom na začatie akéhokoľvek konania policajných orgánov (napr. vyšetrovanie trestnej činnosti), použitie donucovacích, či špecifických informačno-technických prostriedkov ap. Policajti sú povinní nielen získavať, uchovávať, spracovávať a odovzdávať relevantné informácie súvisiace s ich činnosťou, ale zároveň sú aj špecifickým orgánom na budovanie vlastných informačných systémov a databáz, ktoré vyplývajú zo zákona. Inými slovami povedané, polícia je nielen zberateľom, tvorcom a distribútorom informácií, ale aj relatívne samostatným

---

[9] BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018.* Bratislava: Akadémia PZ v Bratislave, 2018. s. 11-12.

[10] BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018.* Bratislava: Akadémia PZ v Bratislave, 2018. s. 11.

[11] BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018.* Bratislava: Akadémia PZ v Bratislave, 2018. s. 12.

[12] BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018.* Bratislava: Akadémia PZ v Bratislave, 2018. s. 11.

prevádzkovateľom a správcom informačných systémov (napr. informačného systému občianskych preukazov, cestovných dokladov, dopravných evidencií atď.).

Špecifickou zvláštnosťou informácií, s ktorými pracuje polícia je to, že sú to v podstate sociálne informácie. Informácie, ktoré sú sprostredkovávané sociálnymi subjektami (občanmi, spoločenskými inštitúciami, nástrojmi sociálnej komunikácie ap.), týkajú sa sociálnych subjektov (jednotlivcov, sociálnych skupín, organizácií, spoločnosti), najmä v oblasti zaisťovania ich bezpečnosti a spravidla tieto informácie majú aj sociálne (politické, trestno-právne, ekonomické, bezpečnostné ap.) dôsledky. Proces získavania, spracovávania a hodnotenia bezpečnostných informácií Policajným zborom determinuje taktiež množstvo sociálnych faktorov. Okrem subjektívnej optiky jednotlivých policajtov, ich kognitívnej, emocionálnej a hodnotiacej spôsobilosti je to celý rad vonkajších, zámerne i nezámerne pôsobiacich činiteľov. Sprostredkovateľom bezpečnostných informácií môžu byť nielen občania, oficiálne bezpečnostné inštitúcie (ozbrojené sily, spravodajské služby ap.), ale aj iné, neoficiálne zdroje (verejná mienka, médiá atď.). Rozhodujúci podiel na sprostredkovávaní informácií o činnosti polície majú obzvlášť médiá. V modernej spoločnosti je bezpečnosť oveľa viac než ktorákoľvek iná spoločenská sféra života objektom veľmi sugestívneho mediálneho pôsobenia. V dôsledku intenzívneho mediálneho tlaku vzniká nová mediálna (virtuálna) bezpečnostná realita, ako súčasť mediálnej a virtuálnej reality, v ktorej ľudia strácajú kontakt s reálnou skutočnosťou.

Sociálny charakter policajných, resp. bezpečnostných informácií spočíva taktiež v ich špecifických kriminogénno-sociálnych súvislostiach. Sociálne súvislosti zločinu spravidla zanechávajú po sebe špecifickú sociálnu stopu. Najmä v prípadoch organizovaného zločinu a sofistikovaných podvodov ide spravidla o široko rozvetvenú a dobre maskovanú sieť klientelizmu, korupcie, známostí, úplatkov a provízií. Existencia reálnej zločineckej „sociálnej pavučiny“, do ktorej sú zamotaní politici, podnikatelia (tzv. „biele goliere“), zvyšuje nároky na diagnosticko-poznávaciu činnosť a analytickú spôsobilosť policajta, ako aj na jeho občiansku statočnosť a morálnu odvahu. Od policajta sa vyžaduje predovšetkým dokonalá znalosť spoločenského prostredia a sociálnych vzťahov.

Hypokrates kedysi povedal: „telo nemožno pochopiť bez vecí, ktoré ho obklopujú“. Tak ako chirurg, skôr než dostane do rúk skalpel, musí dokonale poznať anatómiu ľudského tela, tak aj každý správny manažér policajno-bezpečnostnej praxe by sa mal usilovať pochopiť veci, ktoré obklopujú objekt jeho profesionálneho záujmu a predmet jeho policajno-bezpečnostnej činnosti. Spomínaný manažér má k dispozícii nespočetné množstvo informačných zdrojov a nástrojov obsiahnutých vo vedeckých disciplínach, systematicky sa zaoberajúcich človekom a ľudskou spoločnosť. Jedno z ústredných miest patrí bezpochyby sociológii, ktorú môžeme nazvať aj „spoločenskou anatómiou bezpečnostno-policajnej praxe“.

Zložité bezpečnostné situácie zvyšujú nároky na diagnosticko-poznávaciu činnosť a analytickú spôsobilosť policajta nielen vyhodnocovať prijaté informácie, ale aj samostatne získavať informácie a kvalifikovane k ním využívať základy vedeckého poznávania (analýzy, syntézy, dedukcie, indukcie a komparácie). Získané vedomosti zo sociológie môžu budúcim policajtom účinne napomôcť k samostatnej orientácii v zložitom a dynamickom bezpečnostnom prostredí, pri analýze sociálnych súvislostí kriminality a v tvorivej aplikácii teoretických poznatkov na riešenie konkrétnych policajno-bezpečnostných problémov a situácií. Sociologicko-politologický spôsob myslenia a analýzy núti budúceho policajta k objektivite, kritickému premýšľaniu, učí ho zovšeobecňovať, vidieť v individuálnom sociálne a v konkrétnom všeobecné.

Vzhľadom na uvedené požiadavky je základným cieľom výučby sociológie na Akadémii PZ v Bratislave poskytnúť všetkým študentom adekvátny systém poznatkov zo všeobecnej sociológie, sociologického výskumu a vybraných aplikovaných sociologických disciplín, ktoré môžu využiť pri štúdiu nadväzujúcich profilujúcich predmetov (policajného

manažmentu, vybraných policajno-bezpečnostných služieb, ale aj kriminológie, kriminalistiky, teórie trestného práva ap.). Dôraz je však položený predovšetkým na potreby ich budúcej policajnej praxe. Absolvent školy by mal podľa schválených učebných programov získať relevantný súbor vedomostí o spoločnosti, jej vývoji, štruktúre a fungovaní. Dôraz je položený najmä na poznatky o aktuálnych spoločensko-politických, etnických, socio-kultúrnych a demografických procesoch, ktoré ovplyvňujú existenciu sociálno-patologických javov a deviácií, výskyt rôznych sociálnych konfliktov, násilia, kriminality a nových foriem organizovaného zločinu.

Aplikatívne možnosti využitia sociológie pri poznávaní policajno-bezpečnostných situácií spočívajú taktiež v tom, že sociológia má k dispozícii dostatočný metodologický aparát, umožňujúci kvalifikovanú analýzu sociálnej skutočnosti, ktorá je často objektom policajnej práce. Najmä sociologický výskum, ako špecifický výskumný postup zameraný na skúmanie spoločenských javov, nadobúda veľmi konkrétnu aplikatívnu funkciu v "policajno-bezpečnostnom výskume" pri získavaní informácií o sociálnych javoch, súvisiacich s policajno-bezpečnostnou problematikou. Sociológia prostredníctvom sociologického výskumu môže sprostredkovať policajným vedám aktuálne empirické údaje z rôznych oblastí spoločenského života.

Je pochopiteľné, že zmyslom výučby sociologických metód poznávania nie je urobiť z policajtov sociológov - výskumníkov, v tom lepšom prípade vyškolených anketárov. Zvládnutie všeobecných zásad vedeckého poznávania je skôr nevyhnutné z iných dôvodov. Sociológia pomocou vedeckých metód poznávania spoločnosti napomáha rozvíjať osobnú skúsenosť policajta (jeho tzv. „zdravý rozum“) a umožňuje mu pozerať sa na spoločenské udalosti spôsobom, ktorý G.W. Mills nazval „sociologickou imagináciou“. Táto imaginácia napomáha vidieť jednotlivé bezpečnostné udalosti a javy v širších spoločenských súvislostiach, vo väzbe na konkrétne sociálne problémy a z viacerých sociologických perspektív. Sociologický spôsob myslenia a analýzy núti policajta k objektivite, kritickému premýšľaniu, učí ho zovšeobecňovať a vidieť v „individuálnom sociálne a v konkrétnom všeobecné.“[13]

Aplikácia sociológie pri digitálnej tvorbe krízových scenárov

Rozvoj digitálnych kompetencií je rovnako dôležitý aj v príprave študentov bezpečnostno-právnych služieb vo verejnej správe. Využitie sociologických informácií zo širokej palety aplikačných možností môžeme ilustrovať na príklade tvorby krízových scenárov. Ich digitálna podoba je v dnešnej dobe samozrejmosťou. Pomocou výpočtovej techniky je možné simulovať rôzne scenáre a varianty. Konštruktívne alebo virtuálne simulácie, založené na výpočtovej technike nahradzujú ľudský objekt a tým umožňujú ľubovoľne modelovať akékoľvek podrobnosti a krízové situácie v ktoromkoľvek geografickom regióne, bez ohľadu na ekologické a sociálne dôsledky.

Napriek nespochybniteľným informačno-technickým výhodám tohto spracovávania nesmieme zabúdať na jeden dôležitý fakt. Každé bezpečnostné riziko má špecifický sociálny rozmer a sociálne osobitosti. Dôvodom podľa U. Becka je po prvé to, že riziko vzniká vždy v určitom sociálnom systéme; po druhé, rozsah rizika je funkciou kvality sociálnych vzťahov a procesov; a po tretie, stupeň rizika závisí od expertov a expertných znalostí[14]. Pre bezpečnostné riziká sú z tohto dôvodu prakticky spoločné všetky charakteristické vlastnosti, ktoré sú typické aj pre mnohé ďalšie sociálne javy a procesy, tzn.:

- spontánnosť a neopakovateľnosť - spoločenské udalosti nemôžeme zastaviť (vrátiť späť), resp. zopakovať, z čoho vyplýva obmedzenosť použitia experimentu.

[13] URBAN, L. *Sociologie.* Praha: Eurolex Bohemia, 2006. s. 46.
[14] BECK, U. *Riziková společnost - Na cestě k jiné moderně.* Praha: SLON, 2004.

- originálnosť - dva javy týkajúce sa toho istého problému nie sú nikdy identické – ani záchranné práce počas povodní
- senzitívnosť (emocionalita) – človek je spravidla súčasťou prebiehajúcich spoločenských procesov, čo výrazne ovplyvňuje jeho psychiku, správanie, postoje, objektívnosť a nezávislosť.
- nadindividuálny charakter – prejavuje sa vonkajším tlakom na jednotlivca (napr. verejná mienka).
- spoločenské javy majú kvantitatívnu aj kvalitatívnu stránku - každý spoločenský jav má určitú dimenziu, rozsah a intenzitu (napr. pracovná spokojnosť môže byť veľmi vysoká, ale aj veľmi nízka). Z jednoty kvantity a kvality vyplýva kvantitatívna a kvalitatívna metodológia v sociologickom výskume.
- pravdepodobnostný charakter – na rozdiel od fyzikálnych javov, sociálne sú mnohostranné a podmienené viacerými neočakávanými, situačnými faktormi, ktoré nemôžeme tak jednoznačne a presne vypočítať.

V uvedenom kontexte sociologický spôsob myslenia má veľký význam v činnosti pracovníkov bezpečnostno-právnych služieb napríklad pri sociologickej analýze špecifických zvláštností bezpečnostných javov, procesov a situácií, ktoré sa stávajú súčasťou tvorby krízových scenárov, najmä v tom, že:

1. Bezpečnostné javy majú oveľa silnejšie a intenzívnejšie sociálno-deštruktívne dôsledky.
2. Možnosti identifikácie a skúmania bezpečnostných javov sú oveľa obmedzenejšie (skrytejšie). Najmä v dôsledku subjektivizmu expertných systémov a zložitej štruktúry skúmaných javov.
3. Percepcia (vnímanie) bezpečnostných javov sa vyznačuje väčšou emocionalitou (vyvolávajú väčšie obavy a strach) - možnosť skreslenia, manipulácie, vplyv médií (neodôvodnené obavy).

Bezpečnostné hrozby a riziká nadobudli oveľa širší sociálny rozmer a kvalitatívne nové sociálne osobitosti najmä v súčasnej etape vývoja spoločnosti. Bezpečnostné riziká vznikajúce v súčasnej rizikovej spoločnosti podľa U. Becka sú takého charakteru, že ich nemožno sociálne ohraničiť. V predindustriálnej spoločnosti boli riziká lokálne ohraničené, hierarchicky usporiadané podľa bohatstva, spoločenskej triedy ap. Kým napr. bieda v minulosti zasahovala len časť, prevažne chudobnej populácie, atómové riziká dnes postihujú všetky životné formy bez rozdielu bohatstva, triednej príslušnosti a to globálne. „Zatiaľ čo bieda je hierarchická, smog je veľkoryso demokratický“, tvrdí U. Beck[15].

Dôležitým sociologickým aspektom v tvorbe krízových scenárov[16] je skutočnosť, že uvedené scenáre sú špecifickým sociálnym konštruktom, sú vytvorené ľuďmi (na základe ich poznatkov, ale aj potrieb, záujmov, cieľov a možností), sú o ľuďoch a pre ľudí. Úprimná snaha niektorých teoretikov čo najviac zdokonaliť a sofistikovať tvorbu krízových scenárov často vedie k opačnému efektu. To, čo by malo byť jednoduché, jasné a zrozumiteľné sa stáva príliš komplikovaným, nejasným a nezrozumiteľným. V matematických funkciách, algoritmoch, kalkuláciách sa stráca podstatné, tzn. to, že krízové scenáre sú o ľuďoch a pre ľudí. Adresátmi i užívateľmi krízového scenára v konečnom dôsledku sú ľudia, ktorí by im mali rozumieť za každých okolností a ktorí by mali podľa týchto scenárov ľahko pochopiť svoje poslanie i úlohy.

Dominantným v obsahu krízového scenára preto nie je technický popis katastrofy, ale najmä návod akým spôsobom by mali kompetentní ľudia reagovať bez toho, aby museli dlho

---

[15] BECK, U. *Riziková společnost - Na cestě k jiné moderně.* Praha: SLON, 2004. s. 47.

[16] Podrobnejšie viď.: BUZALKA, J., BLAŽEK, V., DWORZECKI, J., URBANEK, A. a kol. *Rozvoj bezpečnostných rizík a tvorba krízových scenárov pre verejnú správu.* Bratislava: Akadémia Policajného zboru v Bratislave, 2014.

premýšľať a strácať drahocenný čas. To, že krízový scenár je o predovšetkým o ľuďoch znamená, že by mal predvídať nielen fungovanie a stabilitu technických, či zabezpečovacích systémov, ale mal by predvídať aj správanie a reakcie ľudí v krízových situáciách. Správanie a reakcie ľudí v krízových situáciách sú často rozhodujúce pre úspešne vykonávanie záchranných prác a dodržiavanie naplánovaných postupov. Okrem štandardizovaných postupov by mal obsahovať aj varianty atypických a neštandardných situácií.

Ak akceptujeme uvedené skutočnosti, že bezpečnostné riziká sú vo svojej podstate sociálne javy a procesy, resp. každé bezpečnostné riziko má svoje špecifické sociálne osobitosti, je logické, že aj krízové scenáre, ktorých cieľom je minimalizovať negatívne dopady týchto rizík, resp. minimalizovať dezintegráciu určitého subjektu musia rešpektovať uvedené skutočnosti a pri ich tvorbe je nutné zohľadňovať sociologické aspekty. Bez využitia sociologickej imaginácie by sme pravdepodobne nedokázali rekonštruovať vzorce správania ľudí v odlišnom socio-kultúrnom prostredí. Na vytvorenie reálneho obrazu preto nestačí iba analyzovať postupy a jednotlivé kroky záchranných zložiek a vyhodnocovať ich efektívnosť. Komplexná príprava vyžaduje znalosť mentality, možných reakcií ap.

Sociálne správanie je správanie podmienené skupinovými vplyvmi. Z hľadiska cieľov, ktoré uvedené spoločenské vplyvy sledujú, rozlišujeme prosociálne a antisociálne správanie.

Z hľadiska organizačnej formy rozlišujeme:

- organizované správanie (resp. inštitucionalizované správanie)
- neorganizované – spontánne – kolektívne správanie

V rámci vykonávanej záchrannej činnosti musíme plánovať nielen organizované formy správania, ale treba počítať aj z tzv. neorganizovanými, tzn. kolektívnymi formami správania. Kolektívne správanie *(*collective behaviour) je prevažne emocionálne spontánne, neštruktúrované sociálne správanie, ktoré vzniká ako reakcia väčšieho množstva ľudí na neštandardné a neurčité sociálne situácie, javy a procesy. Do sociológie uviedol tento pojem Robert Ezra Park, vedúci predstaviteľ tzv. Chicagskej školy, ktorý ho použil v roku 1930 pre relatívne spontánne, neinštitucionalizované správanie. Snahou bolo odhaliť protiklad typu inštitucionalizovaného, organizovaného správania. Medzi základné druhy kolektívneho správania patrí: dav a davové správanie, panika, masová hystéria, fáma, verejná mienka ap.

Kolektívne správanie je:

- hromadné správanie (správanie väčšieho množstva ľudí, uskutočňované v rovnakom čase, pričom títo ľudia môžu ale aj nemusia byť v priamom fyzickom kontakte),
- spontánne, neštruktúrované a neinštitucionalizované správanie (vnútorne neorganizované a neusporiadané, odohrávajúce sa bez existencie vopred stanovených pravidiel). Je to nepredvídateľné a ťažko predvídateľné správanie z hľadiska jeho vývoja,
- vzniká a vyvíja sa ako kolektívna reakcia ľudí na vplyvy, resp. podnety, stimuly, ktorými sú neštandardné (výnimočné, zriedkavé) a nejasné, nejednoznačné javy, procesy a ich výsledky.

Kolektívne správanie je špecifický proces, v ktorom spravidla rozlišujeme nasledujúce štádiá:

1. Štruktúrnu podporu – v sociálnej štruktúre musí byť zabudovaná možnosť vzniku kolektívneho správania. Niektoré zvláštnosti štruktúry spoločnosti umožňujú vznik kolektívneho správania viac, iné menej. (napr. v spoločnosti tvorenej ľuďmi jednej rasy nevznikajú rasové nepokoje).

2. Štruktúrne napätie – existujúce usporiadanie spôsobuje, že za určitých okolností sa situácia dramatizuje, stáva sa neprehľadnou, problémovou, vzniká súbor negatívnych sociálno-psychických stavov vyvolávajúcich napätie a konflikty.
3. Prijatie všeobecného presvedčenia – existujúce napätie musí byť nejakým spôsobom vysvetlené. Tento všeobecne prijímaný názor sa spája s návrhom na riešenie. Nemusí ísť o racionálne riešenie.
4. Spúšťajúca udalosť (faktor) – vo všetkých prípadoch existuje neočakávaná, náhla udalosť, ktorá iniciuje, podnieti ku kolektívnemu správaniu („rozbuška“).
5. Mobilizácia (aktivizácia) ľudí – pre určitý druh kolektívneho správania môže prebiehať pred výskytom i po výskyte neočakávanej udalosti. Ak k mobilizácii dochádza až po udalosti, táto môže prebiehať dvoma spôsobmi: spontánne alebo organizovane. V druhom prípade sa utvoria skupinky vodcov, ktorí plnia rolu iniciátorov a organizátorov kolektívneho správania.
6. Pôsobenie mechanizmov sociálnej kontroly – nevhodný zásah polície môže odštartovať kolektívne správanie.

Najčastejším druhom kolektívneho správania, s ktorým musíme počítať už pri tvorbe krízových scenárov je najmä panika. Panika je špecifický druh kolektívneho správania, ktorým ľudia neprimerane reagujú na určitý podnet (krízový jav, krízovú situáciu, mimoriadnu udalosť). Ide o emocionálny, spontánny, neprimeraný a často i bezohľadný alebo seba zničujúci spôsob reakcie. Podľa druhu stimulu sa panika rozlišuje na:

- útekovú (únikovú) paniku – podnetom býva vznik nejakého ohrozenia zdravia alebo životov ľudí zhromaždených na jednom mieste (požiar budovy, zemetrasenie, hroziaci výbuch bomby)
- získavaciu (chamtivú) paniku – nákupná panika
- Vznik paniky urýchľuje celý rad faktorov a podmienok:
- ľudia si musia uvedomovať výnimočnosť a krízový charakter situácie, v ktorej sa ocitli
- musia pociťovať neistotu, vzrušenie, úzkosť alebo strach z tejto situácie
- musia uveriť, že existuje iba jedno, resp. najlepšie riešenie
- musia byť presvedčení, že ostatné riešenia sú nevhodné, neefektívne, alebo že iné riešenia neexistujú
- v dave zlyháva komunikácia – výsledkom čoho je zlá informovanosť
- v dave neexistuje spolupráca, vzájomná pomoc, koordinácia, prípadne vodcovstvo a usmerňovanie
- medzi členmi davu sú ľudia s psychickou predispozíciou prepadnúť panike
- v dave existuje vzájomná stimulácia – dav umožňuje vznik davovej nákazy

Panika, tak ako aj ostatné druhy kolektívneho správania využíva princípu kumulácie, nabaľovania, „efekt snehovej gule“. Krízový scenár musí počítať s tým, že záchranné práce sa nebudú uskutočňovať v sterilných, laboratórnych podmienkach, ale vo vyhrotenej, psychicky veľmi náročnej, záťažovej situácii, s množstvom rušivých vplyvov. Z uvedeného dôvodu je potrebné premyslieť aké správanie u ľudí treba predvídať, tzn. vytvoriť typológiu scenárov neštandardizovaného správania v krízovej situácii, v ktorých sú zobrazené predpokladané reakcie obetí a ich širšieho sociálneho okolia.

Záver

Digitálne kompetencie sú neodmysliteľnou súčasťou práce príslušníkov PZ a zamestnancov v oblasti bezpečnostno-právnych služieb vo verejnej správe. V podmienkach narastajúcich nových bezpečnostných rizík, sociálnej radikalizácie a vzniku atypických sociálno-patologických javov je táto príprava objektívnou nevyhnutnosťou.

Získané vedomosti zo sociológie môžu budúcim absolventom Akadémie PZ účinne napomôcť k samostatnej orientácii v zložitom a dynamickom bezpečnostnom prostredí, pri analýze sociálnych súvislostí výskytu bezpečnostných rizík a v tvorivej aplikácii teoretických poznatkov na riešenie konkrétnych problémov a situácií.

Sociologický spôsob myslenia a analýzy núti budúceho bezpečnostného manažéra k objektivite, kritickému premýšľaniu, učí ho zovšeobecňovať, vidieť v individuálnom sociálne a v konkrétnom všeobecné. Na záver je nutné pripomenúť aj veľmi dôležitú myšlienku Ľ. Baričičovej, ktorá označuje za chybu zastarané nazeranie na informačné technológie optikou doterajších procesov, tzn. ich využívanie na to, „čo robíme“ a nie na to, čo „sme doteraz nerobili“[17].

Zoznam použitej literatúry:

1. BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality*. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018. Bratislava: Akadémia PZ v Bratislave, s. 11-12. ISBN 978-80-8054-773-8.
2. BECK, U. *Riziková společnost*. Na cestě k jiné moderně. Praha: SLON, 2004, ISBN 80-86429-32-6.
3. BRZEZINSKI, Z. *Between Two Ages*. American's Role in the Technetronic Era. New York: Basic Books, 1970. ISBN 978-0313234989.
4. BUZALKA, J., BLAŽEK, V., DWORZECKI, J., URBANEK, A. a kol. *Rozvoj bezpečnostných rizík a tvorba krízových scenárov pre verejnú správu.* Bratislava: Akadémia Policajného zboru v Bratislave, 2014. ISBN 978-80-8054-589-5.
5. CROZIER, M. *La société bloquée*. Paris: Seuil, 1970. ISBN: 978-2020232142.
6. DIGCOMP 2.0. *The Digital Competence Framework for Citizens*. [online]. [cit. 2019-05-07]. Dostupné na: <https://ec.europa.eu/jrc/sites/jrcsh/files/DIGCOMP-FINAL-%20UPDATED%2002-06-2016.pdf>
7. MASUDA, Y. *The Information Society and Post-Industrial Society*. Washington: World Future Society, 1980. ISBN: 978-0930242152.
8. Odporúčanie Európskeho parlamentu a Rady z 18. decembra 2006 o kľúčových kompetenciách pre celoživotné vzdelávanie (2006/962/ES). [online]. [cit. 2019-05-07]. Dostupné na:<https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32006H0962&from=SK>
9. Stratégia rozvoja slovenskej spoločnosti. 2010. [online]. [cit. 2019-05-07]. Dostupné na: <http://archiv.vlada.gov.sk/old.uv/data/files/5613.pdf>
10. URBAN, L. *Sociologie*. Praha: EUROLEX BOHEMIA, 2006. 373 s. ISBN: 80-86861-45-7.
11. VÁŇA, J. *Informačný manažment (Informácie – fenomén evolúcie ľudstva).* Bratislava: APZ, 2017. 287 s. ISBN 978-80-8054-737-0.

Kontaktné údaje:

Doc. Karol Murdza, PhD.
Katedra spoločenských vied
Akadémia PZ v Bratislave
karol.murdza@minv.sk

[17] BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov s medzinárodnej vedeckej konferencie konanej dňa 21.3.2018.* Bratislava: Akadémia PZ v Bratislave, 2018. s. 11.

Aktuálny pohľad na vývoj v oblasti zaisťovania kybernetickej bezpečnosti a ochrany informácií na národnej a nadnárodnej úrovni

Pavel Nečas, Radoslav Ivančík

Abstrakt:
Sektor komunikačných a informačných technológií v súčasnosti predstavuje jednu z najrýchlejšie sa rozvíjajúcich oblastí spoločnosti. Vďaka rozvoju týchto technológií sa v dnešnom modernom svete stali hranice, vzdialenosti a čas relatívnejšími. Bola vytvorená nová doména – kybernetický priestor. S kontinuálnym prehlbovaním prepojenosti a závislosti v kybernetickom priestore však narastá aj zraniteľnosť jednotlivých aktérov. Hrozby v kybernetickom priestore majú široký rozmer, preto sa čoraz dôležitejšou a naliehavejšou stáva ochrana informácií a zaistenie kybernetickej bezpečnosti.
Kľúčové slová:
Kybernetická bezpečnosť, komunikačné a informačné technológie, ochrana informácií.

Abstract:
The sector of communication and information technologies is currently one of the fastest growing areas of the human society. Thanks to the development of these technologies, in today's modern world, borders, distances and time have become more relative. A new domain was created - cyberspace. However, the perceived vulnerability of participating actors is increasing with the continuing deepening of interconnection and dependence in cyberspace. Threats in cyberspace are wide-ranging, and therefore, information protection and cyber security are becoming increasingly important and urgent.
Key words:
Cyber security, communication and information technologies, information protection.

Úvod

Sektor komunikačných a informačných technológií (ďalej len „KIT“) v súčasnosti predstavuje jednu z najrýchlejšie sa rozvíjajúcich oblastí spoločnosti. Výrazne sa premieta nielen do súkromnej a hospodárskej sféry, ale čoraz viac aj do štátnej a verejnej správy, a tým aj do oblasti bezpečnosti a obrany. 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 KIT. Súčasne tým dochádza nielen k zvyšovaniu ich vzájomnej prepojenosti, ale aj k nárastu ich vzájomnej závislosti. Vedecko-technický a technologický pokrok tak prináša nielen nové benefity, príležitosti a výzvy, ale aj isté negatíva[1] spojené s novými bezpečnostnými rizikami a hrozbami. Preto sa čoraz dôležitejšou a naliehavejšou stáva ochrana informácií, kybernetického priestoru a kritickej informačnej infraštruktúry, čiže zaistenie kybernetickej bezpečnosti.

Vďaka rozvoju KIT sa v dnešnom modernom svete stali hranice, vzdialenosti a čas relatívnejšími. Bola vytvorená nová doména – kybernetický priestor. S kontinuálnym

[1] K hlavným negatívnym stránkam spoločnosti založenej na informáciách patrí predovšetkým:
- strata súkromia spôsobená interpersonálnou komunikáciou prostredníctvom elektronických médií,
- strata sociálnych väzieb,
- nebezpečenstvo informačného pohltenia vyvolaného informačnou explóziou,
- existencia informačnej vojny, či informačného “smogu” so snahou o šírenie dezinformácií,
- zvýšený rozmach počítačovej kriminality s prvkami veľmi nebezpečnej trestnej činnosti organizovanej v kyberpriestore,
- možná selekcia spoločnosti na informačne bohatých a chudobných z pohľadu ich počítačovej gramotnosti, či dostupnosti nových informačno-komunikačných technológií,
- rôzne filozofické, etické i zdravotné problémy.

Pozri: BARIČIČOVÁ, Ľ. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018. s. 10.

prehlbovaním prepojenosti a závislosti v kybernetickom priestore však narastá aj vyššie zmienená zraniteľnosť jednotlivých aktérov. Hrozby v kybernetickom priestore majú široký rozmer. Môže ísť o nezákonný zber informácií o jednotlivcovi, skupine alebo organizácii či už aktívnou alebo pasívnou cestou, prípadne môže ísť o organizovaný zločin, ktorý tento priestor zneužíva ako prostriedok na nelegálny zisk. Kybernetický priestor môže byť taktiež zneužitý na šírenie a propagáciu rôznych extrémistických názorov a podporu terorizmu. Zároveň môže ísť aj o hackerské útoky vedené s cieľom poškodiť jednotlivca, skupinu alebo organizáciu. Najextrémnejšou potenciálnou hrozbou je uskutočnenie kybernetických útokov namierených voči kritickej infraštruktúre štátu, čo môže mať výrazný negatívny dopad na bezpečnosť a obranu štátu a životy a zdravie jeho občanov.

Vývoj v ostatných rokoch ukázal, že kybernetický priestor je zároveň prostredím na presadzovanie národných záujmov, čoho dôkazom sú kybernetické útoky namierené proti určitým krajinám ako doplnok alebo súčasť politického či vojenského konfliktu. Tieto udalosti dokazujú, že štát ako najzákladnejšia entita postvestfálskeho medzinárodného systému čelí novému druhu hrozieb – kybernetických hrozieb – v dynamicky sa vyvíjajúcom bezpečnostnom prostredí, pričom s narastajúcou závislosťou na informačných a telekomunikačných technológiách je pre každý štát životne dôležité riešiť otázky vlastnej bezpečnosti a obrany v kybernetickom priestore.

Bezpečnosť[2] kybernetického priestoru si vyžaduje širokú škálu ochranných, obranných aj záchranných opatrení, ktoré je potrebné vykonať za účelom minimalizovania následkov potenciálneho útoku protivníka. Z pohľadu ochranných opatrení táto škála môže predstavovať národnú politiku v správaní sa v kybernetickom priestore, odbornú a informačnú prípravu obyvateľstva a odborného personálu s prístupom k informačným a telekomunikačným technickým prostriedkom formou posilňovania bezpečnostného povedomia, ako aj aktualizáciu a nastavenia adekvátnych softwarových a hardwarových štandardov, ktorých cieľom je minimalizovať potenciálne riziká plynúce pre informačné a komunikačné technické prostriedky.

Obranné opatrenia predstavujú defenzívne, ofenzívne a spravodajské aktivity, ktoré je nutné realizovať v prípade prebiehajúceho útoku s cieľom takýto útok zastaviť a zabrániť tak útočníkovi v spôsobovaní škôd. Teóriu vychádzajúcu z diela Carla von Clausewitza, že boj obsahuje dve časti – obranu a útok, je možné plnohodnotne aplikovať aj v prípade boja v kybernetickom prostredí, nakoľko kybernetický boj zahŕňa tak defenzívne, ako i ofenzívne aktivity. Defenzívne aktivity sú zamerané na zabránenie útočníkovi vykonávať, resp. pokračovať v kybernetickom útoku. Cieľom ofenzívnych aktivít je oslabenie alebo úplná eliminácia protivníkových kybernetických a eventuálne aj kinetických spôsobilostí s cieľom zlomenia jeho vôle bojovať. Za kombináciu defenzívneho a ofenzívneho elementu je možné považovať kybernetické operácie zamerané na zber spravodajských informácií.

Aj preto problematika ochrany informácií a kybernetickej bezpečnosti a obrany jednoznačne zaujíma v rámci Severoatlantickej aliancie (ďalej len „NATO“) a Európskej únie (ďalej len „EÚ“) neustále prominentnejšiu úlohu. Na druhej strane je možné konštatovať, že Aliancia i Únia sa začali touto témou vážnejšie zaoberať až počas ostatných rokov. Ešte pred pár rokmi, boli kybernetické hrozby a súvisiace bezpečnostné problémy a otázky diskutované iba v úzkych kruhoch technikov a expertov.

[2] *Poznámka*: Všeobecne platí, že v systémoch každý dej, jav alebo proces prebieha v štandardných podmienkach spôsobom, ktorý je možné s určitou pravdepodobnosťou predvídať a popísať, príp. ktorý je priamo plánovaný. V uvedených prípadoch možno vo všetkých oblastiach života (v prírode i spoločnosti) hovoriť o bezpečnosti (BELAN, L. *Vlastnosti bezpečnosti*. 2016. s. 32.)

Po prvých vážnych kybernetických útokoch namierených proti určitým krajinám ako doplnok alebo súčasť politického či vojenského konfliktu[3] však prišlo na národnej i nadnárodnej úrovni k zásadnému uvedomeniu si faktu, že kybernetický svet znamená vážnu zraniteľnosť pre stále viac vzájomne prepojené spoločenstvá (zoskupenia), NATO a EÚ nevynímajúc. Kybernetické útoky patria medzi tie bezpečnostné hrozby, ktorým budú štáty i zoskupenia musieť čeliť v nasledovných rokoch stále výraznejšie. Kybernetické konflikty sa postupne stávajú súčasťou tradične vedených konfliktov, a preto „digitalizované" krajiny i zoskupenia musia pracovať na konkrétnych plánoch a opatreniach ako zabezpečiť ochranu informácií a bezpečnosť a obranu svojho kybernetického priestoru, a tým aj svojich individuálnych i kolektívnych záujmov.

Nové kybernetické bezpečnostné hrozby a riziká

Kybernetické hrozby sú vo všeobecnosti považované za nové, vznikajúce a vyvíjajúce sa asymetrické bezpečnostné hrozby. Prvýkrát bola problematika kybernetickej obrany spomenutá v Strategickej koncepcii Severoatlantickej aliancie z roku 1999. Na samite vo Washingtone NATO vôbec po prvýkrát vo svojom oficiálnom dokumente zaradilo informačné systémy a závislosť NATO na nich medzi potenciálne hrozby pri eliminácii prevahy Aliancie v tradičných zbraňových systémoch.[4] Následne, rok po dátume 11. 9. 2001, ktorý sa ukázal byť ako prelomový vo vnímaní nových bezpečnostných hrozieb a rizík, vydalo NATO „výzvu k zdokonaleniu schopností nutných pre obranu proti kybernetickým útokom" v rámci záväzku k spôsobilostiam, vyhláseným počas samitu v Prahe, v novembri 2002.[5] V nasledujúcich rokoch sa však Aliancia orientovala predovšetkým na implementáciu pasívnych ochranných opatrení, ktoré vyžadovali ozbrojené sily.

Až udalosti v Estónsku, na jar roku 2007, prinútili NATO k radikálnemu prehodnoteniu koncepcie kybernetickej obrany a k príprave protiopatrení nového formátu. Aliancia preto vypracovala po prvýkrát oficiálny dokument *„Politika kybernetickej obrany NATO"*, ktorý bol schválený v roku 2008, a ktorý stanovil tri hlavné piliere politickej koncepcie kybernetickej obrany Aliancie:

- subsidiarita, napr. asistencia je poskytovaná iba na žiadosť; inak je zachovávaná zásada vlastnej zodpovednosti zvrchovaných štátov;
- zamedzenie duplikácii, napr. predchádzanie zbytočnej duplikácie štruktúr a schopností na medzinárodnej, regionálnej i národnej úrovni;
- bezpečnosť, napr. spolupráca založená na vzájomnej dôvere, so zreteľom na senzitivitu informačného systému, ktorý musí byť dostupný a na eventuálnu zraniteľnosť.[6]

Tento dokument znamenal veľký kvalitatívny krok vpred a zároveň otvoril cestu zásadnému rozhodnutiu z lisabonského summitu kontinuálne pokračovať v zdokonaľovaní kybernetickej obrany. NATO vypracovalo prvé mechanizmy a spôsobilosti kybernetickej obrany a koncipovalo osnovu Politickej koncepcie kybernetickej obrany.

Vývoj vo vnímaní kybernetickej obrany, ako dôležitej súčasti komplexnej obrannej mozaiky budovanej NATO, je zrejmý aj pri čítaní Strategickej koncepcie NATO prijatej v roku 2010 v Lisabone. Problematike kybernetickej bezpečnosti a obrany je tam venovaný výrazne

---

[3] *Poznámka:* Ako príklad kybernetických útokov ako súčasti politického boja je možné uviesť kybernetické útoky na Estónsko v roku 2007 alebo Gruzínsko v roku 2008, ktoré boli zasa príkladom využitia kybernetických útokov ako doplnku k útokom kinetickým.

[4] NATO. 1999. *The alliance's strategic concept.* [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/cps/ie/ natohq/official_texts_27433.htm>

[5] NATO. 2002. *Prague Summit Declaration*. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.nato.int/cps/en/natohq/ official_texts_19552.htm?>

[6] THEILER, O. 2011. *Nové hrozby – kybernetické dimenzie*. [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/ docu/review/2011/11-september/cyber-Threads/SK/index.htm>

väčší priestor ako v predchádzajúcich koncepciách, pričom okrem definovania kybernetických útokov ako novej hrozby v bezpečnostnom prostredí (§ 12) navrhuje Aliancia (§ 19) celú sériu opatrení, ktoré je nevyhnutné realizovať s cieľom odstrašiť a ubrániť Alianciu proti tejto hrozbe: „*Zaistíme, aby NATO malo plný rozsah spôsobilostí potrebných na odstrašovanie a obranu proti akejkoľvek hrozbe voči bezpečnosti našich obyvateľov. Z tohto dôvodu budeme ďalej rozvíjať našu schopnosť prevencie, detekcie a obrany proti kybernetickým útokom a obnovy po nich, vrátane využitia procesu plánovania NATO na zlepšenie a koordináciu národných spôsobilostí kybernetickej obrany, zaistenia centralizovanej kybernetickej ochrany pre všetky orgány NATO a lepšieho integrovania kybernetickej informovanosti, varovania a reagovania členských krajín*.“[7]

Na základe rozhodnutí zo samitu v Lisabone, v novembri 2010, Aliancia vytvorila úspešné predpoklady pre autonómne riadenie a konkrétne skúmanie kybernetickej obrany a pre vytvorenie konkrétnych opatrení na reakciu v prípade potreby. Následne boli vypracované a schválené základné dokumenty NATO pre kybernetickú obranu: Koncept kybernetickej obrany NATO (2011), Politika NATO v oblasti kybernetickej obrany (2011) a najmä Akčný plán pre kybernetickú obranu NATO (2011), ktorého implementácia má a v nasledujúcich rokoch bude mať reálny dopad na úroveň spôsobilostí NATO a jeho členov v tejto oblasti.

Aj napriek rastúcemu používaniu ofenzívnych kybernetických spôsobilostí zločineckými sieťami či teroristickými organizáciami, dosiaľ stále najnebezpečnejšími aktérmi v oblasti kybernetických agresií sú zvrchované štáty, ktorých aktivity sa vyznačujú vysoko sofistikovanou špionážou či sabotážou informačných sietí.

Ohrozenia pochádzajúce z kybernetického priestoru sú potenciálne širokospektrálne. Pri istej miere zjednodušenia je možné hrozby existujúce v kybernetickom priestore rozdeliť do štyroch základných podskupín, ktoré sa líšia svojimi cieľmi, postupmi a aj následnými možnými škodami:

a) kybernetické vojny,
b) kybernetický terorizmus,
c) kybernetická špionáž a
d) kybernetická kriminalita.

Z hľadiska sofistikovanosti a komplexnosti je možné podľa Denningovej definovať tri úrovne kybernetického ohrozenia:

a) jednoducho štruktúrované so spôsobilosťou vykonávať základné útoky (hacky) proti jednotlivým systémom s využitím nástrojov vytvorených niekým iným; útočiaca organizácia disponuje jednoduchou cieľovou analýzou, velením a riadením a tiež nízkou schopnosťou učenia;
b) pokročilo štruktúrované so spôsobilosťou vykonávať zložitejšie útoky rôznych systémov alebo sietí a prípadne upraviť alebo vytvoriť základné hackerské nástroje; útočiaca organizácia disponuje elementárnou cieľovou analýzou, velením a riadením a tiež elementárnou schopnosťou učenia;
c) komplexne štruktúrované so spôsobilosťou koordinovaného útoku, ktorý môže spôsobiť masové narušenie integrovanej heterogénnej obrany (vrátane šifrovania); útočiaca organizácia disponuje schopnosťou vytvárať sofistikované hackerské nástroje, pričom disponuje pokročilou cieľovou analýzou, velením a riadením a pokročilou schopnosťou učenia.[8]

---

[7] NATO. 2010. *The Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf>

[8] DENNING, D. E. 2000. *Cyberterrorism*. [online]. [cit. 2019-05-07]. Dostupné na:<http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>

Aktuálny vývoj na nadnárodnej úrovni

Z vyššie uvedeného je zrejmé, prečo sa problematika kybernetickej obrany v ostatných rokoch dostáva do absolútneho popredia agendy NATO a EÚ. Estónsko sa pravidelne viac či menej úspešne snažilo dostať túto otázku na rokovania vrcholných orgánov NATO už od udalostí z jari 2007, keď bola sieťová infraštruktúra krajiny komplexne napadnutá a tento útok spôsobil masívne škody. Následne bola schválená *Politika NATO v kybernetickej obrane*, ktorá definuje kybernetické hrozby ako potenciálny zdroj kolektívnej obrany v zmysle článku 5 Washingtonskej zmluvy. Okrem toho, nová *Politika NATO v kybernetickej obrane* a *Akčný plán jej implementácie* poskytuje členským štátom NATO príslušné direktívy a schválený zoznam priorít, ktorých cieľom je pokrok Aliancie v kybernetickej obrane, vrátane zdokonalenia koordinácie medzi spojencami a partnermi NATO.

Na úrovni EÚ úlohy v oblasti výmeny informácii a poskytovania poradenstva v oblasti KIT plní European Network and Information Security Agency[9] (ďalej len „ENISA“). Jej úlohou je zároveň slúžiť ako centrála pre výmenu informácií o najlepších postupoch a praktikách v danej oblasti, napomáhať kontaktom medzi inštitúciami EÚ, jednotlivými členskými štátmi EÚ a súkromným sektorom, ako aj významnými odvetvovými hráčmi a záujmovými skupinami.

Keďže KIT pre svoj ďalší rozvoj vyžadujú stabilné, bezrizikové a bezpečné prostredie, ENISA poskytuje expertné rady a odporúčania Európskej komisii a členským štátom Únie, pričom vykonáva aktívnu podporu v oblasti stabilizácie prostredia KIT. Primárnym cieľom ENISA je dôvera zákazníkov v bezpečnosť elektronického komunikačného prostredia, ktoré sa používa pri podnikaní, práci alebo v osobnom živote. Realitou však je skutočnosť, že veľa krajín EÚ nie je pripravených čeliť masívnemu kybernetickému útoku. To bol jeden z dôvodov pre vznik ENISA, ako katalyzátora a propagátora, s úlohou urýchliť naprieč krajinami EÚ dosiahnutie uspokojivej úrovne odolnosti voči kybernetickým hrozbám.

Spolupráca s partnermi a medzinárodnými organizáciami, vrátane Európskej únie, je dôležitým prvkom politiky NATO v oblasti kybernetickej obrany. V súčasnosti prebiehajú diskusie spojencov o konkrétnych modalitách spolupráce. Každopádne by bolo iracionálnym riešením pre tie členské krajiny NATO, ktoré sú zároveň aj členmi EÚ, aby budovali duplicitné štruktúry a vypracovali duplicitné procedúry v oblastiach ako sú napr. krízové riadenie, vzdelávanie, školenie a výcvik, atď. Spolupráca teda musí prebiehať na základe spoločných hodnôt a spoločných prístupov s dôrazom na komplementárnosť a vylúčenie duplicít. Ciele na budovanie spôsobilostí v kybernetickej obrane boli začlenené tiež do približne 75 % z dvojstranných programov spolupráce, ktoré boli dohodnuté na úrovni oboch organizácií.

V poslednom období sa k Estónsku, snažiacemu sa zvýšiť úroveň vnímania kybernetických hrozieb, pridali aj USA, Francúzsko či Veľká Británia, čo je možné zdôvodniť výrazne rastúcim počtom kybernetických útokov na tieto krajiny, ktoré pochádzajú pravdepodobne z Ruska, Číny, Iránu či Severnej Kórei. Dôsledkom prebiehajúcej intenzívnej diskusie v zriadených pracovných skupinách či výboroch bolo samostatné rokovanie ministrov obrany členských krajín NATO na tému kybernetickej obrany 4. júna 2013. Hlavným dôvodom bol fakt, že viaceré krajiny čelia kybernetickým útokom prakticky denne Žiaľ, viaceré členské krajiny NATO majú vybudované veľmi limitované mechanizmy na potlačenie kybernetického útoku, a preto Aliancia po prvýkrát zaradila úlohy v oblasti budovania spôsobilostí v tejto oblasti medzi tzv. Národné ciele pre spôsobilostí.

Keďže oblasť kybernetickej obrany sa neustále vyvíja, z dlhodobého hľadiska existuje potreba inštitucionalizovať spoločné vzdelávanie a výcvik v tejto oblasti. Z uvedeného dôvodu NATO spracovalo dokument *Koncept NATO pre vzdelávanie a výcvik v oblasti kybernetickej obrany*. Ide o záujem Aliancie zrýchliť svoje úsilie v oblasti vzdelávania a odbornej prípravy

[9] Bližšie pozri: ENISA. 2019. *European Network and Information Security Agency*. [online]. [cit. 2019-05-07]. Dostupné na: <https://www.enisa.europa.eu>

prostredníctvom existujúcich škôl a tiež Centra výnimočnosti pre oblasť kybernetickej obrany[10] v Tallinne v Estónsku. Toto centrum, ktoré bolo akreditované zo strany NATO aj EÚ v roku 2008, vykonáva výskum a odbornú prípravu pre kybernetickú obranu odborníkov z aliančných štruktúr, členských krajín oboch organizácií, vrátane odborníkov zo sponzorských a partnerských krajín.

Rovnako dôležitou, ako zintenzívnenie a štandardizácia procesov vzdelávania a výcviku, je tiež organizácia pravidelných cvičení krízového manažmentu, ktoré ponúkajú vynikajúcu príležitosť na testovanie a konzultácie postupov pri riešení kybernetickej krízy. Prioritou v oblasti kybernetickej obrany je chrániť komunikačné systémy a siete vlastnené a prevádzkované Alianciou a Úniou. Ochrana národných kritických infraštruktúr zostáva v právomoci členských štátov, čo si vyžaduje, aby štáty investovali adekvátne zdroje do rozvoja vlastných spôsobilostí. NATO i EÚ pomáhajú spojencom v ich úsilí vybudovať adekvátnu národnú kybernetickú obranu prostredníctvom zdieľania informácií a osvedčených postupov a už spomínanou účasťou národných predstaviteľov na realizovaných medzinárodných cvičeniach.

Okrem uvedeného v súčasnosti prebieha na aliančnej pôde tiež diskusia o možnom nasadení kolektívnej aliančnej kybernetickej spôsobilosti, ako reakcie na kybernetický útok voči členskej krajine, ak táto o kolektívnu pomoc požiada.

Rozvoj partnerstva s priemyslom je zasa zásadným krokom smerom k zabezpečeniu účinnej kybernetickej obrany v rámci členských štátov NATO a tiež pre Alianciu samotnú. Partnerstvo s priemyselnou oblasťou by malo v čo najväčšej miere zahŕňať výmenu informácií, tzv. Lessons Learned,[11] spoluprácu v krízovom riadení, v plánovaní a tiež spoločnú participáciu na cvičeniach. Napriek istému pozitívnemu posunu stále existuje v tomto smere výrazný priestor na zintenzívnenie spolupráce. Konferencie národných riaditeľov pre vyzbrojovanie z členských štátov (Conference of National Armaments Directors – CNAD[12]), ako aj priemyselnej poradnej skupiny (NATO Industrial Advisory Group – NIAG[13]) by mali spoločne s predstaviteľmi priemyslu hľadať ďalšie konkrétne formy vzájomne prospešnej spolupráce. V zmysle schválenej politiky v oblasti kybernetickej obrany poskytuje Severoatlantická rada politický dohľad nad všetkými aspektmi jej implementácie. Rada je informovaná o závažných kybernetických incidentoch a útokoch. Výbor pre obrannú politiku a plánovanie zabezpečuje dohľad a poradenstvo na odbornej úrovni. Správna rada NATO pre kybernetickú obranu na pracovnej úrovni zodpovedá za koordináciu kybernetickej obrany medzi civilnými a vojenskými orgánmi NATO.

Na technickej úrovni je dôležitá činnosť Rady NATO pre konzultácie, velenie a riadenie (NATO Consultation, Command and Control Board – NC3Board[14]), ktorá je hlavným orgánom zodpovedným za konzultácie o technických aspektoch kybernetickej obrany. Vojenské orgány NATO a Agentúra NATO pre komunikačné a informačné systémy (NATO Communications

[10] Bližšie pozri: NATO. 2019. *The NATO Cooperative Cyber Defence Centre of Excellence*. [online]. [cit. 2019-05-07]. Dostupné na: <https://ccdcoe.org>

[11] *Poznámka*: Leassons Learned obsahuje štruktúrovane zaznamenané skúsenosti, ktoré nadobudol tím (projektový, výcvikový, operačný, realizačný, atď.) v priebehu celého životného cyklu projektu (výcviku, operácie, aktivity, atď.). Je cenným zdrojom poučenia pre tímy, ktoré budú realizovať obdobné aktivity či projekty. Poučenie z projektu (výcviku, priebehu operácie) obsahuje nielen súbor vyskytnuvších sa problémov, ale aj pozitívnych udalostí, ich vplyv na projekt (aktivitu, výcvik, operáciu) a odporúčania, ako postupovať, aby problém nabudúce nenastal, alebo naopak, aby pozitívne udalosti nastali.

[12] Bližšie pozri: NATO. 2019. *The Conference of National Armaments Directors*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.nato.int/cps/ua/natohq/topics_49160.htm>

[13] Bližšie pozri: NATO. 2019. *The NATO Industrial Advisory Group*. [online]. [cit. 2019-05-08]. Dostupné na: <https://diweb.hq.nato.int/niag/Pages_Anonymous/Default.aspx>

[14] Bližšie pozri: NATO. 2019. *The NATO Consultation, Command and Control Board*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.nato.int/cps/en/natohq/topics_69279.htm>

and Information Agency – NCIA[15]) nesú zodpovednosť za prevádzkové požiadavky, obstarávanie, implementáciu a prevádzkovanie spôsobilostí NATO v oblasti kybernetickej obrany. NCIA je prostredníctvom svojho technického centra NCIRC[16] (NATO Computer Incident Response Capability) zodpovedná za poskytovanie technických a prevádzkových služieb kybernetickej bezpečnosti v celej Aliancii. Technické centrum NCIRC predstavuje hlavnú technickú a prevádzkovú spôsobilosť NATO a má kľúčovú úlohu v reakcii na kybernetickú agresiu proti Aliancii.

NATO sa v súčasnosti venuje v oblasti kybernetickej obrany viacerým konkrétnym iniciatívam s cieľom komplexne vyskladať mozaiku konkrétnych opatrení a spôsobilostí potrebných v boji proti kybernetickým hrozbám. V súlade so závermi z lisabonského samitu,[17] konaného v novembri 2010, bola v apríli 2012 kybernetická obrana začlenená do procesu obranného plánovania NATO (NATO Defence Planning Process – NDPP[18]). Obranné plánovanie pritom predstavuje kľúčový nástroj Aliancie na zabezpečenie harmonizácie národných a aliančných plánovacích činností pri napĺňaní cieľov a zámerov v oblasti budovania spôsobilostí čo najefektívnejším spôsobom. Uvedomenie si dôležitosti a významu zaisťovania ochrany informácií a kybernetickej bezpečnosti dokazuje fakt, že všetky členské krajiny Aliancie, ktorým boli ciele v oblasti budovania spôsobilostí v rámci kybernetickej obrany alokované, s nimi aj v plnej miere súhlasili.

Celkovo boli ciele v oblasti kybernetickej obrany v rámci NATO integrované do iniciatívy inteligentnej obrany – *Smart Defence*[19], ktorá predstavuje nový spôsob myslenia pri zaisťovaní individuálnej i kolektívnej obrany a umožňuje krajinám spolupracovať na rozvoji a udržiavaní tých spôsobilostí, ktoré si členské krajiny najmä z dôvodu vysokej finančnej náročnosti nemôžu dovoliť vyvíjať alebo obstarať samé.

Aktuálny vývoj na národnej úrovni

Na úvod tejto časti je nutné skonštatovať, že problematike kybernetickej obrany, resp. budovaniu národných spôsobilostí potrebných pre uskutočňovanie ofenzívnych a defenzívnych operácií v kybernetickom priestore nie je v Slovenskej republike (ďalej len „SR“) venovaná dostatočná pozornosť. Tento stav sa odzrkadľuje aj v nedostatočnom budovaní obranných a útočných spôsobilostí pre potrebu presadzovania národných záujmov. Na druhej strane je však potrebné uviesť, že aj vďaka stále intenzívnejšiemu vnímaniu tejto témy zo strany medzinárodných organizácií, ktorých je SR členom, najmä NATO a EÚ, sa záujem zodpovedných inštitúcií a organizácií v ostatnej dobe rapídne zvyšuje. V podmienkach SR je problematika bezpečnosti kybernetického priestoru rozpracovaná vo forme stratégií a koncepcií, tie sú však zamerané najmä na informačnú bezpečnosť, rozvoj informačnej spoločnosti a na ochranu kritickej infraštruktúry.

Význam kybernetického priestoru a jeho bezpečnosti bol prvýkrát v SR oficiálne zdôraznený v najvyššom strategickom bezpečnostnom dokumente Bezpečnostnej stratégii SR z roku 2001, ktorá zadefinovala zneužitie informačných technológií, narušenie alebo úplné zlyhanie informačných systémov štátu v dôsledku terorizmu a pirátstva ako jednu

[15] Bližšie pozri: NATO. 2019. *The NATO Communications and Information Agency*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.ncia.nato.int/Pages/homepage.aspx>

[16] Bližšie pozri: NATO. 2019. *Cyber Security*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx>

[17] Bližšie pozri: NATO. 2010. *Lisbon Summitt Declaration*. Press Release (2010) 155. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nato.int/cps/en/natolive/official_texts_68828.htm>

[18] Bližšie pozri: NATO. 2019. *NATO Defence Planning Process*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nato. int/cps/en/natohq/topics_49202.htm>

[19] Bližšie pozri: NATO. 2019. *Smart Defence*. [online]. [cit. 2019-05-09]. Dostupné na:<https://www.nato.int/cps/ua/natohq/ topics_84268.htm>

z potenciálnych hrozieb pre bezpečnosť SR.[20] O štyri roky neskôr, Bezpečnostná stratégia SR z roku 2005 bola vo vzťahu k hrozbám v kybernetickom priestore konkrétnejšia. Uvádza sa v nej, že: *„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.“*[21]

S cieľom efektívne čeliť týmto nežiaducim hrozbám SR prijala v roku 2008 *Národnú stratégiu pre informačnú bezpečnosť v Slovenskej republike*[22] (ďalej len „NSIB“), ktorá si stanovila za cieľ vytvoriť základný rámec informačnej bezpečnosti v SR. Súčasťou dokumentu je základný popis jednotlivých úloh s cieľom zabezpečiť ochranu celého digitálneho priestoru SR, mimo oblasti utajovaných skutočností, ktoré rieši Národný bezpečnostný úrad SR[23] (ďalej len „NBÚ“). NSIB a jej podporné dokumenty sa zameriavajú výhradne na oblasť neutajovaných informácií. Oblasť ochrany utajovaných informácií, teda kybernetický priestor spadá výhradne do kompetencie NBÚ, ktoré túto problematiku rieši vo vlastnej pôsobnosti v zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov. Cieľom NSIB je pozitívne vplývať na podnikateľské prostredie na Slovensku, prispieť k zvýšeniu dôvery v spoľahlivosť a hodnovernosť elektronickej komunikácie v každodennom živote a zabezpečiť ochranu digitálneho priestoru SR v rozsahu neutajovaných informácií.

Ministerstvo financií Slovenskej republiky (ďalej len „MF SR“) ako ústredný orgán štátnej správy zodpovedný za túto oblasť a zastrešujúci orgán informačnej bezpečnosti vo vzťahu k ochrane neutajovaných údajov, do ktorého kompetencie spadá aj informačná bezpečnosť verejnej správy, prostredníctvom svojich príslušných sekcií a odborov usmerňuje tvorbu koncepcií informačných systémov verejnej správy, vydáva štandardy a koordinuje oblasť bezpečnosti týchto systémov a správy internetu a vypracúva ďalšie materiály dotýkajúce sa informatizácie spoločnosti a verejnej správy; monitoruje, analyzuje a hodnotí stav bezpečnosti informačných systémov verejnej správy ako aj informačných systémov pracujúcich s osobnými údajmi a zastupuje SR v medzinárodných inštitúciách pre informačnú bezpečnosť.

Úlohou MF SR je zároveň vykonávať pravidelné prieskumy stavu informačnej bezpečnosti. V podmienkach MF SR bol zároveň zriadený poradný koordinačný výbor – Komisia pre informačnú bezpečnosť. Úlohou tejto komisie je pripravovať návrhy a stanoviská pre oblasť ochrany a bezpečnosti informačných systémov verejnej správy, vyjadrovať sa k bezpečnostným štandardom, navrhovať a skúmať návrhy právnych noriem a relevantných materiálov týkajúcich sa informačnej bezpečnosti a zriaďovať pracovné skupiny pre plnenie stanovených úloh.

Problematika ochrany utajovaných skutočností v kybernetickom priestore spadá do kompetencie NBÚ SR ako ústredného orgánu štátnej správy pre ochranu utajovaných skutočností, šifrovú službu a elektronický podpis.[24] Problematika ochrany utajovaných skutočností a informácií je vo vládnych dokumentoch vyčlenená z digitálneho priestoru a tvorí samostatný kybernetický priestor. Ochranu utajovaných skutočností upravuje Koncepcia ochrany utajovaných skutočností v SR z roku

---

[20] Bezpečnostná stratégia Slovenskej republiky. 2001. [online]. [cit. 2019-05-09]. Dostupné na: <https://web.archive.org/web/20130216175625/http://merln.ndu.edu/whitepapers/SlovakiaSecurity2001.pdf>

[21] Bezpečnostná stratégia Slovenskej republiky. 2005. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.mod.gov.sk/ data/files/833.pdf>

[22] Národná stratégia pre informačnú bezpečnosť v Slovenskej republike. 2008. [online]. [cit. 2019-05-09]. Dostupné na: <www.informatizacia.sk/ext_dok_narodna_strategia_pre_ib/6167c/>

[23] Bližšie pozri: NBÚ. 2019. *Národný bezpečnostný úrad Slovenskej republiky*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nbu.gov.sk>

[24] NR SR. 2004. *Zákon č. 2015/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/20190412>

2007 a Koncepcia šifrovej ochrany informácií v SR z roku 2008 spolu s Návrhom opatrení pre zabezpečenie kybernetickej ochrany v SR, ktoré boli vypracované NBÚ SR.

Keďže v záujme ochrany digitálneho priestoru je potrebné rozvinúť bližšiu spoluprácu v oblasti ochrany utajovaných skutočností a informačnej bezpečnosti celého digitálneho priestoru SR, Uznesením Bezpečnostnej rady SR č. 218 z roku 2008 bol NBÚ SR učený ako národná autorita pre riadenie kybernetickej ochrany, a teda poverený riešením otázok spadajúcich do tejto oblasti a určený za kontaktný bod pre spoluprácu s NATO. NBÚ ako národná autorita pre kybernetickú ochranu zaisťuje taktiež ochranu elektronicky vymieňaných utajovaných skutočností. Vo februári 2009 podpísal NBÚ, ako jedna z prvých národných bezpečnostných autorít členských krajín s NATO Memorandum o kybernetickej obrane s cieľom rozvoja vzťahov a výmeny skúseností na expertnej úrovni v tejto oblasti. V tom istom roku vzniklo v podmienkach Úradu špecializované pracovisko počítačovej bezpečnosti a reakcie na incidenty – SK Computer Security Incident Response Team[25] (ďalej len „CSIRT.SK“) s cieľom koordinovať kybernetickú obranu, zvyšovať bezpečnosť informačných systémov a podieľať sa na medzinárodnej spolupráci.

Ďalšou prioritou NSIB bolo práve vytvorenie Tímu pre reakciu na bezpečnostné incidenty počítačov, tzv. CSIRT.SK – kontaktného miesta pre riešenie bezpečnostných incidentov a následné zriadenie špecializovanej organizácie pre riešenie problematiky počítačového zločinu, vzájomnej spolupráce, výmeny informácií a skúseností na vnútroštátnej úrovni s prepojením do celoeurópskeho priestoru. Tím bol zriadený uznesením vlády SR č. 479/2009 z 1. júla 2009 práve v súlade s vyššie uvedenou Národnou stratégiou pre informačnú bezpečnosť v SR, pričom poskytuje služby prevažne štátnej správe za účelom reakcie na bezpečnostné incidenty namierené na Národnú informačnú a komunikačnú infraštruktúru SR (ďalej len „NIKI“), ako aj služby pre verejnú správu a verejnosť s výnimkou incidentov týkajúcich sa utajovaných informácií. Zároveň zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci celej NIKI.

Hlavné ciele vytvorenia CSIRT.SK spočívajú v:

- riešení informačno-bezpečnostných incidentov v SR v spolupráci s vlastníkmi a prevádzkovateľmi postihnutých častí NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb a prípadne inými štátnymi orgánmi (napr. políciou, justíciou, prokuratúrou, atď.),
- budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti,
- kooperácii so zahraničnými sesterskými organizáciami a
- reprezentácii SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.

Medzi ďalšie kritické oblasti z pohľadu kybernetickej bezpečnosti patria ochrana osobných údajov a elektronický podpis. Na základe platnej legislatívy spadá ochrana osobných údajov do kompetencie Úradu na ochranu osobných údajov Slovenskej republiky[26] (ďalej len „ÚOOÚ“) a oblasť elektronického podpisu do kompetencie NBÚ. Problematika elektronického obchodu patrí do pôsobnosti Ministerstva hospodárstva Slovenskej republiky a počítačová kriminalita patrí do pôsobnosti Ministerstva spravodlivosti Slovenskej republiky a Ministerstva vnútra Slovenskej republiky. Ako už bolo uvedené vyššie, ciele na budovanie spôsobilostí v rámci tzv. Národných cieľov NATO boli zahrnuté do úloh pre viaceré členské krajiny, Slovensko nevynímajúc. Národnou autoritou v SR zodpovednou za plnenie záväzkov k NATO je NBÚ.

[25] Bližšie pozri: NBÚ. 2019. *Národná jednotka CSIRT*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/ kyberneticka-bezpecnost/sk-csirt/index.html>

[26] Bližšie pozri: ÚOOÚ. 2019. *Úrad na ochranu osobných údajov Slovenskej republiky*. [online]. [cit. 2019-05-10]. Dostupné na: <https://dataprotection.gov.sk/uoou/>

Na doplnenie vyššie uvedených informácií je potrebné dodať, že 17. júna 2015 vláda SR schválila uznesením č. 328/2015 Koncepciu kybernetickej bezpečnosti SR na roky 2015-2020,[27] ktorej cieľom bolo navrhnúť nový inštitucionálny rámec riadenia kybernetickej bezpečnosti v SR. 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.

2. marca 2016 zároveň vláda SR schválila dňa uznesením č. 93/2016 akčný plán realizácie predmetnej koncepcie[28] obsahujúci návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru SR pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť SR nenahraditeľné škody, a tak by mohla byť narušená dôveryhodnosť štátu či organizácie. Akčný plán predstavuje jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnost-ných politík, medzinárodnej spolupráce, zvyšovania povedomia a spôsobilostí, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru.

1. apríla 2018 nadobudol účinnosť zákon NR SR č. 69/2018 Z. Z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,[29] ktorý komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti a ktorý zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň do slovenského právneho poriadku transponuje európsku smernicu o sieťovej a informačnej bezpečnosti.[30]

Záver

Ochrana informácií a kybernetická bezpečnosť spolu s kybernetickým priestorom vytvárajú novú a mimoriadne dynamickú doménu. NATO i EÚ a ich členské štáty postupne začínajú objavovať pozitíva (výhody, benefity), ale aj negatíva (hrozby, riziká), ktoré táto doména prináša. Na rozdiel od klasických konvenčných zbraní však kybernetický priestor dáva relatívne veľké možnosti aj stále viac aktívnym neštátnym aktérom. Medzinárodné kybernetické „hry“, ktoré sú plné rôznorodých „hráčov“, prinášajú stále nové otázky o tom, čo vlastne ochrana informácií a kybernetická bezpečnosť znamená, a to tak z národného, ako aj z nadnárodného, medzinárodného hľadiska.

Vzhľadom na kontinuálny rast kybernetických hrozieb v predchádzajúcich rokoch bude preto v záujme zvýšenia ochrany informácií a zabezpečenia kybernetickej bezpečnosti v najbližších rokoch nutné nielen v SR, ale aj v ostatných členských krajinách NATO a EÚ aktualizovať, resp. vypracovať komplexné národné stratégie, postupy a procedúry vychádzajúce z Politiky NATO pre kybernetickú obranu a Smernice EÚ o bezpečnosti sietí a informačných systémov. Súčasne bude nevyhnutné vybudovať spoločné operačné centrum, jasne stanoviť národnú riadiacu štruktúru v tejto oblasti, ako aj autoritu pre strategické

[27] Bližšie pozri: NBÚ. 2019. *Koncepcia kybernetickej bezpečnosti SR*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf>

[28] Bližšie pozri: NBÚ. 2019. *Akčný plán realizácie koncepcie kybernetickej bezpečnosti SR*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf>

[29] NR SR. 2004. *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www. slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20190101>

[30] Bližšie pozri: EÚ. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. [online]. [cit. 2019-05-10]. Dostupné na: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148>

plánovanie. Spravodajské služby by zasa mali intenzívnejšie rozvíjať spôsobilosti defenzívneho i ofenzívneho charakteru, napríklad na detekciu hrozieb a na aktívne operácie (kybernetická špionáž).

V kybernetickom priestore, ako v každej inej operačnej doméne, je pre štátnych aktérov životne dôležité definovať spôsob využitia tohto priestoru pre potreby národnej bezpečnosti. Preto je potrebné vytvoriť podpornú kybernetickú stratégiu s cieľom vytvárania a využívania strategických spôsobilostí pre fungovanie v kybernetickom priestore, integrovaných a koordinovaných s ďalšími operačnými doménami, za účelom dosiahnutia alebo podpory dosiahnutia cieľov naprieč elementmi národnej sily z dôvodu podpory národnej bezpečnostnej stratégie. Strategické spôsobilosti pre fungovanie v kybernetickom priestore zahŕňajú širokú paletu rôznych nástrojov, pričom za jeden z nich je možné považovať budovanie ofenzívnych kybernetických spôsobilostí, ktoré môžu byť využité na zabezpečovanie národných záujmov.

Záverom je možné konštatovať, že SR si uvedomuje dôležitosť bezpečnosti ochrany informácií a kybernetickej bezpečnosti. Toto uvedomenie, okrem iných vplyvov, je však aj výsledkom rastúceho tlaku zo strany najmä NATO a EÚ, ktoré vyvíjajú viaceré iniciatívy na budovanie obranných spôsobilostí v tomto priestore. Napriek existencii viacerých stratégií, koncepcií a právnych úprav jednotlivých elementov kybernetického priestoru v podmienkach SR, však k dnešnému dňu absentuje naozaj kvalitná všeobecná právna úprava jednoznačne riešiaca stav a ambície SR v oblasti obrany kybernetického priestoru a jeho bezpečnosti a tiež jasné vymedzenie zodpovedností a právomocí, čo bude potrebné riešiť vo veľmi krátkom časovom horizonte.

Zoznam použitej literatúry:

1. ANDRASSY, V. – GREGA, M. 2015. Možnosti optimalizácie informačných systémov v bezpečnostnom systéme. In *Košická bezpečnostná revue*, 2015, roč. 5, č. 2, s. 11-18. ISSN 1338-4880.
2. BARIČIČOVÁ, Ľ. 2018. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality*. *Zborník príspevkov z vedeckej konferencie.* Bratislava: APZ, 2018, s. 8-15. ISBN 978-80-8054-773-8.
3. BELAN, L. 2016. Vlastnosti bezpečnosti. In *Národná a medzinárodná bezpečnosť 2016*: zborník príspevkov zo 7. medz. vedeckej konferencie. Liptovský Mikuláš : Akadémia ozbrojených síl gen. M. R. Štefánika, 2016, s. 31-37. ISBN 978-80-8040-534-2.
4. Bezpečnostná stratégia Slovenskej republiky. 2001. [online]. [cit. 2019-05-09]. Dostupné na:<https://web.archive.org/web/20130216175625/http://merln.ndu.edu/whitepapers/SlovakiaSecurity2001.pdf>
5. Bezpečnostná stratégia Slovenskej republiky. 2005. [online]. [cit. 2019-05-09]. Dostupné na: <https://www. mod.gov.sk/data/files/833.pdf>
6. DENNING, D. E. 2000. *Cyberterrorism*. [online]. [cit. 2019-05-07]. Dostupné na: <http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf>
7. ENISA. 2019. *European Network and Information Security Agency.* [online]. [cit. 2019-05-07]. Dostupné na: <https://www.enisa.europa.eu>
8. EÚ. 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. [online]. [cit. 2019-05-10]. Dostupné na: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148>
9. NATO. 1999. *The Alliance's Strategic Concept. Press Release NAC-S(99) 65.* [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/cps/ie/natohq/official_texts_27433.htm>

10. NATO. 2002. *Prague summit declaration. Press release (2002) 127*. [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/cps/en/natohq/official_texts_19552.htm?>
11. NATO. 2010. *Lisbon Summitt Declaration*. Press Release (2010) 155. [online] [cit. 2019-05-09]. Dostupné na: <https://www.nato.int/cps/en/natolive/official_texts_68828.htm>
12. NATO. 2010. *The Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf>
13. NATO. 2019. *Cyber Security*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx>
14. NATO. 2019. *NATO Defence Planning Process*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nato. int/cps/en/natohq/topics_49202.htm>
15. NATO. 2019. *Smart Defence*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nato.int/cps/ua/natohq/ topics_84268.htm>
16. NATO. 2019. *The conference of national armaments directors*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.nato.int/cps/ua/natohq/topics_49160.htm>
17. NATO. 2019. *The NATO Communications and Information Agency*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.ncia.nato.int/Pages/homepage.aspx>
18. NATO. 2019. *The NATO Consultation, Command and Control Board*. [online]. [cit. 2019-05-08]. Dostupné na: <https://www.nato.int/cps/en/natohq/topics_69279.htm>
19. NATO. 2019. *The NATO Cooperative Cyber Defence Centre of Excellence*. [online]. [cit. 2019-05-07]. Dostupné na: <https://ccdcoe.org>
20. NATO. 2019. *The NATO Industrial Advisory Group*. [online]. [cit. 2019-05-08]. Dostupné na: <https://diweb.hq.nato.int/niag/Pages_Anonymous/Default.aspx>
21. NBÚ. 2019. *Akčný plán realizácie koncepcie kybernetickej bezpečnosti SR.* [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf>
22. NBÚ. 2019. *Koncepcia kybernetickej bezpečnosti SR*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf>
23. NBÚ. 2019. *Národná jednotka CSIRT*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.nbu.gov.sk/ kyberneticka-bezpecnost/sk-csirt/index.html>
24. NBÚ. 2019. *Národný bezpečnostný úrad Slovenskej republiky*. [online]. [cit. 2019-05-09]. Dostupné na: <https://www.nbu.gov.sk>
25. NR SR. 2004. *Zákon č. 2015/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/215/20190412>
26. NR SR. 2004. *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti*. [online]. [cit. 2019-05-10]. Dostupné na: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/20190101>
27. THEILER, O. 2011. *Nové hrozby – kybernetické dimenzie*. [online]. [cit. 2019-05-06]. Dostupné na: <https://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm>
28. ÚOOÚ. 2019. *Úrad na ochranu osobných údajov Slovenskej republiky*. [online]. [cit. 2019-05-10]. Dostupné na: <https://dataprotection.gov.sk/uoou/>

Kontaktné údaje:
plk. gšt. v. z. prof. Ing. Pavel Nečas, PhD.
Fakulta politických vied a medzinárodných vzťahov
Univerzita Mateja Bela v Banskej Bystrici
pavel.necas@umb.sk

plk. gšt. v. z. Ing. Radoslav Ivančík, PhD. et PhD.
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
radoslav.ivancik@minv.sk

Kyberpriestor, kybernetická kriminalita a komparácia jej nárastu vzhľadom na dynamiku jej vývoja

Liliana Réveszová

Abstrakt:
Dynamický rozvoj informačných technológií so sebou prináša tak pozitívne vnímanie a javy, ako aj negatívne spoločensky škodlivé správanie resp. konanie. Preto je v súčasnosti kybernetickej kriminalite venovaná čoraz väčšia pozornosť. Pojem kybernetická kriminalita je odvodzovaný od pojmu kybernetický priestor resp. kyberpriestor. Kyberpriestor je virtuálne prostredie, ktoré nemá začiatok a ani koniec, nepozná hranice národných štátov a nemožno určiť, ako je v skutočnosti rozsiahly. Negatívne spoločensky škodlivé správanie resp. konanie v kyberpriestore predstavuje obrovské finančné straty, veľmi často presahuje hranice jedného štátu a stáva sa medzinárodným trestným činom. Z tohto pohľadu sa uvedený príspevok v prvej časti venuje definícii kybernetickej kriminality, kybernetickému priestoru, jeho príčinám zraniteľnosti a v druhej časti sa zameriava na reálnu dynamiku vývoja danej kriminality v Slovenskej republike v rokoch 2013 – 2018. Prostredníctvom tejto komparácie dynamického vývoja kybernetickej kriminality vyjadrenej pomocou grafického zobrazenia jednotlivých trestných činov možno konštatovať, že počet jej obetí denne stúpa.V súčasnosti je najrýchlejšie rozvíjajúcou sa formou kriminality, ktorá si vyžaduje neustále zvýšenú pozornosť.
Kľúčové slová:
Kybernetická kriminalita, trestný čin, dynamika, formy, kyberpriestor, zraniteľnosť, príčiny.

Abstract:
The dynamic development of information technology brings with it both positive perception and phenomena, as well as negative socially harmful behavior, respectively. therefore, cybercrime is increasingly being addressed. The term cybercrime is derived from the concept of cyberspace, respectively. cyberspace. Cyberspace is a virtual environment that has no beginning and no end, does not know the boundaries of national states and cannot determine how large it really is. Negative socially harmful behavior resp. cybersecurity is a huge financial loss, very often crosses the borders of one state and becomes an international crime. In the first part we focus on the definition of cybercrime, cyberspace, its causes of vulnerability and in the second part we focus on the real dynamics of the development of the given crime in the Slovak Republic in the years 2013 - 2018. Through this comparison of the dynamic development of cybercrime expressed by the graphic representation It can be said that the number of its victims is increasing every day, and is currently the fastest growing form of crime that requires ever-increasing attention.
Keywords:
Cybercrime, offence, dinamics, forms, cyberspace, vulnerability, causes.

Úvod

V súčasnosti môžeme konštatovať, že jedným z hlavných fenoménov tejto doby je veľký rozmach informačných technológií a ich neustály rozvoj a napredovanie. Informačné technológie sú každodennou súčasťou celej spoločnosti, našich životov, uľahčujú nám každodenný život, pomáhajú nám riešiť množstvo rôznych problémov. Ale každá minca má dve strany a zároveň s pozitívnym vnímaním rozmachu informačných technológií, nemôžeme privierať oči pred druhou stranou mince, ktorá nám veľmi príkladne poukazuje na negatívny dopad rozmachu tejto oblasti. Negatívny dopad sa odráža v tom, že neustály rozmach informačných technológií nám priniesol zároveň aj priestor pre páchanie ani nie tak nového, ale neustále sofistikovanejšieho druhu kriminality v tejto oblasti nazývaného kybernetická kriminalita. Môžeme konštatovať, že zakaždým sa vyskytujú nové spôsoby kybernetickej kriminality a zároveň sú zdokonaľované tak, aby boli čo najmenej odhaliteľné a postihnuteľné. Páchatelia trestných činov tohto druhu používajú sústavne sofistikovanejšie metódy a prostriedky k páchaniu tejto trestnej činnosti. Táto skutočnosť je vyvolaná aj sústavne stúpajúcim nárastom používateľov počítačovej techniky, počítačových sietí, ich rozširovaním a pod. Avšak niekedy je ťažké udržať krok s vývojom informačných technológií, je tak rýchly, že nie vždy je ľahké sledovať trh s novými produktami, čo následne spôsobuje obrovskú priepasť medzi vlastnými znalosťami a skutočnou realitou v tejto oblasti. Nedostatočná informovanosť ľudí a zabezpečenie počítačov v tejto problematike sú veľkým problémom,

ľudia častokrát podceňujú kvalitné zabezpečenie, pravidelnú údržbu a aktualizáciu. Z toho dôvodu je počítačová kriminalita stále väčším problémom, ktorý spôsobuje každým rokom vysoké škody a náklady, ktoré sú veľmi ťažko vyčísliteľné a pohybujú sa v obrovských sumách. V súčasnej dobe kybernetickú kriminalitu hodnotíme, ako jednu z najnebezpečnejších fenoménov. Vzhľadom k tomu je potrebné tejto problematike venovať osobitne zvýšenú pozornosť.

„Digitálne technológie a internet sú dôležitým pilierom európskej ekonomiky. Počet kybernetických útokov však v Európe rastie každým dňom. Európske krajiny si uvedomujú, že ak budú voči týmto hrozbám postupovať jednotlivo, budú ešte viac zraniteľné. Len spoločným postupom a spoluprácou na európskej úrovni možno účinne bojovať proti negatívnym dopadom počítačovej kriminality.“[1]

Cieľom tohto článku je čitateľom priniesť základné informácie o kybernetickej kriminalite, jej definícii, o jej vzniku, popísanie s ňou úzko súvisiaceho pojmu ako „kyberpriestor“, príčiny zraniteľnosti kyberpriestoru. Zároveň popísať niektoré jej formy v slovenskej právnej úprave s následným grafickým zobrazením a porovnaním vývoja dynamiky konkrétnych foriem kybernetickej kriminality v slovenskej právnej úprave za roky 2013 – 2018.

Vznik kybernetickej kriminality

Kybernetická kriminalita vznikla z dôvodu, pretože veľa základných ľudských a spoločenských činností a aktív, oblastí bežného života sa prenieslo do kybernetického sveta resp. kyberpriestoru. Príkladne máme na mysli a môžeme sem zahrnúť dopravu, bankovníctvo, logistika, sociálne väzby medzi ľuďmi, ich majetok, či prístup k nemu, identita a osobné údaje ľudí a pod. Ľudia tento kybernetický priestor bežne stotožňujú s prostredím internetu, avšak tento prístup je príliš zjednodušujúci. „Kyberpriestor je súhrn technológií, systémov, služieb a ich vzájomných väzieb umožňujúcich výmenu, zhromažďovanie, komunikáciu a spracovávanie informácií v digitálnej podobe.“[2] Z toho nám vyplýva, že sa nejedná výhradne o prostredie internetu, ale zahŕňame sem aj vnútorné firemné prostredie, prostredie pre riadenie technologických procesov a pod. Do kyberpriestoru sme presunuli medziľudskú komunikáciu, využívame ho aj ako nekonečný zdroj informácií o čomkoľvek, vznik virtuálnych mien, čoraz častejším uprednostňovaním bezhotovostných platieb, čo sa odráža v platobnej a transakčnej funkcii, ktorú si už málokto dokáže predstaviť bez kyberpriestoru, kontrolou domácností resp. zariadení, infraštruktúry firiem bez fyzického kontaktu, uskladňovaním citlivých osobných dát, intímnych zážitkov, obrazových spomienok v kybernetickom priestore, ich zverejňovaním rôznym skupinám, spoločnostiam aj prostredníctvom tzv. cloudových aplikácií, ktoré takéto dáta a informácie uchovávajú. „Tým, že ich držíme v kybernetickom priestore, stratili sme do určitej miery aj priamu fyzickú kontrolu, komu ich ukážeme a komu nie. Spolu s týmito zmenami sme konfrontovaní aj s novými druhmi kriminality.“[3]

Kyberpriestor zohráva významnú úlohu aj v zábavnom priemysle, tak ako legálnym zdieľaním – hudby, filmov, kníh, tak aj prostredím pre hranie sieťových hier. Kyberpriestor má svoje využitie aj zo strany štátnej správy, ktorá cez kyberpriestor približuje svoje služby občanom. Už viac-menej každé priemyselné odvetvie využíva rôzne vyspelé technológie pre dosiahnutie svojich cieľov. „Vedu a výskum bez využitia kyberpriestoru si už nevieme predstaviť.“[4] Toto pozitívne pôsobenie kyberpriestoru je len jednou stranou mince. Tak isto je dôležité vnímať aj druhú stranu mince, kde sa kyberpriestor stal aj ideálnym prostredím pre

[1] Počítačová kriminalita. 2016. *Počítačová kriminalita spôsobuje straty.* [online]. [cit. 14. 06. 2019]. Dostupné na internete:<http://sklady.etrend.sk/poradna/tns-pocitacova-kriminalita-sposobuje straty>

[2] ŠPIDLA, A. Úvod do kybernetické a informační bezpečnosti. In: *Security magazín*. č. 6, 2017. s. 35.

[3] HANKO, M. Kybernetický zločin a kybernetická bezpečnosť. In: *Obrana-modernizácia*. č. 9, 2015. s. 32.

[4] ŠPIDLA, A. Úvod do kybernetické a informační bezpečnosti. In: *Security magazín*. Č. 6, 2017. s. 35.

realizáciu, páchanie kybernetickej kriminality, kybernetických vojen, kybernetickej špionáže a rady ďalších funkcií, ktoré už tak pozitívne ani zďaleka nie sú. Je úplne logické, že technické prostriedky, ktoré sú využívané pre pozitívne pôsobenie, je možné využiť aj pre negatívne javy. Kyberpriestor je dôležité vnímať zo všetkých uhlov pohľadov, s jeho skvelými funkciami, ale aj s jeho bezpečnostnými hrozbami, ktoré ohrozujú náš majetok, zdravie, životy tak isto ako integritu štátov a ich ekonomík.

„Technologická rozmanitosť častí kyberpriestoru generuje také veľké množstvo zraniteľností a tým aj hrozieb, ktoré sú schopné na ne útočiť.“[5]

Príčiny zraniteľnosti kybernetického priestoru

Prečo sa hrozby stávajú hrozbami v kybernetickom priestore? Odpoveď nachádzame v tom, že hrozby sa stávajú hrozbami v kybernetickom priestore aj z toho dôvodu, že kybernetický priestor má špecifické vlastnosti, charakteristiky.

Tieto špecifické vlastnosti si môžeme začleniť do piatich bodov:

1. Možnosť okamžitej akcie a reakcie na veľkú vzdialenosť, bez fyzického kontaktu.

Príkladne máme na mysli zraniteľnosť a možné narušenie, či priam zničenie (krádež, špionáž, založenie požiaru a i.) nejakého objektu cez kybernetický priestor, napríklad prísne fyzicky strážené objekty ako banka, či vojenský objekt sú v podstate len fyzickou ochranou vlastne nechránené a hrozí vyššie popísané konanie.

2. Asymetrickosť.

Kybernetický priestor neumožňuje rozpoznať, kto za hrozbou stojí, či jednotlivec, skupina, mocný resp. zlyhávajúci štát. V kybernetickom priestore môže mať skupina kybernetických útočníkov resp. jednotlivcov proporčne neúmerný vplyv a moc.

3. Anonymita.

V kybernetickom priestore je anonymita na internete vnímaná užívateľmi ako kľúčový atribút na zachovanie slobody internetu, naproti tomu v takej miere anonymita v reálnom fyzickom svete nie je možná. Mnohokrát nevieme, kto stojí za škodlivým kódom, resp. e-mailom, malvérom a pod. „Anonymita v kybernetickom priestore znamená tiež do značnej miery bezprostrednosť pre tých, ktorý ho používajú na nekalú činnosť.“[6]

4. Absencia hraníc v kybernetickom priestore.

To, na čom zakladá medzinárodné a humanitárne právo vo fyzickom svete, to v kybernetickom priestore chýba, máme na mysli vymedzenie suverenity jednotlivých štátov.

5. Nedostatok rozlíšenia.

Všetky informácie v procese prenosu vyzerajú rovnako a je náročné a takmer nemožné okamžite rozoznať, na aký účel informácia slúži, príkladne, či na špionáž, či na prehliadanie internetu pre zábavu, či na vedenie kybernetickej útočnej operácie a pod.[7]

Vymedzenie kybernetickej kriminality

Pre vymedzenie pojmu kybernetickej kriminality nie je vo všeobecnosti žiadna uznávaná definícia, z dôvodu, že odborná verejnosť v chápaní tohto pojmu nie je jednotná a definovanie tohto pojmu je veľmi neurčité a to aj napriek tomu, že dnešná doba je počítačmi úplne pohltená. Rozsah kybernetickej kriminality je veľký a zároveň neustále sa meniaci a rozvíjajúci, tak ako sa neustále mení a rozvíja kybernetický priestor. Uvedený druh kriminality sa zvykne najčastejšie označovať ako kybernetická kriminalita, resp. kyberkriminalita,

[5] ŠPIDLA, A. Úvod do kybernetické a informační bezpečnosti. In *Security magazín*. č. 6, č. 6. 2017. s. 35.
[6] HANKO, M. Hrozby kybernetického priestoru. In *Obrana*. č. 8. 2015. s. 32.
[7] HANKO, M. Hrozby kybernetického priestoru. In *Obrana*. č. 8. 2015. s. 32.

počítačová kriminalita, internetová kriminalita. V princípe možno všetky uvedené termíny považovať za synonymá. Ako ho na svoje účely vymedzí záleží len na autoroch, oficiálnom dokumente či právnom predpise. V zahraničnej literatúre, článkoch sa objavujú anglické ekvivalenty týchto pojmov a predstavujú ich tieto pojmy „cybercrime", „high-tech crime", „IT crime", „virtual crime“, či „computer crime", ktorý je časovo najstarším pojmom. V žiadnom zákone, zmluve, ktorú je SR viazaná dodržiavať sa zatiaľ jednotná a záväzná definícia tohto pojmu nenachádza.[8]

V odbornej literatúre sa stretávame s nespočetným množstvom definície počítačovej kriminality, ibaže len ťažko je možné predstaviť bežne prijateľnú a zaužívanú. Za nenáročný pokus o jej definovanie možno uviesť, že: „počítačovou kriminalitou sa rozumie konanie páchateľa za použitia informačnej techniky, ktorým sú naplnené znaky skutkovej podstaty počítačového trestného činu.“[9]

Môžeme podotknúť, že niektoré z definícií už ani neplatia, pretože reflektovali dobu, v ktorej vznikali a odvtedy vzniklo veľa nových technológií a online služieb, ktoré už daná definícia nie je schopná zahrnúť. Vo všeobecnosti sa môžeme prikloniť k názoru, že čím jednoduchšia definícia bude, tým bude zahŕňať väčší počet spoločensky škodlivého konania v kyberpriestore napriek jeho dynamike v čase. Jednou z takýchto jednoduchých definícií kybernetickej kriminality je: "Kybernetická kriminalita je spoločensky škodlivé konanie útočiace na počítačový systém alebo na iný objekt za výrazného použitia počítačového systému."[10] Vzhľadom k domnelej anonymite láka kyberpriestor mnoho predátorov, ktorým navyše dáva obrovské množstvo možností ako svoju obeť prekabátiť. Ak teda v reálnom svete platí "Dôveruj, ale preveruj", vo svete kyberpriestoru je lepšie sa prikloniť skôr k "Nedôveruj". Kybernetická kriminalita sa prejavuje mnohými spôsobmi a presné rozdelenie často nie je možné, pretože sa spravidla jedná o kombináciu niekoľkých spôsobov útokov.

Pojem kybernetická kriminalita môžeme chápať aj ako: „počítačová kriminalita je akékoľvek nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Definícia podľa Dohovoru o počítačovej kriminalite.“[11]

Nech už sú definičné vymedzenia pojmu kybernetická kriminalita akékoľvek, v každom pokuse o definičné vymedzenie sa opakuje niekoľko zhodných skutočností z ktorých si každý môže vyvodiť obraz o obsahu tohto pojmu. Jedná sa o tieto skutočnosti:

- kybernetická kriminalita je charakterizovaná pre ňu typickými spôsobmi jej páchania a utajovania,
- kybernetickú kriminalitu vystihuje dynamika jej rozvoja,
- kybernetická kriminalita vykazuje pomerne vysokú mieru jej latencie,
- kybernetická kriminalita má cezhraničný charakter, najmä ak hovoríme o kybernetickej kriminalite v kontexte informačných sietí.

Kybernetická kriminalita v našej legislatíve

Kybernetickú kriminalitu môžeme rozdeliť na dve základné skupiny a to na priamu počítačovú kriminalitu a na nepriamu počítačovú kriminalitu.

---

[8] Najpravo. 2012. Základné formy počítačovej kriminality. [online]. [cit. 15. 06. 2019]. Dostupné na:<http://www.najpravo.sk/clanky/zakladne-formy-pocitacovej-kriminality.html>

[9] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer s.r.o., 2016. s. 25.

[10] Internetem bezpečně. 2018. *Kybernetická kriminalita*. [online]. [cit. 15. 06. 2019]. Dostupné na: <https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/kyberneticka-kriminalita/>

[11] Preventista. 2017. *Počítačová internetová kriminalita a jej prevencia v školskom prostredí.* [online]. [cit. 15. 06. 2019]. Dostupné na:<http://preventista.sk/info/pocitacova-internetova-kriminalita-a-jej-prevencia-v-skolskom-prostredi/>

Pod priamu počítačovú kriminalitu zahŕňame počítačové trestné činy resp. trestné činy alebo útoky smerujúce priamo na počítač.

Napriek tomu pod nepriamu počítačovú kriminalitu zahŕňame trestné činy, ktoré sú páchané prostredníctvom výpočtovej techniky a to trestné činy ekonomickej povahy, trestné činy útočiace na súkromné osoby a trestné činy predstavujúce ďalšie možnosti zneužitia údajov.

V Trestnom zákone SR sa čoraz častejšie stretávame s trestnými činmi, pri ktorých ku naplneniu obligatórnych znakov skutkovej podstaty môže dôjsť použitím výpočtovej techniky. Jedná sa o niektoré vybrané trestné činy v nasledujúcej kapitole, pri ktorých si zároveň zobrazíme a porovnáme dynamiku ich vývoja v rokoch 2013-2018.

Dynamika vývoja foriem kybernetickej kriminality v slovenskej právnej úprav e za roky 2013 – 2018

Podvody a falšovanie bezhotovostných platobných prostriedkov

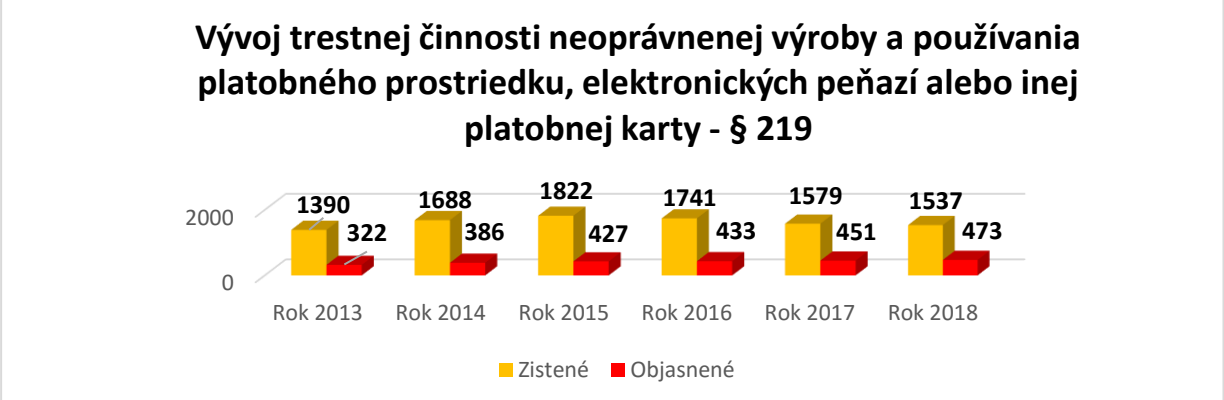
Nové spôsoby trestnej činnosti sa objavili so vznikom elektronických platobných prostriedkov. Uvedenú trestnú činnosť je možné spáchať na akomkoľvek mieste, keďže platobné karty sú prijímané ako prostriedok platenia alebo výberu peňazí doma aj v zahraničí. Ako bezhotovostné platobné prostriedky je ich možné použiť s cieľom vykonania takzvaných non-face to face transakcií, ako napríklad internetové bankovníctvo, tiež pri cezhraničných transakciách, či už v rámci tradičných foriem alebo v internetovom obchode. Pokiaľ ide o trestný čin v Slovenskej republike, ktorý je zhodný s problematikou podvodov a falšovania bezhotovostných platobných prostriedkov, možno upriamiť pozornosť na trestný čin - neoprávnená výroba a používanie platobného prostriedku elektronických peňazí alebo inej platobnej karty - § 219 Trestného zákona.

Neoprávnená výroba a používanie platobného prostriedku elektronických peňazí alebo inej platobnej karty § 219 Trestného zákona

- neoprávnene vyrobí, pozmení, napodobní, falšuje alebo si obstará platobný prostriedok alebo elektronické peniaze alebo inú platobnú kartu vrátane telefónnej karty alebo predmet spôsobilý plniť takú funkciu na účel použiť ho ako pravý, alebo na taký účel ho prechováva, prepravuje použije alebo poskytne inému,
- neoprávnene vyrobí, prechováva, obstará si alebo inak zadováži alebo poskytne inému nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v prvej odrážke.

Následne uvádzame vývoj trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 1.

Graf č. 1



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

Útoky na počítačové systémy

Počítačové systémy patria v dnešnej dobe k nevyhnutnej súčasti života. Ich účelom je uľahčenie a zvýšenie efektivity činnosti, ktoré vykonávame v osobných aj pracovných životoch, napriek tomu ich nie všetci chápu zhodne. Stretávame sa s nimi v dvoch rovinách, pričom prvú rovinu chápeme tak, že jedna skupina ľudí ich využíva pre nich prínosným spôsobom a ich využívaním nespôsobujú iným osobám škody. Naproti tomu druhú rovinu chápeme tak, že druhá skupina ľudí svojím konaním spôsobujú určité škody v počítačových systémoch. Spôsobov ako vykonať škodlivé útoky je niekoľko, ako sme aj vyššie v podkapitole uvádzali. Tieto útoky s vykonávané jednotlivcami, ale aj organizovanými skupinami.

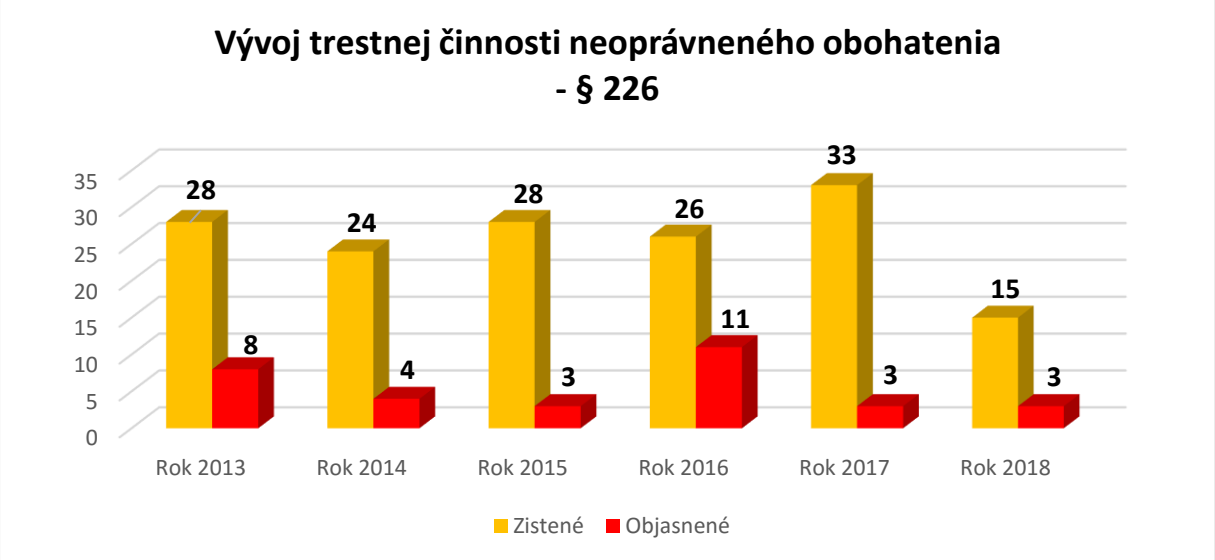
Pokiaľ ide o trestné činy v Slovenskej republike, ktoré sú zhodné s problematikou útokov na počítačové systémy , môžeme poukázať na trestný čin neoprávneného obohatenia (§ 226 TZ), trestný čin neoprávneného prístupu do počítačového systému (§ 247 TZ), trestný čin neoprávneného zásahu do počítačového systému (§ 247a TZ), trestný čin neoprávneného zásahu do počítačového údaja (§ 247b TZ), trestný čin neoprávneného zachytávania počítačových údajov (§ 247c TZ), trestný čin výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov (§ 247d TZ).

Neoprávnené obohatenie § 226 Trestného zákona

Trestného činu neoprávneného obohatenia sa dopustí ten, „kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.“[12] Najčastejším vykonaním tohto trestného činu sú neoprávnené zásahy do výherných automatov.

Následne uvádzame vývoj trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 2.

Graf č. 2



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

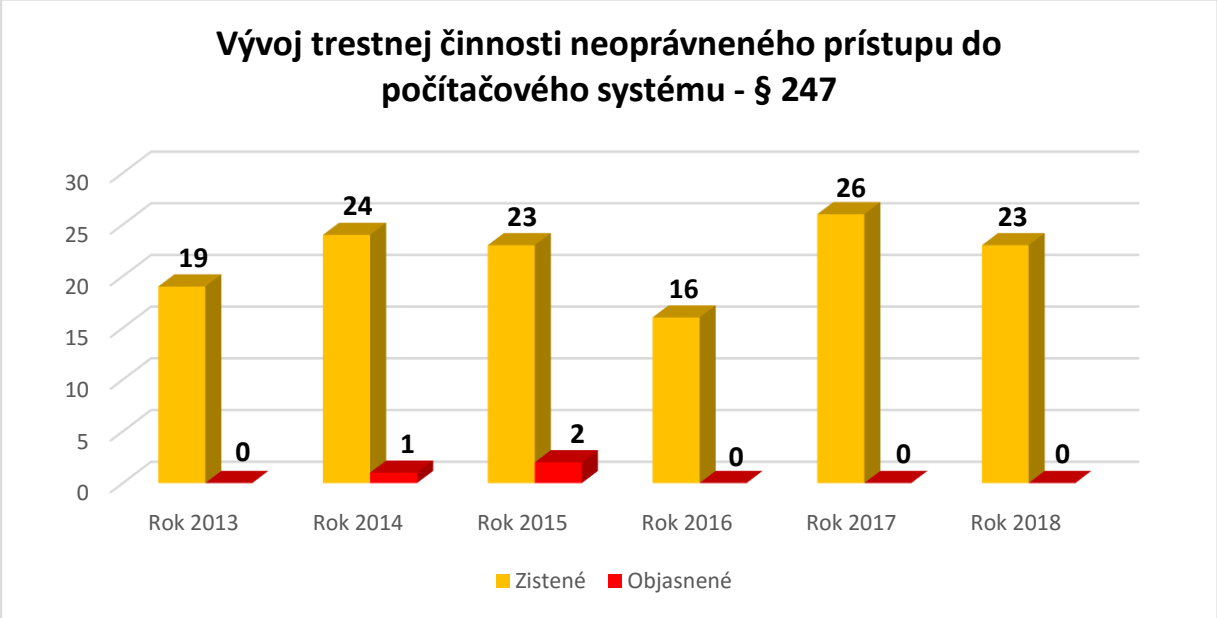
[12] § 226 ods. 1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.

Neoprávnený prístup do počítačového systému § 247 Trestného zákona

Trestný zákon č. 300/ 2005 Z.z. uvádza, že trestného činu neoprávneného prístupu do počítačového systému sa dopustí ten, kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.[13]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 3.

Graf č. 3



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

Porušovanie právnej ochrany softvérových programov a audiovizuálnych diel

Denným využívaním internetu v súčasnej dobe prichádza v spojitosti s nelegálnym využívaním informačných technológii k masovému porušovaniu autorských práv k hudbe, filmom, počítačovým programom a literárnym dielam. Nelegálne kopírovanie počítačových programov, audiovizuálnych diel príde obrovskému množstvu užívateľov ako úplne prirodzené. Ich nezákonná výroba a šírenie je omnoho väčším problémom.[14]

V Slovenskej republike ochranu autorského práva primárne poskytuje Trestný zákon v § 283 a Autorský zákon č. 185/2015 Z.z.

Porušovanie autorského práva § 283 Trestného zákona

Trestný zákon uvádza v § 283 ods. 1 nasledujúce „kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.“[15]

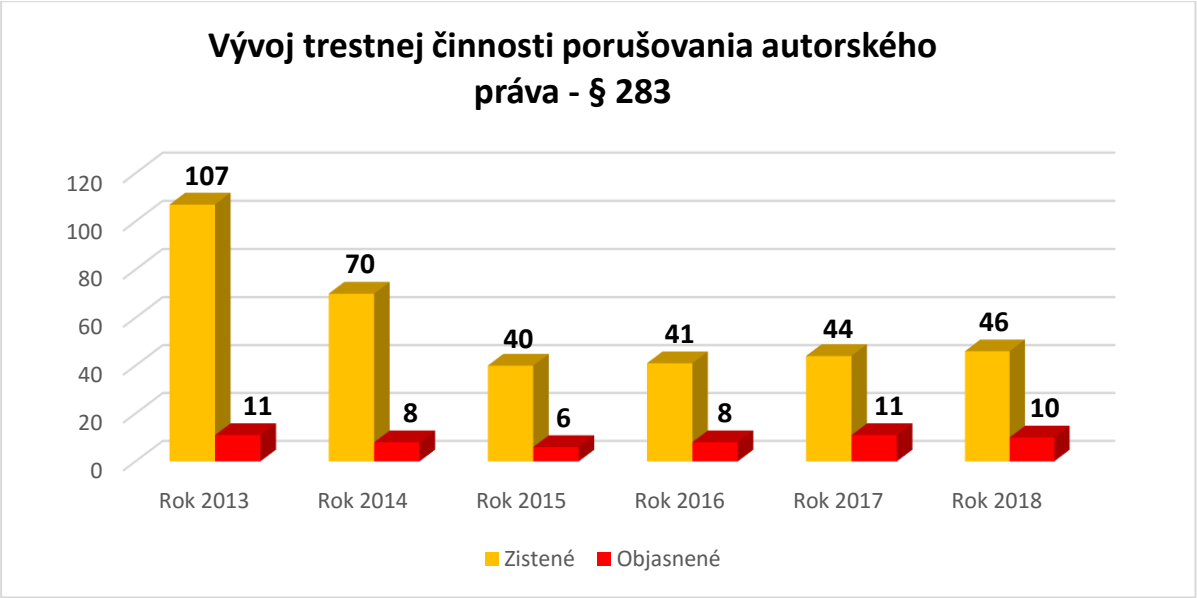
Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 4.

Graf č. 4

[13] § 247 ods.1. *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.

[14] SMEJKAL, V., PORADA, V. Současné problémy spojené s digitalizací, dokazováním, identifikací a autentizací při vyšetřovaní. In *Bezpečnosť, extrémizmus, terorizmus: Zborník príspevkov*, 2015. s. 139.

[15] § 283 ods.1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

Detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia

V súčasnej dobe je sexuálne vykorisťovanie detí úzko spojené s výrobou, rozširovaním a prechovávaním detskej pornografie a éru modernej detskej pornografie môžeme datovať do neskorých 60. a 70. rokov minulého storočia.[16] S rozvojom internetu detská pornografia dostala ďalší rozmer, keďže je priamo prístupná na internete.

Pokiaľ ide o trestné činy v Slovenskej republike, ktoré sú zhodné s problematikou detskej pornografie na internete a kontaktovanie detí na účely ich sexuálneho zneužitia, môžeme poukázať na trestný čin výroby detskej pornografie (§ 368), trestný čin rozširovanie detskej pornografie (§ 369), trestný čin prechovávania detskej pornografie a účasť na detskom pornografickom predstavení (§ 370).

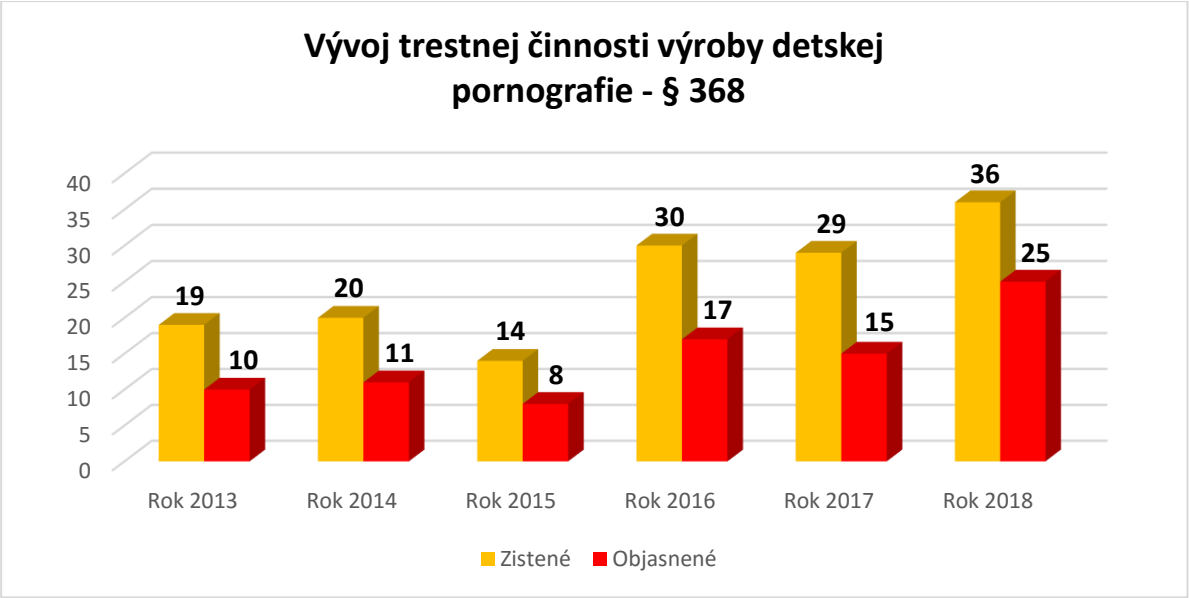
Výroba detskej pornografie § 368 Trestného zákona

V súvislosti v deťmi a mládežou patrí tento trestný čin medzi najzávažnejšie. Trestný zákon v základnej skutkovej podstate uvádza nasledujúce „kto využije, získa, ponúkne alebo inak zneužije dieťa na výrobu detskej pornografie alebo detského pornografického predstavenia alebo umožní také jeho zneužitie, alebo sa inak podieľa na takejto výrobe, potrestá sa odňatím slobody na štyri roky až desať rokov.“[17] K výrobe detskej pornografie zaraďujeme aj výrobu obrázku obalu či obrázku disku s detskou pornografiou.

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 5.

Graf č. 5

[16] KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer s.r.o., 2016. s. 188.
[17] KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer s.r.o., 2016. s. 228.



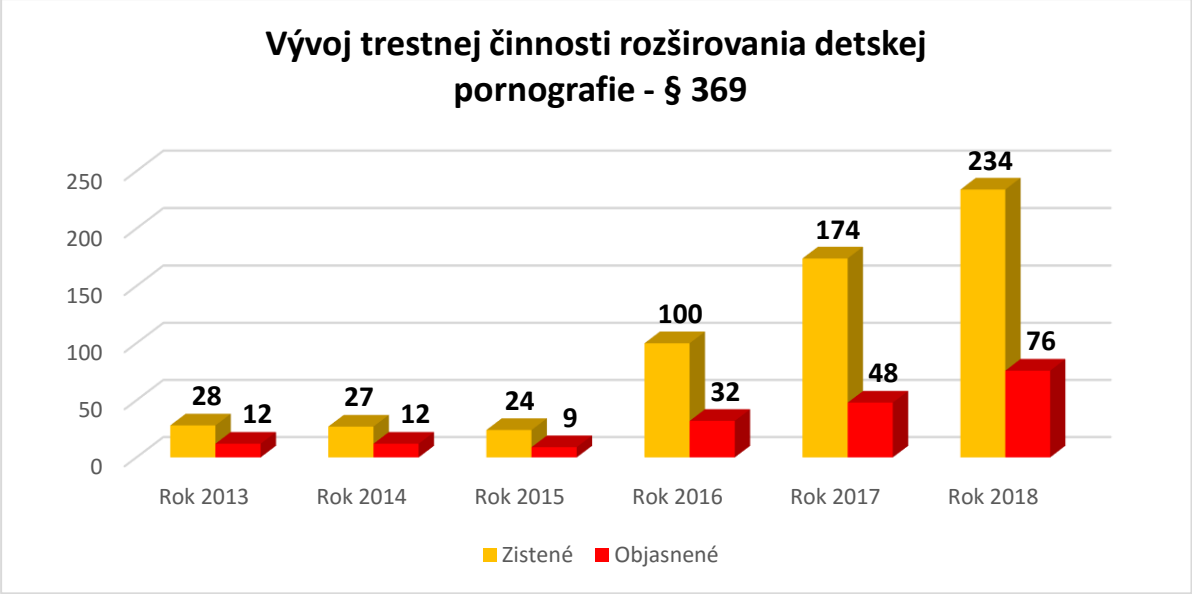
Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

Rozširovanie detskej pornografie § 369 Trestného zákona

Trestný zákon v § 369 ods. 1 uvádza nasledujúce „kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu, potrestá sa odňatím slobody na jeden rok až päť rokov.“[18]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 6.

Graf č. 6



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

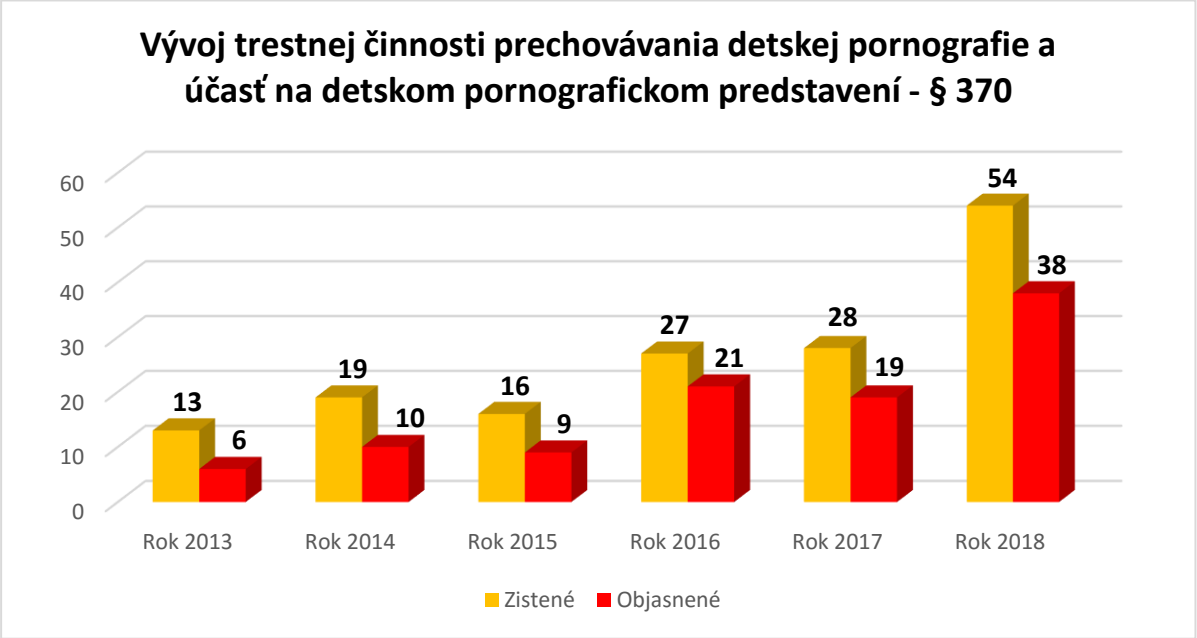
[18] § 369 ods.1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.

Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení § 370 Trestného zákona

„Trestný zákon v základnej skutkovej podstate ustanovuje nasledujúce – kto prechováva detskú pornografiu alebo kto koná v úmysle získať prístup k detskej pornografii prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody až na dva roky.“[19]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu 7.

Graf č. 7



Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: <www.minv.sk>

Záver

Ako sme už spomínali, je veľmi dôležité pochopiť, že kybernetický priestor znamená viac ako len internet. Zahŕňa v sebe nielen hardvér, softvér a informačné systémy, ale takisto prepojenú ekonomiku, ktorá zabezpečuje prácu veľkej časti ľudskej populácie a na záver to najdôležitejšie, vytvára sociálne prepojenia skupín a ľudí. Z toho vyplýva, že hrozby kybernetického priestoru neohrozujú len techniku, technológie, čiže hardvér a softvér, ale aj ich užívateľov to znamená, že ľudí samotných, čo sme si následne graficky zobrazili a porovnali vzhľadom na vývoj dynamiky jednotlivých trestných činov v oblasti kybernetickej kriminality za roky 2013-2018.

Zoznam použitej literatúry:

1. EPRAVO. 2018. *Počítačová kriminalita a jej páchatelia a obete*. [online]. [cit. 27. 06. 2018]. Dostupné na internete:<https://www.epravo.sk/top/clanky/pocitacova-kriminalita-a-jej-pachatelia-a-obete-4113.html>
2. HANKO, M. Kybernetický zločin a kybernetická bezpečnosť. In *Obrana-modernizácia*. 2015. č. 9. s. 32-33.
3. HANKO, M. Hrozby kybernetického priestoru. In *Obrana*. 2015. č. 8. s. 32-33.
4. HROMADA, M. *Kybernetická bezpečnosť*. Praha: Vydavatelství Powerprint, 2015.

[19] KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer s.r.o., 2016. s. 265.

s. 250. ISBN 978-80-87994-72-6.
5. IVOR, J., KLIMEK, L. *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky*. Žilina: EUROKÓDEX, 2013. ISBN 978-80-8155-017.
6. KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016. ISBN 978-80-8168-538-5.
7. Ministerstvo vnútra SR. 2019. *Štatistika kriminality v Slovenskej republike*. [online]. [cit. 16. 06. 2018]. Dostupné na internete: <http://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml>
8. NAJPRAVO. 2012. *Základné formy počítačovej kriminality.* [online]. [cit. 15. 06. 2018]. Dostupné na internete:<http://www.najpravo.sk/clanky/zakladne-formy-pocitacovej-kriminality.html>
9. POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018. s. 640. ISBN 978-80-7598-045-8.
10. PREVENTISTA. 2017. *Počítačová internetová kriminalita a jej prevencia v školskom prostredí.* [online]. [cit. 16. 06. 2018]. Dostupné na internete: <http://preventista.sk/info/pocitacova-internetova-kriminalita-a-jej-prevencia-v-skolskom-prostredi/>
11. SAK, P. *Úvod do teorie bezpečnosti*. Vydavatelství Petrklíč, 2018. s. 271. ISBN 978-80-7229-652-1.
12. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-201-2.
13. SMEJKAL, V., PORADA, V. *Současné problémy spojené s digitalizací, dokazováním, identifikací a autentizací při vyšetřovaní*. In Bezpečnosť, extrémizmus, terorizmus: Zborník príspevkov z medzinárodného vedeckého sympózia konaného dňa 25.marca na Katedre trestného práva Právnickej fakulty Univerzity P.J. Šafárika v Košiciach. Košice: Univerzita P.J. Šafárika v Košiciach, 2015. ISBN 978-80-8054-601-4.
14. SMEJKAL, V., PORADA, V. Vybrané aspekty metodiky vyšetrovaní kybernetické kriminality. In ROMŽA, S. – FERENČÍKOVÁ, S. et MICHAĽOV, L. (eds.) *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty. Zborník príspevkov z medzinárodného vedeckého sympózia* konaného dňa 28.marca na Katedre trestného práva Právnickej fakulty Univerzity P.J. Šafárika v Košiciach. Košice: Univerzita P.J. Šafárika v Košiciach, 2014. ISBN 978-80-8152-146-1.
15. ŠPIDLA, A. Úvod do kybernetické a informační bezpečnosti. In *Security magazín*. 2017. č. 6. s. 35-36.
16. ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR a.s., 2017. ISBN 978-80-7552-758-5.
17. Zákon č. 300/2005 Z.z. trestný zákon v znení neskorších predpisov.

Kontaktné údaje:
npor. Bc. Mgr. Liliana Réveszová
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
liliana.reveszova@minv.sk

Problematika sextingu u detí a mládeže

Zuzana Dobrovanov Šimová

Abstrakt:
Predkladaná práca sa zaoberá problematikou kybernetickej kriminality vo vzťahu ku deťom a mládeži. Príspevok sa zameriava na problematiku sextingu vo vzťahu ku tejto vekovej skupine, a jeho možným dopadom v následnom očierňovaní, tzv.“ revenge porn“. Cieľom príspevku je poukázať na niektoré špecifiká tejto problematiky v praxi a možné preventívne opatrenia.
Kľúčové slová:
Deti a mládež, kybernetická kriminalita, kyberšikana, sexting, legislatíva.

Abstract:
This work deals with the issue of cybercrime in relation to children and youth. The paper focused sexting in relation to this age group and its possible impact in subsequent slander, tzv.“ revenge porn“. The aim of the paper is to point out some specificities of this issue in practice and possible preventive measures.
Key words:
Children and youth, cybercrime, cyberbullying, sexting, legislation.

Úvod

Prudký rozvoj informačných a komunikačných technológií v modernej spoločnosti, ktorý nastal v posledných desaťročiach celosvetovo, sprevádzajú rôzne fenomény. Popri pozitívach, ktoré majú vplyv na náš život, objavuje sa aj celý rad sprievodných negatívnych dopadov, ktoré pôsobia na spoločnosť ako celok, či na jednotlivcov v rámci nej. Medzi najzávažnejšie dopady v tomto smere nepochybne patrí kriminalita v jej nových, špecifických podobách.

Niektorí autori[1] poukazujú na terminologickú rôznosť nielen v našej, ale aj v zahraničnej odbornej literatúre – Greguš hovorí o počítačovej kriminalite, respektíve o kybernetickej kriminalite, pričom tieto pojmy sú niekedy komunikované ako identické, inokedy sú chápané ako nie synonymické – kybernetické kriminalita je vymedzovaná ako časť počítačovej kriminality. Pritom uvádza, že istým harmonizačným prvkom sa stala Convention on Cybercrime.[2] Zahŕňa celý rad trestných činov v rámci počítačovej kriminality – ide o trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov, týkajúce sa nezákonného prístupu, nezákonného zachytávania údajov a zasahovania do nich, zásahov do systému a zneužívania zariadení. Ďalej tiež ide o počítačové trestné činy, prepojené s počítačovými podvodmi a falšovaním počítačových údajov. Treťou oblasťou počítačovej kriminality sú trestné činy, prepojené s porušovaním autorských a príbuzných práv. Poslednou z definovaných oblastí sú trestné činy, týkajúce sa nevhodného obsahu (detské pornografia).

Volevecký [3] rozlišuje z hľadiska formy spracovania pojmy počítačové a elektronické dielo. Pritom elektronické dielo je nadradeným pojmom, popri počítačovom zahrňuje aj mobilné telefóny a ďalšie zariadenia.

Smejkal rozlišuje trestné činy spáchané prostredníctvom počítača ako prostriedku a trestné činy spáchané počítačom ako prostriedkom útoku. [4]

V priebehu času sa výpočet trestných činov, prepojených na počítačové technológie a kyberpriestor, rozširuje. S tým sa niekedy spájajú pôvodné, klasické formy trestnej činnosti,

---

[1] GREGUŠ, L. Obete kybernetickej kriminality. Niektoré trestnoprávne aspekty obetí kriminality prostredia informačných sietí. In: *Obete kriminality*. Zborník príspevkov z medzinárodnej konferencie, Bratislava: Fakulta práva, Paneurópska vysoká škola, 2013. s. 54-68.

[2] u nás známy ako Dohovor o počítačovej kriminalite, s platnosťou od 1. máj 2008, ktorý zahrňuje celý rad trestných činov.

[3] VOLEVECKÝ, P. Kybernetické trestné činy v trestním zákoníku. In: *Trestní právo*, roč. 14, č. 7, 2010. s. 19-43.

[4] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeňek, 2015. 636 s.

akou je nepochybne aj detská pornografia. No vznikajú aj nové formy kriminality – kyberagresia, kyberšikanovanie, kyberstalking. V tejto práci sa zameriavame na jednu z konkrétnych foriem, sexting a jeho prepojenie so zneužitím materiálov formou očierňovania, tzv.“ revenge porn“.

Kyberagresia, kyberšikana, sexting

Vymedzíme základné pojmy problematiky. Najvšeobecnejšie používaným a zastrešujúcim odborným pojmom je pojem kyberagresia. Chápeme ním poškodenie spôsobené zámerným jednorazovým útokom prostredníctvom elektronických prostriedkov, môže byť spôsobené jednotlivcovi alebo skupine osôb. Je nezávisle na ich veku, pričom tieto osoby vnímajú uvedený čin ako urážlivý, hanlivý, škodlivý alebo nežiaduci.[5]

Kyberšikana je súčasťou kyberagresie, ide o útoky opakované a jej súčasťou je nerovnováha moci medzi obeťou a páchateľom. [6]

Rozumieme ňou využívanie informačných a komunikačných technológií, ktoré podporujú úmyselné, nepriateľské a často opakované správanie jednotlivca alebo skupiny s úmyslom ublíženia. [7]

Špecifickou formou správania a možnej trestnej činnosti vo vzťahu ku kyberpriestoru je sexting. Sextingom rozumieme elektronické zasielanie rozličných materiálov s erotickým a sexuálnym obsahom, týkajúcim sa samotného odosielateľa – vlastných textov, fotografií, videí – prostredníctvom sms, mms, e-mailom, prípadne aj ich zdieľanie. Bývajú zasielané rovesníkom, alebo aj neznámym ľuďom z chatu či zoznamky.[8]

Popri romantických vzťahoch býva sexting aj nástrojom pre potlačenie nudy, ako produkt konzumnej spoločnosti, nástrojom sebaprezentácie, pre predvádzanie sa, nástrojom ako produkt sociálneho tlaku, na získanie záujmu, menej častý je finančný dôvod. Sexting môže mať aktívnu alebo pasívnu podobu.[9]

Kopecký a kol. (2015) uvádzajú zistenia z troch výskumov, realizovaných v Slovenskej a Českej republike v rokoch 2014 a 2015 u detí a mládeže.[10] V rámci neho sexting v podobe umiestneného vlastného intímneho obsahu na internete priznalo 7, 6% detskej slovenskej populácie vo veku medzi 11. až 17. rokom života. Vlastné sexuálne ladené materiály odoslalo iným osobám 9, 31% slovenských 11.-17.- ročných respondentov. Ako vidíme z uvedeného, častejšie odosielajú vlastné sexuálne ladené materiály ženy ako muži, a najčastejší, až 60%-ný je výskyt takéhoto konania vo vekovej skupine medzi 15. až 17. rokom života

Revenge porn[11] ako forma nonkonsenzuálneho porna

Frekventným dôvodom sextingu je zasielanie materiálov so sexuálnym obsahom v rámci romantických vzťahov. Podľa výskumu z roku 2008 až 71% adolescentných žien a 67% adolescentných mužov zaslali niekedy správy so sexuálnym obsahom svojmu priateľovi/ priateľke. Pritom až 38% žien a 39% mužov v skúmanom súbore uviedlo, že dostali správy

---

[5] HOLLÁ, K. *Sexting a kyberšikana*. Bratislava: IRIS, 2016. s. 5.

[6] Ako uvádza KOPECKÝ a kol., môže ísť o správanie primárneho páchateľa alebo aj sekundárnych útočníkov, šíriteľov. In KOPECKÝ, K., SZOTKOWSKI, R., KREJČÍ, V. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc: Univerzita Palackého v Olomouci, 2015. 168 s.

[7] HINDUJA, PATCHIN (2012), In HOLLÁ, K. *Sexting a kyberšikana*. Bratislava, 2016. s. 13.

[8] HOLLÁ, HOLLÁ, K. *Detekcia kyberagresie – kyberšikanovania a sextingu.* Nitra: Pedagogická fakulta UKF v Nitre, 2017. 113 s.

[9] v zmysle klasifikácie uvádzanej ÁLVAREZOM – GARCIOM a kol., In HOLLÁ, K.: *Sexting a kyberšikana*. Bratislava, 2016.

[10] výskum bol realizovaný u slovenských detí na vzorke 1466 detí, v Českej republike sa ho zúčastnilo 28 232 detí. Podľa: KOPECKÝ, K. a kol.: *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc, 2015.

[11] Skuročný význam pojmu „revenge porn“ znamená „pomsta formou uverejnenia porna osoby bez jej vedomia“

určené pôvodne inej osobe. Vo vekovej skupine 13.- až 19.- ročných priznala zasielanie správ so sexuálnym obsahov pätina súboru. Vystavenie tlaku, aby zaslali o sebe materiál so sexuálnym obsahom, uvádzalo 51% adolescentných žien a 18% adolescentných dievčat.[12]

Scenár sextingu obvykle začína milostným vzťahom dvoch mladých ľudí, pričom či už na naliehanie partnera alebo z vlastnej iniciatívy vo väčšine prípadov dievčina sama vyrobí a aj posiela fotografie svojho nahého tela priateľovi. Prípadne ich zhotoví v spolupráci so svojim partnerom v čase trvania vzťahu. (Pokiaľ je jeden z partnerov mladší ako 15 rokov, má trestnoprávne následky aj samotný sex medzi nimi – to však nie je v centre pozornosti tejto práce. Zákon tiež sankcionuje osoby vo veku od 15 do 18 rokov, ktorým síce priznáva právo na sex beztrestne, no trestá výrobu akejkoľvek dokumentácie – fotografií, videí, čí zápiskov - o tom).[13]

Pri nezhodách vo vzťahu - v situácii, že sa chce s partnerom rozísť, resp. odmieta návrat k nemu - dochádza ku zverejneniu týchto fotografií partnerom spoločným známym, resp. zdostupní sa na sociálnych sieťach a webových stránkach aj cudzím ľuďom. Ide o tzv. „revenge porn“. [14]

Páchatelia sú najčastejšie ex-partneri, a z ich pohľadu ide o akt zastrašovania, či pomsty a poníženia voči obeti. Okrem pomstivého ex-partnera môže obsah stiahnuť a šíriť hacker. [15]

Odborne o „revenge porn“ hovoríme ako o časti non-konsenzuálneho porna, nakoľko sa intímny materiál zdostupňuje non-konsenzuálnym spôsobom, t. j. bez súhlasu obete. V prípadoch, týkajúcich sa detských a mladistvých obetí nadobúda tento problém i rozmer vekový. Patria medzi zvlášť zraniteľné obete. je nutné špecificky pristupovať k týmto obetiam aj v rámci riešenia prípadu. V zmysle zákona o obetiach sú niektoré z obetí kvalifikované ako zvlášť zraniteľné obeti, či už vo vzťahu ku zvýšenému riziku zastrašovania páchateľom, alebo v dôsledku zvýšeného rizika vzniku druhotnej ujmy v súvislosti s vekom, pohlavím rozumovou vyspelosťou, zdravotným stavom či inými okolnosťami a znakmi, týkajúcimi sa obete. Sú preto pre ne ustanovené špecifické opatrenia, aby sa zabránilo prehlbovaniu stresu a riziku sekundárnej traumatizácie.[16]

Ide o jav, ktorého závažné dopady na obeť preukázali početné odborné výskumy. Nie je preto našim cieľom v tomto príspevku kriminalizovať samotné obete ešte aj prostredníctvom legislatívy. Tvorca sextingu môže byť následne vystavený rizikovému správaniu zo strany ex-partnera či iných osôb - sexuálnemu obťažovaniu alebo sexuálnym útokom, vydieraniu. Prežívanie ujmy zo strany obete je veľmi individuálne, v závislosti od osobnosti obete, jej životnej situácie a okolností činu.

Ako dôsledok je u obetí popisovaná psychická a emocionálna ujma – obeť môže byť zaplavená negatívnymi pocitmi v zmysle hnevu, smútku, návalmi úzkosti, kolísania nálad, narušenia koncentrácie pozornosti, podráždenosti, poníženia, hanby, bezmocnosti, uzavretosti a sociálnej izolácie, aj sprievodné telesné príznaky – ako sú bolesti brucha, hlavy, chrbta, nechutenstvo, nespavosť. V niektorých prípadoch sa môže rozvinúť aj posttraumatická stresová porucha.[17]

---

[12] Sex and Tech. *Results from a Survey of Teens and Young Adults*. [online]. [2019-04-22]. Dostupné na internete: <http://www.thenationalcampaign.org/sextech/pdf/sextech_ summary.pdf.>

[13] KOPECKÝ, K. a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc, 2015.

[14] FRANKS, M. A.: *Combating Non-Consensual Pornoghraphy: A working paper*. [online]. [2019-04-22]. Dostupné na internete:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336537.>

[15] v rámci nástroja pomsty ex-partnerov existujú dokonca stránky, kde sú nahraté fotografie a videá s vulgárnymi komentmi, ako popisuje napríklad výskum WALKER, SANCI, TEMPLE SMITH, 2013, In KOPECKÝ, K. a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc, 2015. s. 46.

[16] Polície ČR. 2019. *Sexuální a mravnostní trestní činy*. [online]. [2019-04-22]. Dostupné na internete: <https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx.>

[17] Polície ČR. 2019. *Sexuální a mravnostní trestní činy*. [online]. [2019-04-22]. Dostupné na internete: <https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx, op. cit.>

V tejto súvislosti je z nášho pohľadu dôležité uvedomiť si dva základné aspekty problematiky – prvým z nich je, že je veľmi dôležité pre obeť následné vyhľadanie psychologickej alebo psychiatrickej pomoci, čo u nás nie je ešte samozrejmosťou, aj napriek tomu, že odborníkmi popisované následky pre obeť sú závažné.

Segool a Crespi (2011) uvádzajú ako dopady sextingu odcudzenie, aj závažné psychické dopady – emocionálnu úzkosť, depresiu, izoláciu, beznádej, suicidálnosť.[18]

Prípady dokonaných samobrážd detí a mladistvých v súvislosti so sextingom popisujú aj Russo, Osborne, Arndt (2011). [19]

Druhým aspektom je potreba uvedomiť si, že dopady na obeť nekončia prešetrením prípadu a nájdením páchateľa. Môže dochádzať ku následnému šíreniu citlivých materiálov v rovesníckom prostredí, či verejne. Ku týmto následkom môžeme pridať aj stratu súkromia, narušenie rodinných vzťahov, šikanovanie, poškodenie povesti a prestíže obete, v dôsledku toho môže mať obeť ťažkosti, získať či udržať zamestnanie, je urážaná a dehonestovaná,[20] viaceré zahraničné výskumy preukázali aj súvis so závislosťami, či s nekontrolovaným sexualizovaným správaním. V prípade detských a mladistvých obetí vzniká aj narušenie vzťahov v rámci rovesníckej skupiny – triedneho a školského kolektívu. [21]

Sexting zanecháva stopy na jej sociálnom statuse a sociálnych vzťahoch. Sú rozdielnosti v prístupe ku sextingu v závislosti od pohlavia, kým chlapcov nestigmatizuje, pre dievča znamená významnú spoločenskú stigmu. Výskumy preukazujú častejší výskyt aj závažnejšie následky u dievčat a žien v porovnaní s mužskými obeťami. [22]

Legislatívne aspekty problematiky

Mravnostné trestné činy zasahujú štyri základné roviny, a to – morálne vzťahy v spoločnosti, život a zdravie človeka, poškodeného v dôsledku protiprávneho konania v oblasti sexuálnych vzťahov, zdravý vývin mládeže a dobré mravy v sexuálnych vzťahoch medzi dospelými. Šíritelia sextingu môžu byť páchateľmi priestupku, resp. aj celého radu trestných činov (výroby, držania a šírenia detskej pornografie (§ 368 TZ), ohrozovania mravnej výchovy mládeže (§ 211 TZ), ale aj vydierania (§ 189 TZ), nátlaku (§ 192 TZ), nebezpečného prenasledovania (§ 360 TZ), poškodzovania cudzích práv (§ 376 TZ), možný je i § 122 ods. 7 TZ, vo vzťahu ku využitiu fyzického či psychického násilia, omámenia, či ľsti páchateľom voči obeti - v závislosti od druhu fotografií a spôsobu ich obstarania, či správania páchateľa. Samo osebe stíhanie páchateľa-šíriteľa týchto materiálov však obvykle nie je riešením celej situácie z hľadiska obete – ide o pokračujúce dopady ujmy na obeť v jej životnom prostredí, resp. v dôsledku držby a šírenia citlivých materiálov ďalšími osobami. Dôsledky môžu dopadať, ako sme poukázali vyššie na obeť aj po rokoch – v rámci jej vzťahov či profesijnej kariéry.

---

[18] ALDRIDGE, M. J. et al. Sexting: You Found the Sext, What to Do Next? How School Psychologists Can Assist with Policy, Prevention, and Intervention. In: *Counselor Education and Human Services Faculty Publications*. Paper 13, s. 6-10. [online]. [2019-04-22]. Dostupné na internete: <http://ecommons.udayton.edu/edc_fac_pub/13.>

[19] ALDRIDGE, M. J. et al. Sexting: You Found the Sext, What to Do Next? How School Psychologists Can Assist with Policy, Prevention, and Intervention. In: *Counselor Education and Human Services Faculty Publications*. Paper 13, s. 6-10.

[20] KOPECKÝ, K. a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc, 2015.

[21] naruší sa ich sociálna pozícia v kolektíve, niektoré obete musia meniť školu, tým na rušia ich vzdelávacie príležitosti.

[22] FRANKS, M. A. *Combating Non-Consensual Pornoghraphy: A working paper*.

Vo vzťahu ku deťom a mladistvým je táto problematika špecificky citlivá, najmä ak môžeme očakávať ďalší rozvoj moderných technológií a musíme rátať s generáciou „digitálnych domorodcov“.[23]

Hinduja a Patchin [24] poukazujú, že práve digitálni domorodci sa stávajú častejšie obeťami sextingu.

Chmelík (2014a) [25] uvádza, že protiprávne konania, ktorých obeťou je dieťa, sú vnímané verejnosťou veľmi citlivo. Vykazujú vysokú mieru spoločenskej škodlivosti a tomu zodpovedajú aj sankcie. Upozorňuje, že v úvode týchto skutkov je často pričinenie samotnej obete, ktorá intímny materiál o sebe vyrobí a samotnému následnému páchateľovi aj dobrovoľne posiela, vzhľadom na vek obete - dieťa – ani nemožno zvažovať akúkoľvek trestnú zodpovednosť. Z pohľadu preukazovania možno podľa neho označiť podľa predchádzajúcej, ale aj súčasnej českej úpravy trestný čin šírenia pornografie (§ 191), a to predovšetkým z pohľadu absencie jednoznačného obsahu tohto pojmu a jeho právneho vymedzenia. Poukazuje na rôznosť vymedzenia čo je a čo nie je pornografické, aj na častú účelovosť takéhoto hodnotenia z aspektu komerčného. [26] S týmto názorom sa nepochybne možno stotožniť. Pokladáme za žiaduce zjednoznačňovať obsah pojmu, s prioritným záujmom spoločnosti a nie komerčnosti.

Vzhľadom na postupné zlaďovanie legislatív členských krajín v rôznych oblastiach života spoločnosti a občanov predpokladáme potrebu prejsť od súčasnej úpravy v zmysle hranice (vymedzenej vnútroštátnym právom vo vzťahu ku vekovej hranici, pod ktorú je v príslušnej krajine zakázaná účasť na sexuálnych praktikách s dieťaťom) ku jednotne stanovenej vekovej hranici. Pokladáme za vhodné smerovať medzinárodné legislatívne iniciatívy ku zjednocovaniu v súčasnosti rozdielnych legislatív a názorov v rámci krajín EÚ na jednotnú vekovú hranicu 18 rokov ako vek plnej pohlavnej dospelosti za účelom stanovenia hranice detskej pornografie. Domnievame sa, že vyššia veková hranica je podstatná aj v záujme zvýšenej ochrany obetí v rámci sextingu a následného šírenia „revenge porna“, uľahčí vymáhanie práva pre ne.

Nepochybne najzásadnejšou ochranou obetí sextingu však je prevencia, realizovaná už u detí v mladšom školskom veku. V súvislosti s tým je podstatná multirezortná spolupráca pri riešení problematiky – upovedomovanie detí o možných následkoch sextingu a to tak voči následkom pre obete, ako aj následkom pre páchateľov samotných formou preventívnych programov, realizovaných odborníkmi v prostredí škôl. Žiaduce je tiež z nášho pohľadu informovať deti a mládež o tom, že následné šírenie sexuálne citlivých materiálov, zasielaných či uverejňovaných v rámci nekonsenzuálneho sextingu a „revenge porna“, prináša takisto trestnoprávne následky nielen pre páchateľa samotného, ale aj pre jeho ďalších šíriteľov.

Záver

V predkladanej práci poukazujeme na základné aspekty problematiky sextingu u nás a následného „revenge porna“. Vo vzťahu ku skutočnosti, že počet takýchto prípadov má v spoločenskej praxi narastajúci trend a vzhľadom na vyrastajúcu generáciu digitálnych

[23] GKIOULOS et al. (2017) zavádza tento termín na generáciu detí, vyrastajúcich v digitálnej dobe, In Kurucová, Z. Hrozba a výskyt negatívnych javov na internete u detí – digitálnych domorodcov. In *Zborník Kriminológia ako súčasť trestnej politiky*. Praha: Leges, 2018. s. 145-156.

[24] KURUCOVÁ, Z. Hrozba a výskyt negatívnych javov na internete u detí – digitálnych domorodcov. In *Zborník Kriminológia ako súčasť trestnej politiky*. Praha, 2018. s. 146.

[25] CHMELÍK, J. 2014. Otázky spojené s mravnostní trestnou činností - II. část. *Právní proctor*. [online]. [2019-04-22]. Dostupné na internete: <https://www.pravniprostor.cz/clanky/trestni-pravo/otazky-spojene-s-mravnostni-trestnou-cinnosti-ii-cast>

[26] CHMELÍK, J. 2014. Otázky spojené s mravnostní trestnou činností - I. část. *Všehrd*. [online]. [2019-04-22]. Dostupné na internete: <https://www.vsehrd.cz/clanek/otazky-spojene-s-mravnostni-trestnou-cinnosti-i-cast_fda541ee-85de-4a77-bcff-ddf47408a78a.>

domorodcov možno očakávať do budúcnosti ešte pribúdanie takýchto prípadov, a to najmä vo vekovej skupine detí a mladistvých. Je preto problematike potrebné venovať dôslednú legislatívnu pozornosť. V súvislosti s tým vyvstáva aj dôležitosť multirezortnej spolupráce nielen pri riešení prípadov a pomoci obetiam, ale tiež v oblasti prevencie tohto konania u detí v prostredí škôl.

Zoznam použitej literatúry:

1. ALDRIDGE, M. J. et al. 2013. *Sexting: You Found the Sext, What to Do Next? How School Psychologists Can Assist with Policy, Prevention, and Intervention*. [online]. [cit. 2019-04-22]. Dostupné na internete:<http://ecommons.udayton.edu/edc_fac_pub/13.>
2. ČIČKÁNOVÁ, D. *Procesnoprávne aspekty práva na informačné sebaurčenie a práva byť zabudnutý.* Zborník z medzinárodnej vedeckej konferencie Bratislavské právnické fórum, 2013.
3. FRANKS, M. A. 2014. *Combating Non-Consensual Pornography: A working paper*. [online]. [cit. 2019-04-22]. Dostupné na internete: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336537.>
4. GREGUŠ, L. Obete kybernetickej kriminality. Niektoré trestnoprávne aspekty obetí kriminality prostredia informačných sietí. In *Obete kriminality*. Zborník príspevkov z medzinárodnej konferencie, 2013. Bratislava : Fakulta práva, Paneurópska vysoká škola, 2013. 416 s. ISBN 978-80-8153-015-9.
5. HOLLÁ, K. *Sexting a kyberšikana*. Bratislava : IRIS, 2016. 147 s. ISBN 978-80-8153-061-6.
6. HOLLÁ, K. *Detekcia kyberagresie – kyberšikanovania a sextingu*. Nitra : Pedagogická fakulta UKF v Nitre, 2017. 113 s. ISBN 978-80-558-1205-2.
7. CHMELÍK, J. 2014. *Otázky spojené s mravnostní trestnou činností - I. část.* [online]. [cit. 2019-04-22]. Dostupné na internete:<https://www.vsehrd.cz/clanek/otazky-spojene-s-mravnostni-trestnou-cinnosti-i-cast_fda541ee-85de-4a77-bcff-ddf47408a78a.>
8. CHMELÍK, J. 2014. *Otázky spojené s mravnostní trestnou činností - II. část.* [online]. [cit. 2019-04-22]. Dostupné na internete:<https://www.pravniprostor.cz/clanky/trestni-pravo/otazky-spojene-s-mravnostni-trestnou-cinnosti-ii-cast.>
9. KOPECKÝ, K., SZOTKOWSKI, R., KREJČÍ, V. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc : Univerzita Palackého v Olomouci, 2015. 168 s. ISBN 978-80-244-4861-9.
10. KURUCOVÁ, Z. Hrozba a výskyt negatívnych javov na internete u detí – digitálnych domorodcov. In *Zborník Kriminológia ako súčasť trestnej politiky*. Praha : Leges, 2018. 330 s. ISBN 978-80-7502-279-0.
11. POLÍCIE ČR. 2019. *Sexuální a mravnostní trestní činy*. [online]. [cit. 2019-04-22]. Dostupné na internete:<https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx.>
12. SEX AND TECH. 2008. *Results from a Survey of Teens and Young Adults.* [online]. [cit. 2019-04-22]. Dostupné na internete: <http://www.thenationalcampaign.org/sextech/pdf/sextech_ summary.pdf.>
13. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň : Vydavatelství a nakladatelství Aleš Čeňek, 2015. 636 s. ISBN 978-80-7380-501-2.
14. ŠEVČÍKOVÁ, A. a kol. *Děti a dospívajíci online.* Praha : Grada Publishing, 2014. 183 s. ISBN 978-80-210-7527-6.
15. ŠKOHEL, D. *Obete kyberšikany.* 2015.
16. VOLEVECKÝ, P. Kybernetické trestné činy v trestním zákoníku. In *Trestní právo,* 2010, roč. 14, č. 7, s. 19-43. ISSN 1211-2860.

17. ZÁHORA, J. Ochrana obetí trestných činov ako súčasť trestnej politiky. In *Zborník Kriminológia ako súčasť trestnej politiky*. Praha : Leges, 2018. 330-s. ISBN 978-80-7502-279-0.
18. KOŠECKÁ, D. In *Obete kriminality*. Seminár s medzinárodnou účasťou. Bratislava : Fakulta práva, Paneurópska vysoká škola, 2015. 416 s. ISBN 978-80-89726-45-5.

Kontaktné údaje:
JUDr. Zuzana Dobrovanov Šimová
Konkurzný a reštrukturalizačný správca advokát v Lučenci
zuzana.simova11@gmail.com

„Fake news“ a propaganda v kybernetickom priestore

Stanislav Šišulák, Martina Cíchová

Abstrakt:
Autori príspevku sa snažia poukázať na dezinformácie, v modernejšom poňatí „fake news“, ktoré v súčasnej dobe predstavujú vážny bezpečnostný problém. Fake news, hoaxy a propaganda, to všetko narúša dôveru vo verejné inštitúcie, v zavedené médiá aj demokratické zriadenie. Konštantný prísun nedôveryhodných informácií navyše ľudí demotivuje a vzbudzuje v nich apatiu proti fake news nejako zasiahnuť. Kyberpriestor je zaručene tou najväčšou hrozbou medzi formami šírenia fake news. Uvedené prostredie je síce najmladším médiom zo všetkých, avšak v popularite je na prvom mieste. V dnešnej dobe sa do prostredia internetu pravidelne pripojí sto miliónov ľudí.
Kľúčové slová*:*
Propaganda, fake news, hoax, internet, kyberpriestor.

Abstract:
The authors of the post are trying to point out the misinformation, in modern concept of "fake news", which currently represent a serious security problem. Fake news, hoax and propaganda, all of this undermines trust in public institutions in the established media and the democratic establishment. A constant flow of untrusted information in addition people demotivations and inspires in them an apathy against fake news somehow hit. Cyberspace is guaranteed to be the greatest threat among the forms of dissemination of fake news. Given environment it is the youngest medium of all, however its first in popularity. Nowadays, in the environment of the internet regularly connects hundred million people.
Key words:
Propaganda, fake news, hoax, internet, cyberspace.

Úvod

Presná, jediná definícia dezinformácie neexistuje. Odborníci sa nevedia dohodnúť, väčšinou sa ale zhodujú na kľúčových aspektoch tohto pojmu. Dezinformáciu teda možno definovať ako „*úmyselne nesprávnu či skreslenú informáciu, ktorá je zámerne implantovaná do informačnej sústavy oponenta so zámerom ovplyvniť jeho aktivity*“[1]. Ide teda o zámerne nepravdivú či zavádzajúcu informáciu, či už ide o správu, upravenú či misinterpretovanú fotografiu alebo hlasový prejav, ktorá má za úlohu ovplyvniť príjemcu danej správy tak ako to zamýšľa dezinformátor.

Zmienka o cieli dezinformácie je výsostne dôležitá. Zámer dezinformácie je totiž to, čo ju odlišuje od misinformácie, teda prostej fámy. Zatiaľ čo fáma je šírená bez toho, aby jej šíritelia tušili, že ide o lož, pôvodcovia dezinformácie zámerne vysielajú do sveta nepravdivú informáciu. Je síce možné, či dokonca pravdepodobné, že dezinformácia v sebe bude obsahovať nejakú časť pravdy, zároveň tu ale bude klbko nezmyslov, ktorým práve správne informácie dodajú na kredibilite[2].

Modernejšie poňatie dezinformácií predstavuje termín „fake news“, ktorý bol oficiálne uvedený do lexikónu v roku 2017. Ide o dezinformácie pod iným, moderným názvom[3]. Tento pojem radi používajú verejní činitelia, ktorí chcú podrývať stabilné základy demokracie. Na prvom mieste je možné zmieniť amerického prezidenta Donalda Trumpa, ktorý veľmi často obviňuje novinárov a reportérov z rozširovania fake news[4].

Pojem fake news o propaganda sú dva pojmy, ktoré sú spolu v histórii často veľmi tesne spojené. Termín propaganda sa vždy nepoužíval v rovnakom význame ako v dnešnej dobe.

---

[1] KRKOŠKA, D. *České dezinformační weby a jejich obsah*. 2018. s. 9.
[2] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích*!!! 2018. s. 8-9.
[3] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích*!!! 2018. s. 8.
[4] EGAN, L., T. The fake news is creating violence. 2019.

Skôr išlo o neutrálny termín, ktorý až časom nadobudol skôr negatívnu, či pejoratívnu hodnotu dnešného chápania. V neutrálnom význame však propaganda znamená šíriť, hájiť alebo podporovať konkrétne myšlienky.

Slovo propaganda pochádza z latinského „propagatio“, čo znamená šírenie. Zrejme prvé využitie tohto výrazu v kontexte, v akom ho poznáme dnes, sa pripisuje katolíckej cirkvi začiatkom 17. storočia. S tým ako šírila cirkev svoju vieru do krajín Nového sveta a vyhradzovala sa proti protestantizmu, stratilo slovo propaganda svoj neutrálny význam[5].V roku 1622, pod záštitou pápeža Gregora XV., založila cirkev kongregáciu zameranú na šírenie viery s názvom „Congregatio de Propaganda Fide“. Postupom času sa tento výraz začal používať aj mimo náboženských kruhov, no svoje značne pejoratívne podfarbenie, ktoré si drží dodnes, získal až v polovici 19. storočia, keď sa začal používať hlavne v spojení s politikou[6]. Pre mnohých rimo-katolíkov preto pojem propaganda môže mať, aspoň v misionárskej alebo cirkevnej rovine, vysoký úctyhodný význam. Ale aj týmto osobám a určite mnohým ostatným sa tento pojem často spája s niečím negatívnym, ktoré má tendenciu naznačovať také veci, ako sú zdiskreditované príbehy o zverstve a klamne vyhlásené vojnové ciele svetových vojen, operácie nacistického Nemecka a propagandy a klamlivé sľuby tisíce politikov. Tiež pripomína nespočetné množstvo falošných a zavádzajúcich reklám (najmä v krajinách používajúcich latinský jazyk, v ktorých „propagande commerciale“ alebo nejaký ekvivalent je spoločným výrazom pre komerčnú reklamu).

„Propaganda je úmyselná, systematická snaha formovať vnímanie, manipulovať poznávanie a riadiť správanie za účelom dosiahnutia odozvy zodpovedajúcej požadovanému zámeru propagandistu.“[7] Propaganda predstavuje prácu veľkých organizácií alebo skupín s cieľom získať verejnosť pre svoje špecifické záujmy za masívneho použitia príťažlivých argumentov zabalených tak, aby skryli ako svoj presvedčovací zámer, tak nedostatok dôkazov[8]. Propaganda, aby bola efektívna, musí byť videná, zapamätaná, chápaná. Aby taká bola, musí byť prispôsobovaná konkrétnym potrebám situácie a publiku, na ktoré je cielená[9].

Z vyššie uvedeného možno vyvodiť, že propaganda je forma komunikácie, ktorá sa snaží ovplyvniť myslenie či správanie adresáta tak, aby vyhovovalo skrytým zámerom propagandistu. Za týmto účelom využíva propagandista rôzne priame či nepriame komunikačné prostriedky, ktoré prispôsobuje svojim zámerom. Pri propagande dochádza k zámernému skresleniu faktov, či využitiu poloprávd a klamstiev s cieľom manipulovať s myslením a/alebo správaním recipienta. Propagandistom zmenená, či celkom vytvorená realita je však vždy predkladaná ako pravdivá, adresát nemá vedieť, že je manipulovaný. Z uvedeného dôvodu je na propagandu nazerané ako na niečo negatívne.

Formy šírenia propagandy a fake news

V spoločnosti pretrváva dojem, že fake news a propagandu využívajú len štáty, ktoré sú neliberálne, nedemokratické. Tieto nemorálne nástroje by predsa nemohol využívať štát, ktorý dodržiava ľudské práva a pýši sa demokratickým zriadením?! Z uvedeného dôvodu ako prvý dezinformátorský štát napadne Ruská federácia. Na tomto mieste musíme zmieniť hlavnú operáciu INFEKTION, pri ktorej ruská KGB rozšírila klamlivú informáciu, podľa ktorej americké ministerstvo obrany vyvinulo vírus HIV ako smrteľnú biologickú zbraň. Predmetná

[5] JOWETT, G., S., O´DONNELL, V. *Propaganda and* Persuasion, Thousands Oaks. 2006. s. 2.
[6] DIGGS-BROWN, B. *Strategic Public Relations: Audience Focused Practice*. 2011. s. 48.
[7] JOWETT, G., S., O´DONNELL, V. *Propaganda and Persuasion, Thousands Oaks*. 2006. s. 21.
[8] SPROULE, J., M. *Propaganda and Democracy: The American Experience of Media and Mass Persuasion* (Cambridge Studies in the History of Mass Communication). 1996. s. 34.
[9] QUALTER, T., H. *Opinion Control in the Democracies*. 1985. s. 217.

kampaň bola tak účinná, že v roku 1991, krátko po rozšírení tejto fámy, jej verilo 15 % Američanov[10].

Poňatie autoritárskych štátov ako jediných, ktoré využívajú fake news, však nie je úplne zhodné so skutočnosťou. Aj napriek tomu, že Rusko je šampiónom medzi dezinformátormi a Čína mu šľape na päty, demokracia a právny štát nie sú zárukou úplne čistej hry. Počas druhej svetovej vojny napríklad fake news využili Spojenci k tomu, aby zmiatli nepriateľa. Nacisti si mali myslieť, že vylodenie na francúzskom pobreží prebehne v Pas de Calais, zatiaľ čo skutočný útok bol vykonaný na plážach Normandie[11].

Je dôležité uviesť, akými spôsobmi sa fake news vôbec dostávajú k ľuďom. Zlatý vek fake news nastal s masovosťou médií. Šíriť klamlivé správy išlo do tej doby veľmi ťažko, keď boli jej príjemcovia roztrúsení po celej krajine a navyše boli negramotní, okrem toho bol tento proces zdĺhavý, pretože sa knihy prepisovali ručne. Neskôr došlo k mnohým vynálezom, ktoré distribúciu dezinformácií podstatne uľahčili, medzi nimi napríklad kníhtlač Johanna Gutenberga z roku 1440, v 19. storočí potom rádio, film a fotografie, ku ktorým sa nakoniec pridali počítače a internet.

Rozširovať fake news nie je ľahké, pokiaľ je realizované skrz tzv. tradičné médiá, televízia, noviny, rádio. Väčšina týchto médií sa fake news vyhýba, osoby, ktoré v nich pracujú, majú určité vzdelanie či prax, ktorá im bráni v publikovaní správ, ktoré nie sú overiteľné. Tieto média tiež potrebujú čitateľov, poslucháčov a divákov, ktorí ich obsah budú sledovať a odoberať, aby mali z čoho platiť svoju činnosť, a to je ťažšie (nie však nemožné), pokiaľ rozširujú falošné informácie.

Pre súčasnú dobu je charakteristické, že pokiaľ sa povie „fake news“ alebo „dezinformácia“, väčšina ľudí si okamžite vybaví dezinformačné weby. Na internete ľudia už tak zdomácneli, že denne sa pýtajú vyhľadávača Google na 3 bilióny otázok a každú minútu pošlú 200 miliónov emailov[12].

V televízii a rádiu sa tradične fake news nevyskytujú, v tlači sa objavujú prevažne ako bulvárne správy, ktoré sú snáď nebezpečné len pre zdravý rozum, ale nie pre demokraciu. Dôležitou osobou v tradičných médiách je tzv. gatekeeper alebo inak povedané editor. Ten vyberá správy, ktoré sa dostanú k verejnosti, a ktoré budú zapamätané. Úplne iné je to ale v kyberpriestore, ktorý nemá žiadneho gatekeepera, ktorý by obsah cenzúroval. Kontrolu obsahu vystaveného v kyberpriestore vykonáva až polícia. Kyberpriestor nemá centrálneho vlastníka ani nie je ukotvený v jedinej krajine. Ide o médium nemajúce hranice a nepodliehajúce prísnej regulácii[13], akej sú podrobené klasické média. Možnosť založiť internetovú stránku má v podstate každý. Na nej potom môže publikovať čokoľvek chce, a to v podstate bez obmedzenia.

Pre kyberpriestor sú špecifickým fenoménom takzvané hoaxy (pozn. autorov, rozširovanie reťazových správ). Ide teda o poplašné správy, ktoré sú rozosielané prostredníctvom komunikačných vírov alebo inými nebezpečenstvami, vždy ale obsahujú urgentnú výzvu k preposlaniu ďalšej obeti[14]. Od fake news sa líšia tým, že ich cieľom väčšinou nie je primárne manipulovať ľudí, ale skôr príjemcu oklamať alebo od neho vylákať peniaze.

---

[10] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 14.

[11] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 12.

[12] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 44.

[13] BOHÁČKOVÁ, G. *Kvalita a objektivita informací v médiích: pravda versus manipulace a dezinformace*. 2006. s. 11.

[14] ZADRAŽILOVÁ, I. *Informace a dezinformace z hlediska jejich dopadu na společnosti*. 2007. s. 51.

Tvorcom hoaxu nie je vláda štátu alebo jeho zástupca ako u fake news[15], ale skôr jedinec konajúci na vlastnú päsť pre osobný prospech.

Pre šírenie fake news v kyberpriestore je snáď najdôležitejším pojmom dezinformačný web. Taký web môžeme poznať podľa niekoľkých kritérií, a to štruktúra, presnosť, objektivita, aktuálnosť a pokrytie.

Pokiaľ je pravý autor textu neznámy, informácie neobsahujú fakty, ale skladajú sa z nepravdivých a nepresných dát, nie sú pravdivé a majú za cieľ oklamať čitateľa, dáta o zdroji informácie a o čase a mieste chýbajú a web sa nedá kontaktovať, ide pravdepodobne o dezinformačný web[16]. Tieto požiadavky samozrejme nemusia byť vždy splnené všetky, ide len o pomôcku, ktorá nemôže byť celkom presná vo všetkých prípadoch.

Dezinformačných webov je mnoho a každú chvíľu sa objaví nejaký nový. Ich zoznam bol vytvorený napríklad investigatívnym denníkom think-tankom Európske hodnoty. Jedinec zvyknutý prijímať správy zo zavedených, vierohodných zdrojov nad týmito stránkami vrtí hlavou a domnieva sa, že ide o zveličovanie situácie, keď sa hovorí o hrozbe týchto „médií".

Spôsob preberania fake news a propagandy v kyberpriestore

Fake news samé o sebe, teda nepravdivé informácie vyslané medzi verejnosť, by v ideálnom prípade nemali veľký význam. Jedinec by na nich narazil, podľa úrovne mediálnej gramotnosti by im uveril, alebo si ich overil a zamietol ich ako nezmysel. Tým by cesta fake news skončila. Dezinformátor ale stavia na to, že klamlivá informácia bude dostatočne zaujímavá a uveriteľná, aby z pochybných médií prenikla na stránky zavedené a mainstreamové[17]. Pokiaľ správa pochádza z dôveryhodného a vyskúšaného zdroja, často o nej nebude pochybovať ani človek, ktorý by si rovnakú správu pochádzajúcu z iného média preveril.

Problémom je tiež uponáhľaná moderná doba. Čitateľ si v lepšom prípade nájde čas na prečítanie správ, ktoré očami prelietne a zapamätá si len nadpisy, v horšom prípade preberá správy od známych. Keďže overovanie informácií (alebo fact-checking) je časovo náročná aktivita, mnoho čitateľov sa uspokojí s prijatím informácie za svoju bez toho, aby o nej pochybovali.

Najčastejším spôsobom preberania fake news v kyberpriestore je prostredníctvom sociálnych sietí. Tie je v smršti nadpisov náročné rozpoznať, obzvlášť pokiaľ ich zdiela niekto človeku blízky. Mozog človeka na také množstvo informácií nie je zvyknutý ani stavaný. Svoju prácu spracovania vnemov si teda zjednoduší pomocou skratiek a hesiel tak, že keď sa jedinec stretne so známou, už skôr zhodnotenou situáciou, automaticky uspôsobí svoje konanie predchádzajúcej skúsenosti[18]. A keďže sa človek najskôr rozhodne podľa emócií, a až potom logicky, emotívne zafarbené a šokujúce dezinformačné správy sú pre neho automaticky viac atraktívne. Navyše kritické myslenie vyžaduje veľkú námahu oproti dôvere, ktorá je automatická. Ľudské podvedomie teda logicky preferuje cestu najmenšieho odporu[19]. Tieto fakty teda spôsobia, že pokiaľ jedinec nevyvinie vedomú snahu byť k novej informácii skeptický, sám od seba jej uverí a až bude neskôr konfrontovaný s rovnakou situáciou, bude očakávať rovnaký výsledok ako v prvom prípade. Kvôli tejto skutočnosti je teda tak ťažké

[15] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 46.

[16] TUDJMAN, M., MIKELIC, N. *Information Science: Science about Information, Misinformation and Disinformation.* 2003.

[17] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 46.

[18] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 78.

[19] GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 2018. s. 80.

zmeniť názor na oblasť, ku ktorej má už človek zaujatý pevný postoj. Následne sa ľudia vo svojich sociálnych bublinách utvrdzujú vo svojich názoroch zdieľaním ďalších správ podporujúcich danú ideu, navyše tomuto efektu nepomáhajú ani samotné sociálne siete. Na Facebooku či Youtube napríklad funguje algoritmus, ktorý na základe toho, čo ľudia sledujú a čo sa im páči, navrhujú rovnaký či obdobný obsah.

Je zrejmé, že propagandisti 20. storočia využívali multiplikačné prostriedky na doručovanie svojich správ pomocou reklamy a iných techník na sprostredkovanie zamýšľaného posolstva[20]. Všetky tieto metódy boli asynchrónne dodané. Technologický pokrok 21. storočia v oblasti komunikácie, počítačov, sietí, inteligentných telefónov, internetu poskytuje širšiu oblasť a sýtosť v arzenáli propagandistov. Úloha sociálnych médií v šírení Arabskej jari (pozn. autorov, séria protivládnych protestov, povstaní a ozbrojených povstaní, ktoré sa koncom roka 2010 rozšírili po celom Blízkom východe) viedla k novému dôveryhodnému zdroju správ pre používateľov. Vzostup sociálnych médií spôsobil, že táto nová oblasť je užívateľsky prívetivejšia, avšak pre mnohých užívateľov aj najdôveryhodnejšia.

V 21. storočí sa funkciou používania internetu stala schopnosť rýchlo šíriť klamlivé údaje, a to asynchrónne aj synchrónne. Počiatočné šírenie informácií vo veľkej miere spočívalo v technike a finančnom zabezpečení na vytvorenie východiskového bodu. Ako náhle sa stanovil východiskový bod, šírenie informácií v kyberpriestore dosiahlo ciele priamo, prostredníctvom dôveryhodných kanálov sociálnych médií, a ich previazanosťou. Okrem toho, načasovanie uvoľnenia klamlivých informácií využilo neschopnosť rýchlo rozpoznať pravdu, čo umožnilo nekontrolované šírenie klamstiev. Toto strategické načasovanie zverejnenia klamlivých informácií je tiež známe ako „weaponized information“[21] (pozn. autorov „informačné zbrojenie“). Ide teda o načasované hromadné šírenie informácii, ktoré dávajú zdroju väčšiu kontrolu nad šírením ako v minulosti. Táto synchrónna zložka sa spolieha na zmes „true believers“ (v preklade „verní veriaci“), v zahraničnej odbornej literatúre tiež označovaní ako „useful idiots” (v preklade „užitoční idioti“), ktorí pôsobia ako trollovia, platení trollovia a umelí spravodajcovia ovládaní umelou inteligenciou.

Nová oblasť propagandy neustále rastie a množstvo informácií dostupných v tomto novom kyberprostredí je bohaté. Nová technológia využívajúca techniky informačnej vedy umožňuje presnejšiu identifikáciu cieľa a nepretržité bombardovanie špeciálnych vytvorených správ z dôveryhodných alebo kvázidôveryhodných zdrojov. Objem týchto správ, ktoré posilňujú hodnoty, môže účinne zmeniť vnímanie cieľa. Keď sa cieľový používateľ snaží overiť obsah správ, vráti sa veľký počet podobných správ a cieľ teraz vie, že iní ľudia zdieľajú rovnaké hodnoty a presvedčenia.

Výskyt správ s falošnými príbehmi je problematický z dôvodu, že ak sa čitateľ pokúsi nájsť príbeh, vráti sa mu veľký počet rovnakých príbehov, čím sa čitateľovi potvrdzuje falošný príbeh. Kontrolné miesta si vyžadujú čas na výskum a na zaslanie zistenia detekovania falošných informácií, a keď zdrojom falošných správ je priateľ alebo iná blízka osoba, zaujatosť je na scéne. Čitatelia, ktorí nie sú schopní určiť pravdivosť správy, často nemajú dostatok času a zdrojov na určenie dôveryhodnosti zdroja, a preto sa spoliehajú na mentálne skratky, ako sú predsudky[22] a povesť zdroja, čo determinuje jeho dôveryhodnosť[23].

Spoliehanie sa na reputáciu využíva dva spôsoby. Prvým je používanie populárnych sociálnych médií - aplikácií, kde sa prostredníctvom zacielenia skupín znásobujú dôveryhodné položky, stanú sa prístupovými bodmi väčšej spoločnosti. Je dôležité myslieť na to, že

[20] JOWETT, G., S., O'DONNELL, V. *Propaganda and Persuasion*, 5th Edition. 2011. s. 34 – 36.

[21] DARRAJ, E., SAMPLE, C., COWLEY, J. *Information Operations: The use of weaponized information in the 2016 US presidential election*, 2017. s. 113.

[22] TANIS, M., POSTMES, T. *A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour*. 2005. s. 413.

[23] CHO, J., H., CHAN, K., ADALI, S. *A survey on trust modeling*, 2015.

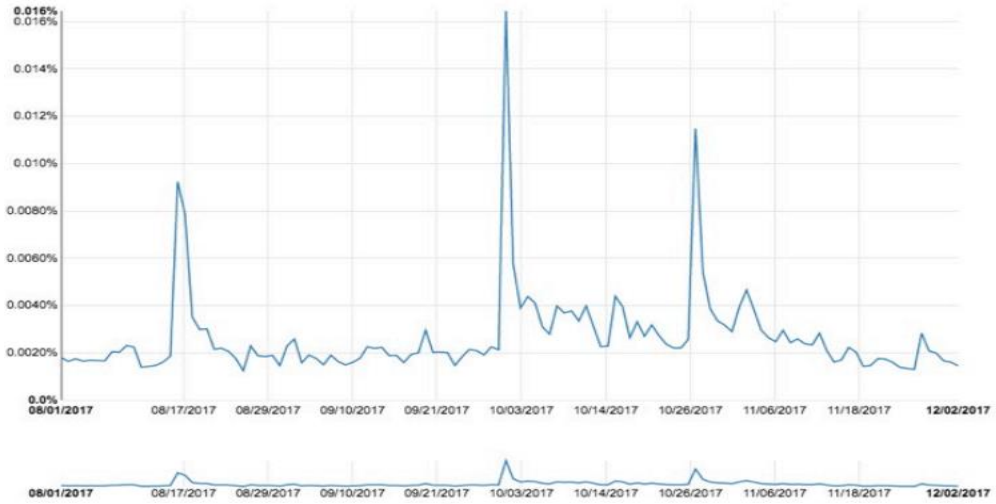
pôvodným poslaním sociálnych médií je združovať podobne zmýšľajúcich ľudí a informácie v duchu priateľstva. Priateľstva týchto skupín ľudí však poskytli aj kanál na distribúciu fake news, pretože tieto stránky tiež propagujú tlačové správy. Tie isté stránky, napríklad ako Twitter, sa stali dôveryhodnými zdrojmi správ zohrávajúc dôležitú úlohu pri Arabskej jari[24].

Vybrané aktivity na ochranu kyberpriestoru pred fake news a propagandou

Viesť boj proti klamstvu, obzvlášť potom takému, ktoré financujú ľudia s hlbokými kapsami vo vysokých verejných funkciách, je neľahké, ale tým viac potrebné. Každý jednotlivý človek môže s fake news bojovať, pokiaľ bude používať kritické myslenie.

Výskum v oblasti výpočtovej lingvistiky ukázal, že správy môžu byť presne rozdelené na pravdu, nepravdy a satiru, prostredníctvom analýzy jazykových prvkov[25]. Súbor nástrojov na overenie dôveryhodnosti[26] poskytuje možnosť hodnotiť články novín pozdĺž osi spoľahlivosti a objektivity, ako aj potenciálne spoločenstvá sociálnych médií, ktoré by mohli mať záujem o obsah článku, spolu s vizualizačnými nástrojmi na pomoc pri interpretácii. Teda výpočtová lingvistika môže ponúknuť prostriedky na vykonanie predbežného označovania spravodajského článku, na rýchle vyhodnotenie pravdivosti tohto článku. Okrem výpočtovej lingvistiky môže analýza reputácie a šírenia ponúkať aj platný prehľad, ktorý pomáha pri hodnotení pravdivosti nového príbehu.

Počiatočná reakcia na fake news sa opierala o kontrolu faktov prostredníctvom zdroja, ako sú napríklad Snopes[27], PolitiFact[28] alebo iné miesta kontroly faktov. Táto metóda fungovala dobre niekoľko rokov, ale je časovo náročná a ľahko ohromená objemom príbehov fake news, ktoré sa vytvárajú v priebehu kampane. Obrázok 1 poskytuje príklad hashtag značky spojenej s naratívom založeným na faktoch a obrázok 2 ilustruje hashtag súvisiaci s falošným príbehom, ktorý je prekrytý faktickým príbehom[29]. Obrázok 2 ukazuje rozprávanie založené na faktoch, ktoré je ľahko zaplavené falošným príbehom.

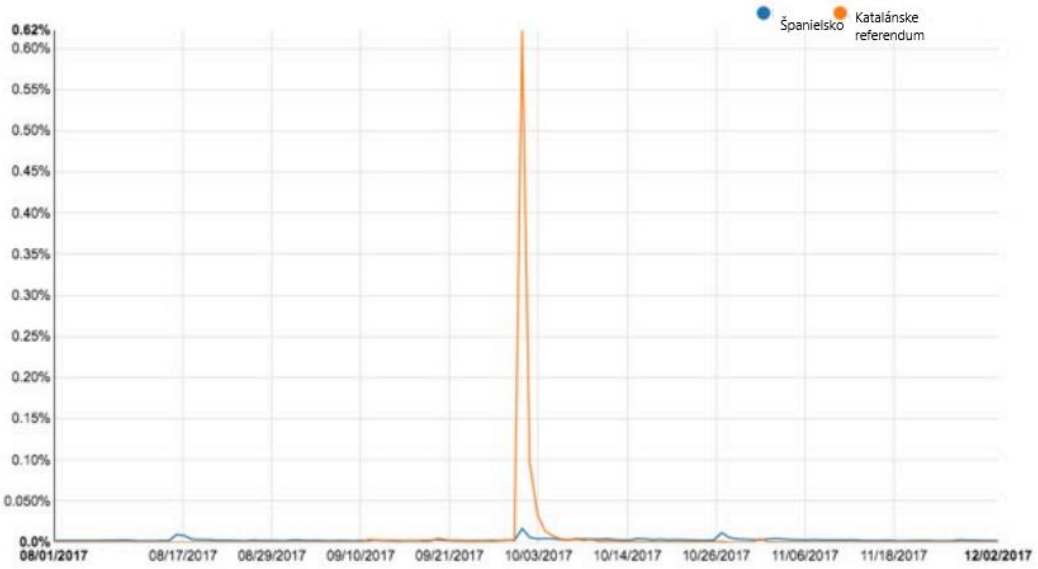


Obr. 1: Hashtag spojený s naratívom založeným na faktoch
Zdroj: SAMPLE, CH. – JUSTICE, C. – DARRAJ, E. A Model for Evaluating Fake News. Washington DC, 2017, p. 4

[24] PARENT, O., ZOUACHE, A. *Role of peer effects in social protest. Evidence from the Arab spring.* 2017.
[25] HORNE, B., ADALI, S. *This Just In: Fake News Packs a Lot in Title, Uses Simpler, Repetitive Content in Text Body*, More Similar to Satire than Real News. 2017.
[26] Nelatoolkit. [online]. [cit. 14. 6. 2019]. Dostupné na:<http://nelatoolkit.com>
[27] Snopes. [online]. [cit. 14. 6. 2019]. Dostupné na:<https://www.snopes.com>
[28] Politifact. [online]. [cit. 14. 6. 2019]. Dostupné na:<https://www.politifact.com>
[29] BADAWY, A., FERRARA, E., LERMAN, K. *Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign*, 2018. s. 258-265.

Obrázok 1 ilustruje aktivity v Španielsku v období od 1. augusta 2017 do 1. decembra 2017 v porovnaní so skutočným hlasovaním, ktoré sa uskutočnilo 1. októbra 2017[30].

Zvislá čiara na obrázku 2 ukazuje rýchlu a intenzívnu dávku hashtagu katalánskeho referenda, ktorá súvisí s falošným rozprávaním v rovnakom časovom okne ako v prípade Španielska. Je dôležité si všimnúť nielen vysokú odozvu, ale aj veľmi krátku časovú líniu za falošným príbehom[31]. Zavedením konkrétnej tváre do príbehu tesne pred konaním volieb (podobne ako Clintonove e-maily[32] a Macronove e-maily[33], má cieľ len veľmi málo času na reagovanie. Informácie v tomto bode sú teda informačným zbrojením a aktívne.



Obr. 2: Falošný hashtag prekrytý hashtagom založeným na faktoch
Zdroj: SAMPLE, CH. – JUSTICE, C. – DARRAJ, E. A Model for Evaluating Fake News. Washington DC, 2017, p. 4

Podľa Európskej komisie by mal byť boj proti dezinformáciám vedený pomocou nasledujúcich princípov[34]:

- Usilovať sa o zlepšenie transparentnosti prostredia, v ktorom informácie vznikajú a šíria sa;
- Usilovať sa o podporu rôznorodej ponuky informácií;
- Posilniť vierohodnosť správ uvádzaním údajov o ich spoľahlivosti;
- Presadzovať inkluzívne riešenia;

Hlavným problémom boja proti fake news z pohľadu ústavného práva je riziko zásahu do slobody prejavu. Aj napriek tomu je sloboda prejavu jedným zo základných pilierov štátu, aj ona má svoje medze, nie každé obmedzenie tejto slobody je teda nezákonné. Prevažná časť fake news hrozbu vnútornej bezpečnosti a demokratického zriadenia štátu nepredstavuje, tieto sú slobodou prejavu bez debát chránené. V boji proti fake news sú však z pohľadu štátu problematické fake news, ktoré majú negatívny dopad na vnútornú bezpečnosť štátu. Pokiaľ majú teda dezinformácie legálny obsah, vzťahuje sa na ne sloboda prejavu, aj pokiaľ je hanlivý, škodlivý či urážlivý. Rozdielne je potom potrebné zaobchádzať s obsahom nezákonným, pri takom prejavu štát slobodu prejavu nechráni absolútne.

[30] HAYWARD, P. A. *Factoids, Dishonesty and Propaganda in the Middle Ages*, 2018.
[31] IUNI. [online]. [cit. 14. 6. 2019]. Dostupné na:<https://osome.iuni.iu.edu/tools/trends/#>
[32] FARIS, R., ROBERTS, H., ETLING, B., BOURASSA, N., ZUCKERMAN, E., BENKLER, Y. *Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election.* 2017.
[33] BURGESS. M. *The Emmanuel Macron email hack warns us fake news is an ever-evolvong beast.*
[34] OZNÁMENIE EÚ KOMISIE COM (2018) 236.

Opatrenia proti fake news logicky vzbudzujú obavu z cenzúry, akéhosi Orwellovského štátu. Je totiž veľmi zložité rozlíšiť dezinformáciu od misinformácie a určiť, kde je hranica, za ktorú je už potrebné fake news odstraňovať, to všetko v obrovskom množstve obsahu, ktorý je v kyberpriestore nahraný každú minútu, takže dochádza k chybám.

Také aktivity tiež nemôže vykonávať jedna osoba, ale aby bola iniciatíva úspešná, musí ísť o koordinovanú snahu väčšieho počtu ľudí. Pre boj proti fake news sú ideálne súkromné občianske iniciatívy, pretože tie môžu kritizovať a poukazovať na fake news, nikto ich ale nemôže obviniť zo zneužitia moci ako verejnú osobu. Pokiaľ proti fake news brojí verejná osoba alebo dokonca štátny orgán, je pochopiteľné, že sa bude musieť mať viac na pozore než osoba súkromná, keďže bude okamžite podozieraná z cenzúry a snahy potlačiť „pravdu". Obmedzenie, ktoré sa zo začiatku prezentuje ako ochrana ľudských práv, sa totiž môže ukázať ako potlačenie slobody prejavu, ako príklad môžeme uviesť Egypt. Tu režim nariadil zrušenie 21 spravodajských webov kvôli obvineniu z rozširovania fake news, jedným z nich boli noviny MadaMisr, nezávislý denník, ktorý podporoval opozičné sily[35].

Je dôležité uznať, že boj proti fake news obmedzuje slobodu prejavu dezinformátorov. Súčasťou slobody prejavu je ale uznanie slobody a plurality všetkých médií a právo všetkých jednotlivcov „*zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania verejnej moci a bez ohľadu na hranice*."[36] Fake news manipuláciou s verejnou mienkou toto právo narúšajú a tým sami obmedzujú slobodu prejavu. Z tohto pohľadu teda boj proti fake news zaručuje slobody všetkých ostatných.

Nielen štáty, ale aj medzinárodné organizácie si uvedomujú hrozbu, ktorú predstavujú fake news v kyberpriestore. Už v roku 2015 boli Európskou radou prijaté závery, v ktorých sa zmieňuje, že je naďalej nevyhnutné čeliť dezinformačným kampaniam Ruskej federácie a vyzýva vysokých predstaviteľov, aby bol pripravený akčný plán pre strategickú komunikáciu. V nadväznosti na to, bola zriadená pracovná skupina East StratCom, ktorá má za cieľ posilňovať mediálne prostredie vo východnom susedstve (Arménsko, Ázerbájdžán, Gruzínsko, Bielorusko, Moldavsko, Ukrajina), vyvíjať produkty a kampane pre tieto krajiny, ktoré lepšie vysvetlia únijné postupy, a analyzovať dezinformačné trendy a zvyšovať povedomie o dezinformaciách prichádzajúcich z ruského územia.

Pred voľbami do Európskeho parlamentu v roku 2019 a všeobecne k ochrane demokracie v členských štátoch prijala Európska rada v máji 2018 závery ohľadom migrácie, inovácie či práve bezpečnosti. Tu vyzýva Európsku komisiu a vysokú predstaviteľku, aby do novembra 2018 v spolupráci s členskými štátmi predstavili akčný plán, ktorý bude obsahovať presný spoločný postup proti dezinformáciám.

Akčný plán bol vydaný Komisiou v novembri v roku 2018. Komisia sa v ňom zameriava na štyri hlavné oblasti[37]:

ide o účinnejšie odhaľovanie hybridných hrozieb, ktorý chce docieliť posilnením zamestnancov v orgánoch zaoberajúcich sa strategickou komunikáciou

cieľom je dosiahnuť koordinované reakcie, k čomu by mal vzniknúť systém včasného varovania na šíriace sa dezinformácie medzi orgánmi EÚ a členskými štáty a to v reálnom čase;

zvýšiť povedomie občanov o klamlivých správach a podporovať mediálnu gramotnosť pomocou osobitných programov a nezávislých overovateľov faktov;

sledovať dodržiavanie kódexu zásad prijatého online platformami ako je Google, Facebook, Twitter či Mozilla. Tento kódex vymenúva oblasti, na ktoré by sa títo internetoví giganti mali zamerať, a zmieňuje ciele, ktoré sa zaviazali plniť, teda prijať pravidlá a procesy, ktoré okrem iného nedovolia dezinformátorom ťažiť z reklám, obmedzia používanie

[35] VILMER, J., B., J., ESCORCIA, A., GUILLAME, M., HERRERA, J. *Information Manipulation - A Challenge for Our Democracies*. 2018. s. 191.
[36] OZNÁMENIE EÚ KOMISIE COM (2018) 236.
[37] EURÓPSKA KOMISIA. Európa, ktorá chráni. 2018.

automatizovaných botov, zaručia transparentnosť politickej reklamy a pomôžu užívateľom rozoznať a overovať dezinformácie[38].

Za zmienku tiež stojí extenzívna správa dvoch francúzskych thinktankov, Strediska analýz, prognóz a stratégií Ministerstva zahraničných vecí (CAPS) a Inštitútu strategického výskumu pri vojenskej škole (IRSEM) zo 4. septembra 2018. Tvorcovia vykonali stovky rozhovorov v dvadsiatich krajinách, aby kompaktne obsiahli danú tému. Dokument s názvom „Manipulácia s informáciami: výzva pre naše demokracie" sa zaoberá otázkami prečo a ako fake news fungujú, zhŕňa už existujúce opatrenia, ktoré boli zavedené po celom svete, a navrhuje spôsoby ako sa vyrovnať s rizikom manipulácií s informáciami do budúcna. Správa predstiera, že najväčšia hrozba príde od štátov, ktoré budú schopné skĺbiť sociálnu psychológiu, big dáta a umelú inteligenciu. Na koniec dokumentu odborníci zaradili 50 odporúčaní pre vlády, občiansku spoločnosť, súkromných aktérov a všeobecne pre všetkých. Pre predstavu uvádzame napríklad radu nepodľahnúť pokušeniu „protipropagandy", neprenechať internet extrémistom či nepodceňovať hrozbu fake news[39].

Existuje celý rad zahraničných občianskych projektov, ktoré sa zaoberajú vyhľadávaním a odhaľovaním fake news a hoaxov.

PolitiFact je nezávislý americký portál, ktorý má za cieľ transparentné a spravodlivé overovanie výrokov domácich politikov. Zmyslom tohto projektu je ponúknuť ľuďom informácie, ktoré potrebujú, aby sa mohli pohybovať v demokratickom prostredí a kontrolovať svojich zástupcov[40]. Projekt dokonca v roku 2009 vyhral Pulitzerovú cenu v kategórii lokálne spravodajstvo za spravodajstvo o prezidentských voľbách v roku 2008[41]. Na podobnom princípe potom funguje web FactCheck.org.

Ďalšou iniciatívou v boji proti fake news je projekt Polygraph.info. Stránka vznikla pod taktovkou známeho rádia Slobodná Európa/ Sloboda (RFE/RL) a multimediálnej stanice Hlas Ameriky (Voice of America), odhaľuje a uvádza na pravú mieru dezinformácie z celého sveta. Novinári analyzujú prejavy, správy a dokumenty, a to hlavne pre ľudí z krajín s obmedzenou slobodou tlače.

Elfovia je skupina občanov, ktorá sa snaží bojovať s dezinformačnými kampaňami a prokremeľskou propagandou, ktorá číha hneď za hranicami. Projekt začal s približne dvoma desiatkami Litovcov najrôznejších povolaní, ktorí mali záujem vyvracať nekončiace falošné správy o ich krajine, NATO, EÚ a USA. Teraz ich počet stúpol na stovky a svojich zástupcov majú elfovia v Estónsku, Lotyšsku aj Fínsku. Ich boj sa odohráva na Facebooku a pod článkami online denníkov, kde sa snažia vyvracať fake news a zistiť identitu trollov, šíriteľov fake news. Práve pre povahu svojich aktivít držia svoju totožnosť v utajení zo strachu pred pomstou ruských dezinformátorov[42].

V neposlednom rade je nutné spomenúť, že na rozkrývanie dezinformačných kampaní pracuje mnoho novinárov. Medzi nimi napríklad známa fínska investigatívna reportérka Jessikka Aro, ktorá je považovaná za expertku na ruských trollov. Pri svojom pátraní po ruských farmách trollov odhalila, že prokremeľská štátom schválená propaganda sa šíri po Twitteri pomocou automatizovaných účtov a botov. Krátko potom sa na novinárku zamerali trollovia, ktorí o nej začali šíriť falošné informácie a odhalili jej osobné údaje na internete. Tá sa sama nechala počuť, že silou útoku na jej osobu trollovia len potvrdili to, že odkryla veľmi vážny problém[43].

---

[38] EURÓPSKA KOMISIA. EU code of practise on disinformation. 2018.

[39] VILMER, J., B., J., ESCORCIA, A., GUILLAME, M., HERRERA, J. *Information Manipulation - A Challenge for Our Democracies.* 2018. s. 167-169.

[40] DROBNIC, H., A. *The Principles of the Truth-O-Meter*, 2018. s. 36-37.

[41] ADAIR, B. *PolitiFact wins Pulitzer*. 2009. s. 26.

[42] WEISS, M. *The Baltic Elves Taking on Pro-Russian Trolls*. 2019. s. 29.

[43] YATES, W. - ARO, A. *How pro-Russian trolls tried to destroy me*. 2019. s. 19.

Záver

Propaganda je viac či menej systematické úsilie na manipuláciu názorov, postojov alebo činností iných ľudí prostredníctvom symbolov (slová, gestá, bannery, pamiatky, hudba, oblečenie, odznaky, účesy, návrhy na mince a poštové známky atď.). Závažnosť a pomerne veľký dôraz na manipuláciu rozlišujú propagandu od neformálnej konverzácie alebo slobodnej a ľahkej výmeny myšlienok. Propagandista má stanovený cieľ alebo súbor cieľov. Na dosiahnutie týchto cieľov zámerne vyberá fakty, argumenty a zobrazenie symbolov a prezentuje ich spôsobom, o ktorom je presvedčený, že bude mať najsilnejší účinok. Aby mohol maximalizovať účinok, môže vynechať relevantné skutočnosti alebo ich skresľovať a môže sa pokúsiť odviesť pozornosť reaktorov (ľudí, ktorých sa snaží hnať) od všetkého okrem vlastnej propagandy.

Vysoká účinnosť spolu so stratou nákladov robí z propagandy dobrú vojenskú zbraň. Schopnosť manipulovať dôveru prostredníctvom rôznych médií sa spolieha na chybný model dôvery, ktorý sa opiera na objektovo orientované konštrukty[44], čo má za následok stratu kontextu.

Otázka dôveryhodnosti zdroja je komplexná a dlhodobá, je historickým overovaním dôvery. Handshake bol jedným z prvých príkladov overovania dôveryhodnosti[45]. Overenie dôveryhodnosti virtuálneho prostredia je zložitejšie a predstavuje problém označovaný ako dôveryhodnosť údajov[46].

Staré modely môžu slúžiť ako inšpirácia pre dizajn nových modelov na hodnotenie fake news. Dôvera v subjekty bez overenia ich dôveryhodnosti, povedie k ich zneužívaniu a dôvera v informačné zdroje bude ďalej manipulovaná. Propagandisti starostlivo profilujú svoje ciele, hodnoty a presvedčenie ešte pred samotnou tvorbou správy v kyberpriestore.

Propaganda a fake news predstavujú dlhodobý problém, ich šírenie v kyberpriestore len posilňuje účinnosť tohto nástroja. Kyberbernetická bezpečnosť súčasnosti by mala smerovať k riešeniu vyššie zmienených problémov, akými jednoznačne propaganda a fake news sú. Návrh modelu bude určite trvať dlhší čas a vyžaduje si kontextové hodnotenie udalostí a naplnenie komplexných požiadaviek.

Zoznam použitej literatúry:

1. ADAIR, B. 2009. *PolitiFact wins Pulitzer. PolitiFact.* [online]. [cit. 14. 6. 2019]. Dostupné na:<https://www.politifact.com/truth-o-meter/ar-ticle/2009/apr/20/politifact-wins-pulitzer>
2. BADAWY, A. – FERRARA, E. – LERMAN, K. 2016. *Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign*. [online]. [cit. 14. 6. 2019]. Dostupné na:<https://arxiv.org/pdf/1802.04291.pdf.>
3. BOHÁČKOVÁ, G. 2006. *Kvalita a objektivita informací v médiích: pravda versus manipulace a dezinformace* [online]. [cit. 11. 6. 2019]. Dostupné na: <https://is.muni.cz/th/q1lha/diplomovaprace.pdf>
4. BURGESS, M. 2017. *The Emmanuel Macron email hack warns us fake news is an ever-evolvong beast.* [online]. [cit. 11. 6. 2019]. Dostupné na: <https://www.wired.co.uk/article/france-election-macron-email-hack>
5. DARRAJ, E., SAMPLE, C., COWLEY, J. *Information Operations: The use of weaponized information in the 2016 US presidential election*, Proceedings of fthe 16th European Conference on Cyber Warfare and Security, Dublin, Ireland, 2017. s. 113-119.

[44] NISBETT, R., E. *The Geography of Thought: How Asians and Westerners Think Differently ...* and Why. 2010. s. 127 – 129.

[45] CHO, J., H., ChAN, K., ADALI, S. *A survey on trust modelling*. 2015.

[46] SAMPLE, C., WATSON, T., HUTCHINSON, S., HALLAQ, B., COWLEY, J., MAPLE, C. *Data fidelity: Security's soft underbelly.* 2017. s. 317.

6. DIGGS-BROWN, B. *Strategic Public Relations: Audience Focused Practice*. Boston: Wadsworth, CENGAGE Learning. 2011. 520 s. ISBN 978-0534637064.
7. DROBNIC, H., A. *2018. The Principles of the Truth-O-Meter. PolitiFact's methodology for independent fact-checking.* [online]. [cit. 12. 6. 2019]. Dostupné na: <https://www.politifact.com/truth-o-me-ter/article/2018/feb/12/principles-truth-o-meter-politifacts-methodology-i/>
8. EGAN, L., T. 2018. *The fake news is creating violence - NBC News.* [online]. [cit. 12.6. 2019]. Dostupné na:<https://www.nbcnews.com/poli-tics/white-house/trump-fake-news-creating-violence-n930576>
9. EURÓPSKA KOMISIA. 2018. *EU Code of Practice on Disinformation*. [online]. [cit. 11. 6. 2019]. Dostupné na: <https://ec.europa.eu/newsroom/dae/docu-ment.cfm?doc_id=54454>
10. EURÓPSKA KOMISIA. 2018. Európa, ktorá chráni, 2018. EÚ posilňuje opatrenia proti dezinformáciám. [online]. [cit. 11. 6. 2019]. Dostupné na:<https://ec.eu-ropa.eu/czech-republic/news/181205_akcni_plan_proti_dezin-formacim_cs>
11. FARIS, R., ROBERTS, H., ETLING, B., BOURASSA, N., ZUCKERMAN, E., BENKLER, Y. 2017. *Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election.* [online]. [cit. 11. 6. 2019]. Dostupné na: <https://dash.harvard.edu/bitstream/handle/1/33759251/2017-08_electionReport_0.pdf>
12. GREGOR, M., VEJVODOVÁ, P. *Zvol si info. Nejlepší kniha o fake news, dezinformacích a manipulacích!!!* 1. vyd. Brno: CPress, 2018. 142 s. ISBN 978-80-264-1805-4.
13. HAYWARD, P. A. 2018. *Factoids, Dishonesty and Propaganda in the Middle Ages*. [online]. [cit. 11. 6. 2019]. Dostupné na:<https://www.ias.edu/ideas/2012/hayward-historical-texts>
14. HORNE, B., D., ADALI, S. *This Just In: Fake News Packs a Lot in Title, Uses Simpler, Repetitive Content in Text Body, More Similar to Satire than Real News.* Association for the Advancement of Artificial Intelligence. Published at The 2nd International Workshop on News and Public Opinion at ICWSM, 2017.
15. CHO, J., H., CAN, K., ADALI, S. 2015. *A survey on trust modeling, ACM Computing Surveys*. [online]. [cit. 11. 6. 2019]. Dostupné na:<http://dx.doi.org/10.1145/2815595.>
16. JOWETT, G., S., O´Donnell, V. *Propaganda and Persuasion, Thousands Oaks*. United States of America : Library of Congress Cataloging, 2006. 425 s. ISBN 978-1-4129-7782-1.
17. JOWETT, G., S., O'Donnell, V. *Propaganda and Persuasion, 5th Edition*. Thousand Oaks, CA: Sage Publications, Inc. 2011. 464 s. ISBN 978-1412977821.
18. KRKOŠKA, D. *České dezinformační weby a jejich obsah*. Praha: Univerzita Karlova, Fakulta sociálnych vied. Vedúci práce Filip LÁB , 2018. 59 s.
19. QUALTER, T., H. *Opinion Control in the Democracies*. London: Palgrave Macmillan UK, 1985. 317 s. ISBN 978-1-349-17775-2.
20. NISBETT, R., E. *The Geography of Thought: How Asians and Westerners Think Differently ... and Why*. UK : Free Press; Reprint edition, 2010. 288 s. ISBN 978-0743255356.
21. NELATOOLKIT. [online]. [cit. 14. 6. 2019]. Dostupné na:<www.nelatoolkit.com>
22. OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓSPKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV COM(2018) 236 zo dňa 26. 4. 2018 o boji proti dezinformáciám na internete: európsky prístup. In *EUR-Lex.* [právny informačný systém]. Úrad pre publikácie Európskej únie. [online]. [cit. 11. 6. 2019]. Dostupné na:<https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0236&from=en>

23. PARENT, O., ZOUACHE, A. 2017. *Role of peer effects in social protest. Evidence from the Arab spring*. [online]. [cit. 11. 6. 2019]. Dostupné na:<http://erf.org.eg/wp-content/uploads/2018/02/Olivier-Abdallah.pdf.>
24. POLITIFACT. *[online]. [cit. 14. 6. 2019]. Dostupné na:<www.politifact.com>*
25. SAMPLE, CH., JUSTICE, C., DARRAJ, E. 2019. *A Model for Evaluating Fake News.* [online]. [cit. 11. 6. 2019]. *Dostupné na:*<https://www.researchgate.net/publication/330854488_A_Model_for_Evaluating_Fake_News.>
26. SAMPLE, C., WATSON, T., HUTCHINSON, S., HALLAQ, B., COWLEY, J., MAPLE, C. *Data fidelity: Security's soft underbelly*. Proceedings of the 11th International Confereince on Research Challenges in Information Systems, United Kingdom: Brighton, 2017. s. 315 – 321.
27. SPROULE, J. M. *Propaganda and Democracy: The American Experience of Media and Mass Persuasion (Cambridge Studies in the History of Mass Communication).* Cambridge: Cambridge University Press, 1996. 344 s. ISBN 978-052-147022-3.
28. SNOPES. [online]. [cit. 14. 6. 2019]. Dostupné na:<www.snopes.com>
29. TANIS, M., POSTMES, T. *A social identity approach to trust: Interpersonal perception, group membership and trusting behaviour*, European Journal of Social Psychology, Vol. 35, no. 3, 2005. s. 413-424.
30. TUDJMAN, M., MIKELIC, N. 2003. *Information Science: Science about Information, Misinformation and Disinformation*. [online]. [cit. 11. 6. 2019]. Dostupné na: <http://proceedings.informingscience.org/IS2003Procee-dings/docs/204Tudjm.pdf>
31. YATES, W., ARO, A. 2019. *How pro-Russian trolls tried to destroy me*. BBC Trending. [online]. [cit. 12. 6. 2019].
32. VILMER, J., B., J., ESCORCIA, A., GUILLAME, M., HERRERA, J. 2018. *Information Manipulation - A Challenge for Our Democracies - France Diplomatie.* [online]. [cit. 11. 6. 2019]. Dostupné na:<https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf>
33. WEISS, M. 2016. *The Baltic Elves Taking on Pro-Russian Trolls*. *Daily Beast.* [online]. [cit. 13. 6. 2019]. Dostupné na:<https://www.the-dailybeast.com/the-baltic-elves-taking-on-pro-russian-trolls>

Kontaktné údaje:
plk. doc. Ing. Stanislav Šišulák, PhD.
prorektor pre informatizáciu a koordináciu s policajnou praxou
Akadémia PZ v Bratislave
stanislav.sisulak@minv.sk

kpt. JUDr. Martina Cíchová
Prezídium Policajného zboru
martina.cichova@minv.sk

Požiadavky na vzdelávanie používateľov informačných systémov v oblasti kybernetickej bezpečnosti

Viktor Šoltés, Anton Šiser

Abstrakt:
Informačné a komunikačné technológie výrazným spôsobom ovplyvnili všetky aspekty spoločenského života. V snahe vytvoriť podmienky pre kvalitnejšiu komunikáciu a jednoduchý prístup k informáciám sa čoraz väčšia časť bežných aktivít transformuje z fyzickej do kybernetickej úrovne. Okrem širokej škály výhod prináša tento proces aj radu rizík v oblasti kybernetickej bezpečnosti. Jednotliví používatelia informačných systémov musia preto mať špecifické vzdelanie v tejto oblasti. Príspevok sa zaoberá stanovením minimálnych znalostných požiadaviek na vzdelávanie jednotlivých používateľov informačných systémov pre potreby zvyšovania kybernetickej bezpečnosti organizácie.
Kľúčové slová:
Kybernetická bezpečnosť, vzdelávanie, informačný systém, požiadavky, informácia.

Abstract:
Information and communication technologies have significantly influenced all aspects of social life. In order to create conditions for better communication and easy access to information, an increasing proportion of common activities are transformed from physical to cyber level. In addition to a wide range of benefits, this process also brings cyber security risks. Individual users of information systems must therefore have a specific education in this area. The paper deals with the determination of minimum knowledge requirements for education of individual users of information systems for the needs of increasing the cyber security of the organization.
Key words:
Cyber security, education, information system, requirement, information.

Úvod

Pocit bezpečia je jedným z kľúčových aspektov rozvoja spoločnosti. V minulosti bola bezpečnosť podmienená neexistenciou hrozieb vojenského charakteru. Ústup vojenských konfliktov a ukončením studenej vojny sa spustil proces globalizácie, ktorý viedol k vzniku medzinárodných spoločenstiev. Transformácia štátov realizovaná za účelom ich obnovy a sociálno-ekonomického rozvoja so sebou priniesla nové bezpečnostné hrozby vo vnútri štátov. Bezpečnosť v tomto období už nie je ohrozená zvonka vo forme ozbrojených konfliktov ale vo vnútri štátov vo forme kriminality. S technickým a technologickým rozvojom, ktorý so sebou proces transformácie a globalizácie priniesol, vznikol nový druh kriminality, ktorým je kybernetická kriminalita.

Kybernetická kriminalita je na rozdiel od bežnej kriminality páchaná v kybernetickom priestore a najčastejšie môže mať podobu násilnej, majetkovej alebo ekonomickej kriminality. Kriminalita páchaná v kybernetickom priestore je na rozdiel od kriminality páchanej „klasickým“ spôsobom omnoho nebezpečnejšia. Toto nebezpečenstvo vyplýva z anonymity kybernetického priestoru, z čoho vyplýva náročnosť (niekedy až nemožnosť) odhalenia páchateľa a jeho potrestania. Páchatelia kybernetickej kriminality sú v mnohých prípadoch omnoho viac vzdelaní a zruční v práci v kybernetickom priestore a využívajú nedostatočné zručnosti obetí s prácou modernými technológiami. V prípade, ak sa obeťou kybernetickej kriminality stane bežná fyzická osoba, straty nemusia byť značne veľké. V prípade napadnutia informačných systémov veľkej organizácie alebo subjektu verejnej správy môžu byť straty enormné. Práve preto je nevyhnutné zaoberať sa problematikou vzdelávania používateľov informačných systémov v organizáciách. Navrhnutím minimálnych znalostných požiadaviek pre jednotlivé úrovne používateľov informačných systémov v organizáciách je možné predchádzať výskytu kybernetickej kriminality a stratám z nej plynúcim.

Kybernetická bezpečnosť na Slovensku

Problematika kybernetickej bezpečnosti sa na Slovensku začala riešiť v roku 2008, kedy bola uznesením vlády Slovenskej republiky schválená Národná stratégia pre informačnú bezpečnosť v Slovenskej republike. Jej schválením bol vytvorený základný rámec informačnej bezpečnosti na Slovensku. Následne bol v roku 2010 uznesením vlády Slovenskej republiky schválený Akčný plán k Národnej stratégii pre informačnú bezpečnosť v Slovenskej republike na roky 2009-2013.[1] Oba uvedené dokumenty boli aktualizované a v súčasnosti sú nahradené dvoma strategickými dokumentmi v oblasti kybernetickej bezpečnosti, ktorými sú Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.

Na základe pôvodných strategických dokumentov sa v roku 2010 spustil proces prípravy legislatívneho zámeru zákona o informačnej bezpečnosti. Návrh zákona o informačnej bezpečnosti, ktorý bol vypracovaný v roku 2014 však neprešiel legislatívnym procesom a bol zastavený. Namiesto neho sa začalo s prípravou zákona o kybernetickej bezpečnosti, ktorý bol Národnou radou Slovenskej republiky schválený v roku 2018.

Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. v znení neskorších predpisov okrem iného ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti a definuje základné pojmy. Kybernetickou bezpečnosťou sa podľa tohto zákona rozumie stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov. Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo má iný, zákonom stanovený negatívny následok.[2]

Vzdelávanie v oblasti kybernetickej bezpečnosti na Slovensku

Zo Správ o plnení úloh Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a úloh akčného plánu za roky 2008 až 2013 vyplýva, že v oblasti informačnej bezpečnosti sú dosahované pozitívne výsledky najmä v budovaní spôsobilostí, vo vzdelávaní, v prevencii a pripravenosti na zvládnutie bezpečnostných počítačových incidentov, v odstránení ich následkov a následnej obnove informačných systémov v rámci ústrednej štátnej správy. Odborná príprava špecialistov štátnej správy prebieha najmä v gescii Ministerstva financií Slovenskej republiky. Zvyšovanie povedomia a vzdelávania v oblasti kybernetickej, či informačnej bezpečnosti nie je všeobecne obsahovou súčasťou systému vzdelávania v Slovenskej republike (základné, stredné a vysoké školy), ani systému formovania spoločenského povedomia. Vzdelávanie nie je riešené na úrovni špecializovaných odborov, ale nanajvýš na úrovni špecializovaných predmetov v rámci vybraných vzdelávacích inštitúcií.[3]

Kvalita, efektívnosť a účinnosť plnenia opatrení a úloh v oblasti kybernetickej bezpečnosti významnou mierou závisia od úrovne spoločenského povedomia, vzdelanostnej úrovne spoločnosti, ako aj od spôsobilostí aktérov v tejto oblasti. Jednou z možností ako tento problém riešiť je aj podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti. Za tým účelom je potrebné šírenie osvety a zvyšovanie povedomia a zaviesť všeobecný vzdelávací systém (na úrovni základného a stredného stupňa vzdelania)

[1] HOCHMANN, J. 2016. *Kybernetická bezpečnosť a štát*. [online]. [cit. 2019-05-10]. Dostupné na: <http://ideme.net/wp-content/uploads/sites/2/2017/04/Hochmann_iDEME2016.pdf>

[2] Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. v znení neskorších predpisov.

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

a odborný vzdelávací systém (na úrovni stredného a vysokoškolského stupňa vzdelania a na úrovni špecialistov).[4]

Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR

V rámci Slovenska nie je informačná bezpečnosť ustanovená za samostatný vedný a študijný odbor, a z toho dôvodu nie je ani jasne stanovený obsah vzdelávania v tejto oblasti. Interdisciplinárny charakter kladie rôzne požiadavky na užívateľov digitálneho priestoru, medzi ktorých patria laici, manažéri, informatici (vývojári a prevádzkovatelia systémov) a IT špecialisti. Vo všeobecnosti je možné stanoviť 10 oblastí informačnej bezpečnosti, s ktorými sa užívatelia dostávajú do kontaktu. Pri zostavovaní obsahu školení používateľov digitálneho priestoru je potrebné pre každý typ užívateľa stanoviť úroveň poznania desiatich definovaných oblastí informačnej bezpečnosti. Ide o úroveň:

- A – znalosť základných pojmov
- B – znalosť procesov riešenia incidentov v oblasti informatickej bezpečnosti
- C – schopnosť posudzovať bezpečnostné požiadavky[5]

Tabuľka 1 uvádza postačujúcu úroveň znalostí informačnej bezpečnosti pre jednotlivých užívateľov.

Tabuľka 1: Postačujúcu úroveň znalostí informačnej bezpečnosti pre jednotlivých užívateľov

Užívateľ	Manažment IB	Architektúra a modely	Riadenie prístupu	Aplikačná bezpečnosť	Bezpečnosť prevádzky	Fyzická bezpečnosť	Kryptológia	Siete, internet a	Plánovanie kontinuity	Legislatíva a etika
Laici	A	-	A	A	A	-	A	A	A	A
Manažéri	B	A	A	A	B	A	A	A	A	B
Informatici (vývoj)	B	B	B	C	B	A	B	B	B	A
Informatici (prevádzka)	B	B	B	C	C	B	B	B	C	A
IT špecialisti	C	B	C	B	B	B	B	C	C	B

Zdroj: Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR.

Pre budovanie povedomia o informačnej bezpečnosti u laikov sú špecifikované všeobecné a špecifické okruhy znalostí. Na globálnej úrovni je možné sa zaoberať vzdelávaním len v oblasti bezpečnostného prostredia vo všeobecnosti. Špecifické vzdelávanie si musí laik zabezpečiť sám v závislosti od technológií, s ktorými prichádza do kontaktu. Vzdelávanie manažérov a riadiacich pracovníkov je možné zabezpečiť prostredníctvom odborných konferencií, materiálov, školení, kurzov ale aj prostredníctvom celoživotného vzdelávania. Vhodnou formou je aj organizovanie vzdelávania v organizácii prostredníctvom lektorov. Informatici môžu poznatky z získať v rámci samotných informatických alebo špecializovaných predmetov na vysokej škole. Rozširovanie vedomostí je možné individuálne, firemným vzdelávaním alebo celoživotným vzdelávaním. Úlohou štátu v tejto oblasti je špecifikovať obsahové požiadavky na jednotlivé informatické pracovné zaradenia zamestnancov vo verejnej správe a stanoviť vedomostný štandard. Vzdelávanie IT špecialistov je vo veľkej miere

[4] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.
[5] Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR.

pokrývané informatickým vzdelávaním, celoživotným vzdelávaním, absolvovaním certifikovaných kurzov a školení, individuálnym štúdiom, prípadne účasťou na odborných konferenciách a inými aktivitami.[6]

Znalostné štandardy pre oblasť informačnej bezpečnosti

Ministerstvo financií Slovenskej republiky je gestorom odbornej prípravy špecialistov štátnej správy v oblasti kybernetickej bezpečnosti. Na tento účel vypracúva štandardy základných znalostí, metodické materiály, analýzy dokumentov a súvisiacich vykonávacích predpisov a realizuje školenia pre oblasť informačnej bezpečnosti.

Ministerstvo financií Slovenskej republiky stanovuje 10 základných oblastí znalostí informačnej bezpečnosti. Používateľov informačných systémov verejnej správy taktiež rozdeľuje na 5 základných kategórií podľa úlohy, ktorú voči informačnému systému plnia a podľa znalostných potrieb z informačnej bezpečnosti, ktoré na plnenie svojich povinností potrebujú. Základné oblasti znalostí informačnej bezpečnosti a kategórie používateľov informačných systémov verejnej správy sú uvedené v tabuľke 2.

Tabuľka 2: Základné oblasti znalostí informačnej bezpečnosti a kategórie používateľov informačných systémov verejnej správy

Základné oblasti znalostí informačnej bezpečnosti		Kategórie používateľov informačných systémov verejnej správy
Legislatíva a štandardy informačnej bezpečnosti	Riadenie prístupu	Laici
Riadenie informačnej bezpečnosti	Bezpečnosť komunikácie	Manažéri a vedúci pracovníci
Riadenie rizík	Správa bezpečnostných incidentov	Informatici nešpecialisti v informačnej bezpečnosti
Obstarávanie, vývoj a zmeny IKT systémov	Prevádzka IKT systémov a kontinuita činnosti	Špecialisti v informačnej bezpečnosti
Fyzická bezpečnosť	Audit informačnej bezpečnosti	Učitelia informačnej bezpečnosti

Zdroj: Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR.

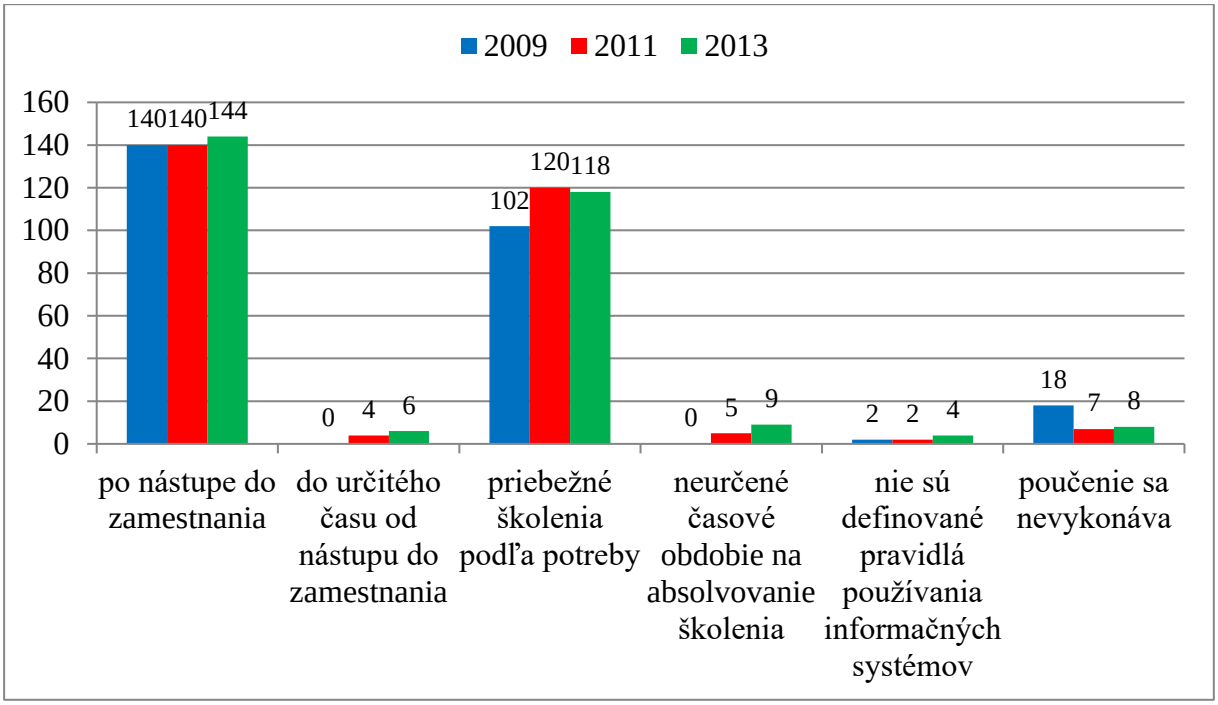
Laici sú ľudia bez systematického informatického vzdelania, ktorí používajú IKT systémy a najmä aplikácie ako nástroje na plnenie svojich pracovných úloh, ale v IKT systéme majú zvyčajne minimálne oprávnenia, postačujúce na plnenie ich základných pracovných povinností. **Manažéri a vedúci zamestnanci** (s výnimkou manažérov IT) na jednej strane spravidla nemajú systematické vedomosti o IKT, na druhej strane zodpovedajú za ochranu aktív organizácie, ktoré sú v ich pôsobnosti. Zároveň rozhodujú o bezpečnostnej politike organizácie, prostriedkoch na jej realizáciu, riadení informačnej bezpečnosti a podobne. Často sú zodpovední za naplnenie legislatívnych požiadaviek na informačnú bezpečnosť v organizácii. Tretiu kategóriu používateľov informačných systémov verejnej správy tvoria **informatici, nešpecialisti v informačnej bezpečnosti**, ktorí IKT systémy vyvíjajú, spravujú po technickej stránke, alebo riadia IT procesy v súlade s potrebami organizácie, implementujú a udržiavajú bezpečnostné opatrenia, ale priamo nezodpovedajú za informačnú bezpečnosť. Vo verejnej správe v tejto kategórii pôsobia informatici v dvoch rolách – IT manažéri a správcovia informačných a komunikačných technológií. Ďalšou kategóriou sú **špecialisti v informačnej bezpečnosti.** Do tejto kategórie patria v prvom rade manažéri informačnej bezpečnosti

[6] Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR.

rozličných úrovní, audítori IKT systémov a produktov, operátori bezpečnostných technológií, bezpečnostní analytici, vyšetrovatelia špecializujúci sa na počítačovú kriminalitu. Vo verejnej správe pôsobia v role manažérov informačnej bezpečnosti, operátorov bezpečnostných technológií, audítorov alebo bezpečnostných analytikov. **Učiteľ informačnej bezpečnosti** je poslednou kategóriou používateľa informačného systému verejnej správy a je možné ho považovať za odborníka v informačnej bezpečnosti, ktorý v tejto oblasti pravidelne vykonáva systematickú vzdelávaciu činnosť. Kvalifikácia učiteľa informačnej bezpečnosti je daná znalosťami, ktoré má poslucháčom odovzdať a schopnosťou podať ich tak, aby im poslucháči porozumeli a osvojili si ich.[7]

Prieskum stavu informačnej bezpečnosti

Ministerstvo financií Slovenskej republiky pravidelne vykonáva prieskum stavu informačnej bezpečnosti v organizáciách, v ktorom na zisťuje prístup užívateľov k ochrane informácií a aktív v digitálnom prostredí. Prieskumy sú vykonávané v súlade s Národnou stratégiou pre informačnú bezpečnosť v SR a doposiaľ boli vykonané trikrát. Otázky prieskumu sú rozdelené do šiestich oblastí. Jednou z oblastí je oblasť vzdelávania v oblasti informačnej bezpečnosti. Cieľom prieskumov je zistiť trend vývoja úrovne informačnej bezpečnosti a určiť silné a slabé stránky vzhľadom na predchádzajúce obdobie. Obrázok 1 poskytuje prehľad odpovedí respondentov na otázku kedy v organizácii prebieha poučenie o pravidlách používania informačných systémov, pričom respondenti mohli označiť viacero odpovedí.[8]

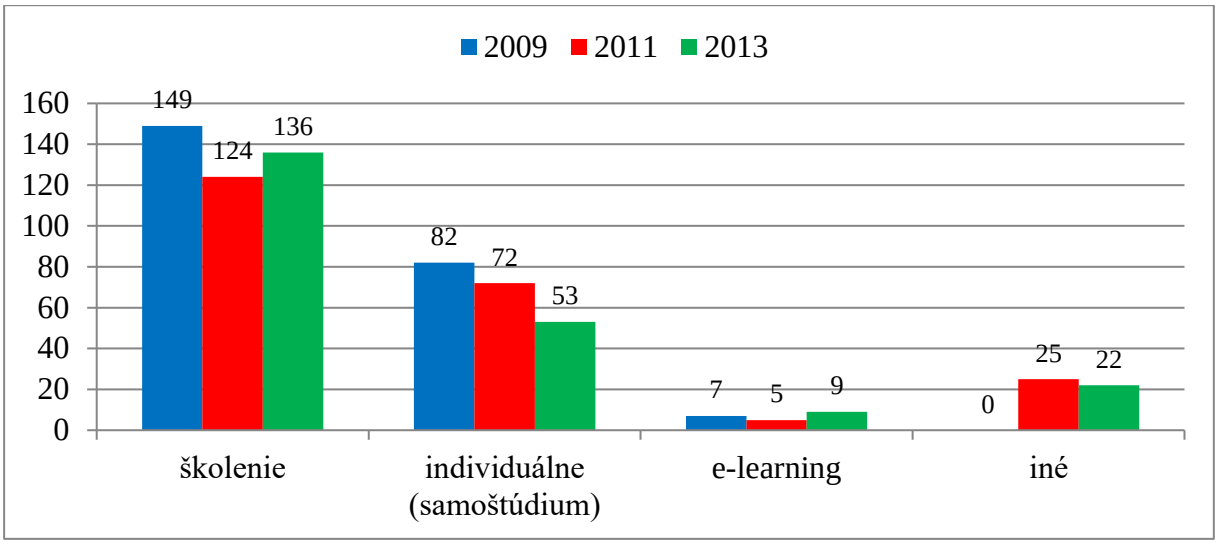


Obr. 1: Kedy v organizácii prebieha poučenie o pravidlách používania informačných systémov
Zdroj: ŠOLTÉS, V. a kol. Education in information security. In INTED 2016 proceedings. Valencia: IATED Academy, 2016.

Vzdelávanie a poučenie zamestnancov o bezpečnosti informačných systémov ihneď po nástupe do zamestnania sa vykonáva v 3 zo 4 oslovených organizáciách. Vo väčšine prípadov sa vykonávajú aj priebežné školenia zamestnancov. Pri porovnaní rokov 2011 a 2013 však je

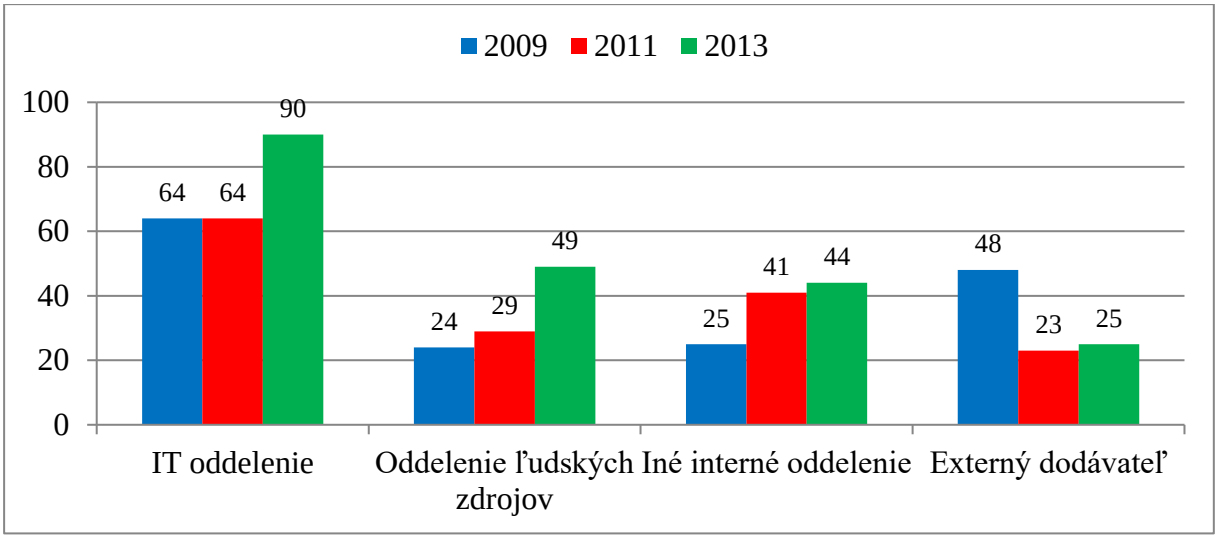
[7] OLEJÁR, D. a kol. *Informačná bezpečnosť*. Bratislava: Ministerstvo financií Slovenskej republiky, 2013.
[8] ŠOLTÉS, V. a kol. Education in information security. In *INTED 2016 proceedings.* Valencia: IATED Academy, 2016. s. 4418-4424.

možné negatívne hodnotiť mierny nárast počtu organizácií, ktoré nemajú určené časové obdobie pre absolvovanie kurzov. Aj v nasledujúcej otázke zaoberajúcej sa formou vzdelávania zamestnancov o informačnej bezpečnosti mohli organizácie odpovedať označením viacerých možností. Obrázok 2 zobrazuje aký je vývoj foriem vzdelávania zamestnancov v organizáciách.



Obr. 2: Forma vzdelávania zamestnancov o informačnej bezpečnosti v organizáciách
Zdroj: ŠOLTÉS, V. a kol. Education in information security. In INTED 2016 proceedings. Valencia: IATED Academy, 2016.

Vzdelávanie je v organizáciách organizované najčastejšie formou školení, ale do vysokej miery sa využíva aj forma samoštúdia. Zatiaľ čo forma individuálneho vzdelávania sa zamestnancov má klesajúci trend, je možné si všimnúť zvýšenie využívania e-learningu vo vzdelávaní. Tretia otázka prieskumu bola zameraná na subjekt vykonávajúci školenia v rámci organizácie, pričom respondenti mohli opäť označiť viacero odpovedí. Obrázok 3 znázorňuje prehľad subjektov zodpovedných za školenia o informačnej bezpečnosti v organizácii.



Obr. 3: Prehľad subjektov zodpovedných za školenia o informačnej bezpečnosti v organizácii
Zdroj: ŠOLTÉS, V. a kol. Education in information security. In INTED 2016 proceedings. Valencia: IATED Academy, 2016.

Najvýznamnejším faktom, ktorý z tejto otázky vyplýva je to, že v takmer 90 % prípadoch vykonáva školenie organizácia interne. Najčastejšie školenie vykonáva IT oddelenie alebo zodpovedný informatický pracovník. Pri porovnaní posledných dvoch rokov je zrejmé, že narástol aj počet prípadov, kedy boli školenia vykonávané oddelením ľudských zdrojov.

Záver

Problematika kybernetickej bezpečnosti sa v súčasnosti stáva jednou z najdiskutovanejších tém z hľadiska ochrany osôb a majetku. Aktuálnosť, významnosť a dôležitosť témy zvýrazňuje aj zvýšený počet zákonov a iných všeobecne záväzných právnych predpisov v tejto oblasti. Aj napriek prijímaniu týchto predpisov sa však čoraz častejšie vyskytujú kybernetické bezpečnostné incidenty. Problémom je nedostatočná osvetová činnosť a nedostatočný systém vzdelávania v oblasti kybernetickej bezpečnosti.

Z dôvodu, že na Slovensku neexistuje študijný odbor informačná bezpečnosť, nie je jasne stanovený obsah vzdelávania v tejto oblasti. Ministerstvo financií Slovenskej republiky preto ešte v roku 2009 vytvorilo Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR, ktorým rozdelil užívateľov digitálneho priestoru a stanovil oblastí informačnej bezpečnosti, s ktorými sa užívatelia dostávajú do kontaktu. Pri zostavovaní obsahu školení používateľov digitálneho priestoru je potrebné pre každý typ užívateľa stanoviť úroveň poznania oblastí informačnej bezpečnosti. Inováciou tohto návrhu systému vzdelávania došlo k novej kategorizácii používateľov informačných systémov verejnej správy a k stanoveniu nových základné oblasti znalostí informačnej bezpečnosti, čím boli stanovené minimálne požiadavky na vzdelávanie používateľov informačných systémov v oblasti kybernetickej bezpečnosti. V rámci prieskumu stavu a vývoja informačnej bezpečnosti je možné konštatovať, že najčastejšou formou vzdelávania zamestnancov sú školenia a kurzy vykonávané interne. Prieskum tiež potvrdil trend vzdelávania zamestnancov vykonávaného ihneď po nástupe do zamestnania. Pozitívnym faktom je však to, že organizácie aj v priebehu pracovného pomeru vykonávajú priebežné školenia zamestnancov.

Poďakovanie

Príspevok bol spracovaný v rámci riešenia projektu VEGA 1/0768/19.

Zoznam použitej literatúry:

1. HOCHMANN, J. 2016. *Kybernetická bezpečnosť a štát*. [online]. [cit. 2019-05-10]. Dostupné na: <http://ideme.net/wp-content/uploads/sites/2/2017/04/Hochmann_iDEME2016.pdf>
2. *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.*
3. *Návrh systému vzdelávania v oblasti informačnej bezpečnosti v SR.*
4. OLEJÁR, D. a kol. *Informačná bezpečnosť*. Bratislava: Ministerstvo financií Slovenskej republiky, 2013. 403 s.
5. *Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2009, 2011 a 2013.*
6. ŠOLTÉS, V. a kol. Education in information security. In: *INTED 2016 proceedings.* Valencia: IATED Academy, 2016. s. 4418-4424. ISBN 978-84-608-5617-7.
7. *Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. v znení neskorších predpisov.*

Kontaktné údaje:
Ing. Viktor Šoltés, PhD.
Fakulta bezpečnostného inžinierstva
Katedra bezpečnostného manažmentu
Žilinská univerzita v Žiline
Viktor.Soltes@fbi.uniza.sk

Ing. Anton Šiser, PhD.
Národný bezpečnostný úrad
Anton.Siser@fbi.uniza.sk

Role manažera kybernetické bezpečnosti v procesu řízení hrozeb

Vladimír Šulc

Abstrakt:
Cílem příspěvku je identifikovat a popsat generické hrozby, kterým je každý informační systém vystaven a zaměřit se na tzv. APT hrozby. Řízení hrozeb je jedna z činností manažera kybernetické bezpečnosti, které by se měl věnovat, neboť rozhoduje o tom, zda útok na organizaci, pro kterou pracuje, bude úspěšný. V rámci řízení hrozeb se předpokládá, že existuje neurčitý počet technických zranitelností, kterých může být zneužito, a které nejsou pro organizaci provozující informační systém známy, tudíž je nemožné je efektivně zvládat.
Klíčová slova:
Řízení hrozeb, kyberprostor, C&C serverem, DNS komunikace.

Abstract:
The aim of the paper is to identify and describe generic threats to which each information system is exposed and to focus on the so-called APT threats. Because it largely decides whether the attack on the organization it works for will be successful. Threat management assumes that there is an indeterminate number of technical vulnerabilities that can be exploited and that are not known to the organization operating the information system, and therefore impossible to manage effectively.
Key words:
Threat Management, Cyberspace, C&C Server, DNS Communications.

Úvod

Vzhledem k zaměření mého příspěvku by měla přinést odpověď na otázku jak efektivně provést zhodnocení úrovně kybernetické bezpečnosti v organizaci a její odolnosti vůči kybernetickým útokům, jsem se rozhodl zaměřit na jednu specifickou činnost manažera kybernetické bezpečnosti a tou je řízení hrozeb. Řízení hrozeb, v anglosaské literatuře označované jako threat management je jedna z mnoha činností manažera kybernetické bezpečnosti, které by se měl intenzivně věnovat, neboť do značné míry rozhoduje o tom, zda útok na organizaci, pro kterou pracuje, bude úspěšný či nikoliv. V rámci řízení hrozeb se předpokládá, že existuje blíže neurčitý počet technických zranitelností, kterých může být zneužito, a které nejsou pro organizaci provozující informační systém známy, a tudíž je nemožné je efektivně zvládat. Zároveň však platí, že k tomuto neurčitému počtu zranitelností, které spadají do určité kategorie, označované jako slabina, lze přiřadit nepoměrně menší počet hrozeb, které řídit lze, byť jejich počet a intenzita se rovněž může měnit v čase. Cílem tohoto příspěvku je identifikovat a popsat generické hrozby, kterým je každý informační systém vystaven a zaměřit se pak na tzv. APT hrozby.

Hrozby

Kybernetický útok (cyber attack) je dle NIST[1] definován jak útok v kyberprostoru s cílem narušit, zničit, odpojit nebo ovládnout daný systém či pozměnit nebo získat citlivá data. S pojmem kybernetický útok pak velice úzce souvisí pojem kybernetická hrozba (cyber threat), která je dle NIST[2] definována jako událost, která má potenciál způsobit škodu na aktivech a vést k dalším následným ztrátám, vyplývajícím z narušení bezpečnosti informací a systémů. Ve svém úzkém pojetí by pak za kybernetické hrozby bylo možno považovat jen hrozby přicházející z kyberprostoru, ovšem v širším pojetí, tak jak např. kybernetické hrozby v ČR vnímá aktuální Zákon o kybernetické bezpečnosti, zkr. ZoKB[3] resp. Vyhláška o kybernetické

[1] NIST. Cyber Attack - Glossary | CSRC. [online]. [cit. 2019-05-06]. Dostupné na:<https://csrc.nist.gov/glossary/term/Cyber-Attack>
[2] NIST. Cyber Threat - Glossary | CSRC [online]. [cit. 2019-05-06]. Dostupné na:<https://csrc.nist.gov/glossary/term/Cyber-threat>
[3] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů.

bezpečnosti VoKB[4], musí být zohledněny i hrozby vyšší moci a fyzické povahy, které by rovněž mohly způsobit škody na informačních aktivech kritické informační infrastruktuře, významných informačních systémech a systémech základních služeb. Kybernetický útok pak na rozdíl od hrozeb může být veden jen z kyberprostoru a jeho cílem jsou informační aktiva. Za informační aktiva pak lze dle ISO 27005:2018[5] považovat data, informace a služby poskytované informačním systémem, které jejich vlastníkovi generují zisk. Zatímco informace a služby jsou tzv. primárními aktivy, tak informační systém, který se skládá z mnoha dalších komponent, pak představuje tzv. sekundární aktiva. Zde je nutné si uvědomit, že byť jsou cílem útočníka zpravidla primární aktiva, tedy informace a služby poskytované daným informačním systémem, tak kybernetický útok je veden na sekundární aktiva, tedy samotný systém, síťovou infrastrukturu, servery, koncová zařízení a jejich uživatele. Vlastník je tedy nucen za účelem ochrany svých informačních aktiv zavést vhodná bezpečnostní opatření organizační a technické povahy, a to taková, která sama o sobě nebudou z pohledu celkových nákladů dražší než možná škoda, která by mohla vzniknout v přímé souvislosti s kybernetickým útokem. Útočník pak v systému hledá jakoukoliv zranitelnost, které by mohl zneužít. Přičemž zranitelnost lze považovat buď za vlastnost aktiva, ale může se nacházet i v samotném bezpečnostním opatření, které může být nedostatečné, anebo zcela chybět, a pak může být s větším či menším úsilím překonáno.

Anatomie hrozeb

Hrozby můžeme rozdělit mnoha různými způsoby. Nejjednodušší je dělení podle toho, jaký atribut bezpečnosti může být hrozbou narušen. Pokud důvěrnost, lze hovořit o **hrozbách pasivních**, protože nedochází ke změně stavu systému ani informací, pokud může dojít k narušení integrity a dostupnosti, lze hovořit o **aktivních hrozbách**, neboť jejich působením ke změně stavu dochází.

Podle původce hrozby (threat agent) můžeme hrozby rozdělit na **hrozby způsobené lidmi** a **vyšší mocí** (vis maior). V prvním případě je to osoba, která realizuje danou hrozbu, ať už vědomě nebo nevědomě a nese za své jednání plnou odpovědnost, tak ve druhém případě za ní nikdo neodpovídá[6].

Podle zdroje, tedy odkud hrozby přichází, je možné je ještě rozdělit na vnější a vnitřní, přičemž **vnější hrozby** pochází z vně organizace a jsou zcela mimo její kontrolu a **vnitřní hrozby** pak přichází z prostředí organizace, které má organizace zpravidla možnost ovlivnit, neboť toto prostředí přímo utváří. Když tyto dva pohledy zkombinujeme, získáme následující matici zachycenou v *Tabulka č. 1: Motiv – zdroj*.

Tabulka č. 1: Motiv – zdroj

Motiv/zdroj	Interní	Externí
Úmyslná	sabotáž, hacking, krádež informací, pozměnění	hacking
Neúmyslná náhodná	strukturální (selhání operátora, selhání stroje)	environmentální (vyšší moc, přírodní pohromy)

Zdroj: vlastní zpracování

[4] Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[5] ISO. Norma ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management. červenec 2018.

[6] KINCL, J., URFUS, V., SKŘEJPEK, M. *Římské právo.* Praha: C.H. Beck, 1995. s. 223.

Tímto způsobem byly v zásadě identifikovány 4 zdroje hrozeb, které NIST 800-30[7] definuje takto:

- **Úmyslné** (adversarial) realizované ze strany jednotlivců, organizovaných skupin, konkurence, státu. Úmyslné hrozby můžeme dále rozdělit podle toho, zda útočník vede útok na konkrétní subjekt anebo je mu jedno, který subjekt se stane jeho příští obětí. Subjektem se v tomto případě myslí buď infrastruktura (koncové zařízení, server, síťový prvek), anebo lidský operátor zastávající v daném systému jakoukoliv roli (uživatel, správce, vývojář). Kdy výsledkem těchto útoků je zpravidla získání informací, kompromitace systému nebo narušení jeho dostupnosti.
- **Náhodné** (accidental), kdy se jedná o chybu zaměstnance, ať už uživatele nebo správce systému při vykonávání běžných denních činností. Náhodné nebo také neúmyslné hrozby jsou hrozby, kdy k narušení bezpečnosti došlo z důvodu nedbalosti nebo selhání zaměstnance, kterým svým konáním nebo naopak nekonáním narušení bezpečnosti způsobil. Přičemž je třeba rozlišovat mezi nedbalostí vědomou a nevědomou, protože zatímco v prvním případě zaměstnanec věděl, že by narušení bezpečnosti mohl způsobit, a v nepřiměřené míře spoléhal, že se tak nestane, tak ve druhém případě toto vůbec nepředpokládal.
- **Strukturální** (structural), kdy došlo k selhání HW nebo SW ať už v důsledku stáří nebo překročení provozních parametrů. Některé tyto hrozby lze předvídat a předcházet jim v okamžiku, kdy se vytváří vanová křivka a sleduje životnost každé použité komponenty, provádí monitoring výkonnostních parametrů, realizuje kapacitní plánování a jsou připraveny příslušné scénáře.
- **Environmentální** (environmental), kdy došlo k nějaké přírodní pohromě/katastrofě a k selhání infrastruktury, která je zcela mimo kontrolu organizace. Patří se hrozby jako povodeň, požár, zemětřesení, tornádo a výpadek infrastruktury jako je voda, elektřina, telekomunikace, na kterých může být organizace rovněž závislá.

Přičemž všechny výše uvedené typy hrozeb mohou mít v případě jejich realizace negativní dopad na informační systémy. Úmyslné kybernetické hrozby mající povahu kybernetických útoků pak lze rozdělit z pohledu velikosti zásahu na útoky:

- **Plošné**, kdy útočníkovi je v zásadě jedno, kdo se stane jeho obětí, a napadne **jakýkoliv subjekt**, která trpí **určitou zranitelností** (Při těchto útocích do určité míry záleží na úrovni zabezpečení ostatních subjektů na trhu, protože útočník realizuje úspory z rozsahu a cílí na tzv. low hanging fruit, tedy ty hůře zabezpečené subjekty).
- **Cílené**, kdy útočník vede útok na **konkrétní subjekt** a hledá **jakoukoliv zranitelnost**, které by mohl zneužít. (U těchto typů útoků nehraje úroveň zabezpečení ostatních subjektů na trhu v podstatě žádnou roli, neboť útočník je připraven vyvinout nezměrné úsilí, prostředky a čas k dosažení svého cíle).

Z pohledu předmětu cílení, byť to ne vždy musí být na první pohled zřejmé, je možné kybernetické útoky rozdělit na útoky vedené primárně na:

- **Lidi**, kdy útočník **zneužívá technik sociálního inženýrství a nedostatečného bezpečnostního povědomí** a snaží se oběť přimět k tomu, aby mu poskytla informaci nebo provedla činnost, kterou on potřebuje[8].

[7] NIST. 2012. NIST Special Publication 800-30 Guide for Conducting Risk Assessments. [online]. [cit. 2019-05-06]. Dostupné na:<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>

[8] MANN, I. *Hacking the human: social engineering techniques and security countermeasures*. Aldershot, England, Burlington, VT: Gower, 2008.

- **Infrastrukturu**, kdy útočník **zneužívá zranitelností, které se nacházejí v návrhu, v kódu anebo implementaci** aplikace, systému nebo sítě, kdy žádná interakce ze strany uživatele není vyžadována.

APT

Na některé společnosti jsou vedeny útoky jen proto, že jsou přítomny na internetu, na jiné však proto, co dělají, to je případ tzv. APT útoků. Dle SANS[9] byl pojem APT poprvé použit v roce 2006 analytiky United States Air Force, a měl vyjadřovat pokročilou a přetrvávající hrozbu (Advanced Persistent Threat, zkr. APT).

Ve výkladovém slovníku NIST[10] je pak APT hrozba definována jako hrozba, kdy útočník disponuje sofistikovanými znalostmi a významnými zdroji, které mu umožňují vytvářet si příležitosti k dosažení svých cílů, které obvykle vedou k průniku a uhnízdění se v infrastruktuře organizace, která je předmětem zájmu útočníka za účelem získání informací, narušení provozu, nebo způsobení škody a to hned anebo kdykoliv v budoucnu, opakovaně, během delšího časového období, kdy se útočník brání odhalení, maskuje se, zahlazuje stopy a zároveň si zajišťuje potřebnou úroveň interakce za účelem splnění svých cílů.

Musa[11] pak dodává, že APT útok je kontinuální proces, kdy dochází k pečlivě připravenému, postupnému a nenápadnému hackování vyhlédnuté entity.

Naproti tomu dle Bruce Schneiera nejsou pokročilé a přetrvávající hrozby (Advanced Persistent Threat, zkr. APT) nic jiného než cílené útoky[12] a jedná se tak trochu o buzzword, a jak tvrdí Čermák, mohlo by se stejně tak hovořit i o léty prověřených technikách, Aged Proven Techniques nebo ještě poetičtěji Ancient Proven Techniques[13], protože se vždy jedná o kombinaci technik sociálního inženýrství a zranitelností nultého dne. To potvrzují i nejrůznější analýzy, např. společnost Imperva tvrdí, že mnohdy je spíše než nějakých pokročilých technik využito technik naprosto běžných[14].

Dle FireEye se doba po kterou zůstává APT útok nedetekován, postupně zkracuje, v roce 2011 to bylo 416 dní, tedy více než rok, zatímco v roce 2018 už jen 78 dní, tedy něco přes dva měsíce[15]. To však v mnoha případech může být stále doba dostatečně dlouhá k dosažení cíle, protože dle společnosti Verizon je cíle dosaženo zpravidla za mnohem kratší dobu[16].

Předmětem APT útoků jsou zpravidla organizace, které jsou součástí kritické infrastruktury státu, provozující kritickou informační infrastrukturu, zkr. KII, významné informační systémy, zkr. VIS a systémy základních služeb, zkr. SZS, disponují cenným know-how, které je předmětem průmyslové špionáže anebo realizují velké obraty peněz.

Tyto útoky jsou realizovány ze strany vysoce organizovaných a dost často i státem sponzorovaných skupin a probíhají i po dobu několika měsíců až let. A byť jsou náklady na tyto

---

[9] BINDE, B. E, MCREE R. a J O'CONNOR, T. *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*, s. 35.

[10] NIST. advanced persistent threat (APT) - Glossary | CSRC. [online]. [cit. 2019-05-06]. Dostupné na: <https://csrc.nist.gov/glossary/term/advanced-persistent-threat>

[11] MUSA, S. Advanced Persistent Threat - APT | Dr. Sam Musa - Academia.edu. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT>

[12] SCHNEIER, B. Advanced Persistent Threat (APT) - Schneier on Security. Schneier on Security. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.schneier.com/blog/archives/2011/11/ advanced_persis.html>

[13] ŠULC, V. *Kybernetická bezpečnost*. Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2018.

[14] HII_The_Non-Advanced_Persistent_Threat.pdf. [online]. [cit. 2019-05-06]. Dostupné na:<https://www. imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf>

[15] FIREEYE. M-Trends. 2019. *FireEye*. [online]. [cit. 2019-05-06]. Dostupné na:<https://content. fireeye.com/m-trends>

[16] DBIR. 2018. *Report.* [online]. [cit. 2019-05-06]. Dostupné na:<https://enterprise.verizon.com/resources/ reports/DBIR_2018_Report.pdf>

útoky značné a pohybují se v řádu stovek tisíc až miliónů, tak výnosy se pohybují v řádu vyšších stovek miliónů až jednotek miliard.

- Samotný APT útok lze rozdělit do několika na sebe navzájem navazujících fází, přičemž jejich počet a pojmenování se autor od autora výrazně liší. Některé zdroje uvádí 12 fází[17], jiné 10 fází[18], 7 fází[19] a některé jen 5 fází[20]. Onen rozdíl je však způsoben jen detailním rozepisováním čtyřech základních fází, kterými jsou: příprava, průnik, kompromitace a dokončení.
- **Příprava** – v této fázi se útočník snaží o předmětu svého cíle zjistit co nejvíce informací. Informace čerpá z veřejných zdrojů, jako jsou sdělovací prostředky, výroční zprávy, webové stránky dané organizace a sociální sítě. Vytváří si tak představu o tom, jak veliká daná organizace je, jaká je její organizační struktura, kdo jsou její zaměstnanci, na jakých pozicích se nachází, a s jakými dalšími organizacemi v odběratelsko-dodavatelském řetězci organizace spolupracuje, protože mnohdy je snazší vést útok na organizaci, která např. dodává HW a SW vybavení a začlenit do něj backdoor, nechat se u dané organizace zaměstnat a tím následně získat fyzický přístup do organizace, která je primárním cílem útočníka. V této fázi dále dochází k zjišťování informací o provozovaných systémech, probíhá skenování služeb vystavených do internetu, a jejich odpovědí na dotazy. Následně pak probíhá hledání zranitelností v provozovaných technologiích a vývoj nebo nákup exploitů potřebných k jejich zneužití, případně k začlenění backdooru do HW nebo SW používaného danou organizací. Tato přípravná fáze, kdy dochází rovněž k vytvoření nezbytné infrastruktury, C&C serverů, phishingových, e-mailů, falešných identit, apod. může probíhat i po dobu několika týdnů až měsíců a útočník při ní může využívat technik sociálního inženýrství, navazovat i intimní vztahy se zaměstnanci dané organizace a účelem získání informací nebo přístupu, neboť mnohdy je spolupráce s někým zevnitř nezbytná. Tuto přípravnou fázi tak lze rozdělit v zásadě na dvě části sběr informací (external reconnaissance) a vývoj nástrojů a přípravu infrastruktury k realizaci útoku (weaponization).
- **Průnik** – v této fázi dochází k fyzickému nebo vzdálenému průniku do prostředí dané organizace, ať už v přestrojení nebo jako skutečný zaměstnanec třetí strany a zapojením vlastního zařízení, např. falešného access pointu, HW keylogeru do vnitřní sítě organizace anebo dodáním HW nebo SW opatřeného backdoorem. Případně může dojít k podvržení falešné aktualizace podepsané klíčem, ke kterému je vydán certifikát od důvěryhodné certifikační autority, která byla za tímto účelem již dříve kompromitována[21]. Daleko častěji se však můžeme setkat s napadením jiného webu, který organizace navštěvuje a umístění exploitu tam (watering hole attack), a v okamžiku, kdy jej zaměstnanec dané organizace navštíví, tak dojde k exploitaci a stažení škodlivého kódu do jeho počítače (drive-by download). Anebo, což je vůbec nejčastější případ, může dojít k distribuci škodlivého kódu e-mailem (spear phishing) nebo na médiu (baiting), které útočník pohodí např. na

[17] Advanced Persistent Threats - Learn the ABCs of APT: Part A. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.secureworks.com/blog/advanced-persistent-threats-apt-a>

[18] RADZIKOWSKI, P., S. 2016. *CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation. Dr.Shem*. [online]. [cit. 2019-05-06]. Dostupné na:<http://DrShem.com/2016/02/11/ cybersecurity-expanded-look-apt-life-cycle-mitigation/>

[19] LACEY, D. a INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. 2013. Advanced persistent threats: how to manage the risk to your business. Rolling Meadows, IL: ISACA. [online]. [cit. 2019-05-06]. Dostupné na: <http://www.books24x7.com/marc.asp?bookid=62388>

[20] MILLS, E. *Attack on RSA used zero-day Flash exploit in Excel. CNET*. [online]. [cit. 2019-05-06]. Dostupné na:<https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/>

[21] ŠULC, V. *Kybernetická bezpečnost.* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2018.

parkovišti nebo na střeše budovy. I v této fázi se využívá technik sociálního inženýrství v kombinaci se zranitelnostmi nultého dne. Táto fáze má nejkratší trvání, a zpravidla probíhá vzdáleně přes internet, neboť se zde útočník vystavuje největšímu riziku, že si probíhajícího útoku někdo všimne, a proto se vše odehraje během několika málo minut nebo hodin. Táto fáze se dá opět rozdělit do několika částí, doručení exploitu (deliver), spuštění exploitu (exploit) obsahující nálož (payload), kdy se útočník pokouší o zvýšení svých oprávnění v napadeném systému (escalate privileges) zajištění perzistence (establish persistence) a instalace komponenty za účelem vzdáleného přístupu (remote access trojan, zkr. RAT) do napadeného systému.

- **Kompromitace** - v této fázi se již útočník nachází v prostředí organizace, kde kompromitoval jedno či více koncových zařízení nebo serverů, zajistil si v nich perzistenci a nyní se seznamuje se síťovou infrastrukturou (internall reconnaissance), a vyhledává systémy, které by mohl dále napadnout (colaterall movement). Za tímto účelem zachycuje přihlašovací údaje, pořizuje snímky obrazovky, zaznamenává činnosti zaměstnanců ve formě videa, a tyto informace pak zasílá na C&C server útočníka k analýze a stanovení dalšího postupu a to tak dlouho, dokud není dosaženo cíle. Komunikace s C&C serverem pak probíhá šifrovaně, je schována do DNS komunikace anebo je využito pokročilé lingvistické steganografie, kdy informace jsou umně schovány v prostém textu nacházejícím se na webech, které uživatel běžně navštěvuje, jako jsou sociální sítě, O365 nebo Google. Vlastní malware na koncových zařízeních a serverech organizace má pak často podobu tzv. fileless malwaru, tedy bezsouborového malwaru, který se ukrývá do registrů, a běžných procesů a maximálně využívá součástí systému, jako je powershell, apod a je proto velice obtížné jej odhalit. Tato fáze, podobně jako fáze přípravy může trvat poměrně dlouho a to po dobu několika měsíců až let, než se útočníkovi podaří zcela ovládnout daný systém nebo získat přístup k citlivým informacím, které jsou předmětem jeho zájmu.
- **Dokončení** – v okamžiku, kdy dojde ke kompromitace cílového systému, kompletního ovládnutí infrastruktury, výroby, služby, vyřazení daného systému z provozu anebo získání citlivých informací, které jsou shromážděny (data gathering) a připraveny ke zkopírování na server útočníka (data exfiltration), tak se přesouváme do poslední fáze. Tato fáze trvá rovněž poměrně krátce, ovšem délka jejího trvání do značné míry závisí na tom, co je cílem útočníka, protože pokud je cílem útočníka exfiltrace informace, tak nemusí být vůbec odhalen a přístup k informacím si může udržovat po poměrně dlouhou dobu. Zde jen záleží na tom, jaké je ono množství informací, které potřebuje exfiltrovat, tedy zkopírovat do tzv. drop zóny a zda si někdo všimne zvýšeného provozu, či jiné anomálie, ke které ale také nemusí dojít, pokud bude jako drop zóna zvolen např. cloud Microsoftu, Googlu anebo Amazonu, který organizace běžně využívá. V případě nedostupnosti anebo pozměnění informací či dat pak zpravidla dojde k nějaké škodě a v tu chvíli se i rozjíždí vyšetřování, a je zahájen audit a forenzní analýza. Zde pak záleží na tom, zda se útočníkovi podařilo malware, a případné účty a logy odstranit a jak zkušený je analytik provádějící forenzní analýzu, a zda najde stopy po přítomnosti malwaru v systému anebo dokonce samotný malware.

Pravděpodobnost realizace hrozby může ovlivňovat spousta faktorů, obzvlášť pokud se jedná o úmyslné hrozby. Už samotné aktivum a vidina potenciálního zisku může útočníka přitahovat a činit pro něj dané aktivum atraktivní. To je i důvod, proč na některé organizace jsou útoky vedeny častěji než na jiné, a na některé vůbec. Nejčastěji se však uvádí tři faktory, které tuto pravděpodobnost ovlivňují, jsou jimi motiv, příležitost a schopnost.

- **Motiv** - může být různý, může se jednat o přímý finanční zisk, což je nejčastější případ, či nepřímý, spočívající v získání nějaké výhody, třeba i tím, že druhé straně vznikne škoda, ale může se jednat i o pomstu, touhu po respektu a uznání. Motiv sám o sobě není dostačující, neboť pokud daná osoba nemá příležitost hrozbu realizovat anebo nedisponuje odpovídajícími znalostmi, nemůže danou hrozbu s úspěchem realizovat.
- **Příležitost** - zde je rozhodující, zda je možné vést útok přes internet anebo je nutné se nacházet na stejné síti anebo se dostat do fyzického kontaktu s předmětným aktivem. V okamžiku, kdy je možné vést útok přes internet, tak se pravděpodobnost hrozby podstatně zvyšuje. Ovšem i když má osoba příležitost hrozbu realizovat, tak to neznamená, že ji realizuje, neboť ještě musí mít dostatečně silný motiv a disponovat i odpovídajícími znalostmi.
- **Schopnost** - čím nižší jsou nároky na její realizaci, tedy znalosti a dovednosti, a jestli jsou tyto nároky nízké a v krajním případě ji může realizovat v podstatě každý uživatel internetu, tak se tím podstatně zvyšuje pravděpodobnost, že dojde k její realizaci. Ale i zde platí, že i když bude daná osoba disponovat danou schopností a dokázala by útok realizovat, tak musí mít i motiv a příležitost.

Z výše uvedeného vyplývá, že tyto faktory nelze vyhodnocovat odděleně, ale je třeba je vnímat komplexně, neboť, vždy musí být přítomny všechny tři, aby došlo k realizaci samotné hrozby. Na druhou stranu je třeba připustit, že v okamžiku, kdy bude existovat dostatečně silný motiv a útočník bude disponovat i odpovídajícími finančními prostředky, tak si může najmout někoho, kdo má dané schopnosti a dokáže si vytvořit i odpovídající příležitosti k tomu, aby hrozbu realizoval.

Jednoduše tak nelze od počtu potenciálních útočníků odvozovat pravděpodobnost realizace hrozby, a tvrdit, že v okamžiku, kdy danou schopností a příležitostí disponuje jen pár osob na světě, tak je pravděpodobnost takové hrozby nízká. Tuto hypotézu potvrzují i nejrůznější státem sponzorované útoky nebo útoky realizované vysoce organizovanými skupinami, kdy došlo ke kompromitaci i velice dobře zabezpečených informačních systémů a k obrovským finančním ztrátám.

Pravděpodobnost úmyslných útoků lze velice špatně odhadnout, nicméně lze monitorovat situaci v kyberprostoru a analyzovat již proběhnuvší útoky a hledat v nich určité společné charakteristiky, jako kdo útok realizoval, jaký vektor útoku byl použit, kdo byl obětí útoku, v jakém odvětví působil, jaké bylo jeho postavení na trhu, v jaké fázi životního cyklu se daná organizace nacházela apod.

A jelikož se může pravděpodobnost hrozeb v čase měnit, především v důsledku změn v kyberprostoru, měla by se analýza opakovat a uplatňovat princip předběžné opatrnosti, tzv. due care a due diligence.

Závěr

Neexistuje jednotná taxanomie hrozeb, každý autor používá různé názvosloví a pojmenování pro jednotlivé hrozby a kategorie hrozeb. Další výzkum by se proto měl zaměřit na určení relevantních zdrojů, které by se daly použít pro stanovení kategorií hrozeb, a určení těch hrozeb, kterým organizace aktuálně čelí a budou čelit v nejbližších letech a navrhnout vhodný způsob, jak posoudit jejich připravenost a odolnost vůči těmto hrozbám.

Zoznam použitej literatúry:

1. Advanced Persistent Threats-Learn the ABCs of APT: Part A. 2016. [online]. [cit. 2019-03-06]. Dostupné na:<https://www.secureworks.com/blog/advanced-persistent-threats-apt-a>

2. BINDE, Beth E., Russ MCREE a Terrence J O'CONNOR. *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*. s. 35.
3. DBIR. *2018. Report.pdf*. [online]. [cit. 2019-03-08]. Dostupné na: <https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf>
4. FireEye. 2019. *M-Trends.* [online]. [cit. 2019-03-08]. Dostupné na: <https://content.fireeye.com/m-trends>
5. *HII. The Non-Advanced Persistent Threat.pdf*. [online]. [cit. 2019-03-08]. Dostupné na: <https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf>
6. ISO. *Norma ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management*. 2018.
7. KINCL, J., URFUS, V., SKŘEJPEK, M. *Římské právo*. Praha: C.H. Beck, 1995. ISBN 978-80-7179-031-0.
8. LACEY, D. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. 2013. *Advanced persistent threats: how to manage the risk to your business*. [online]. [cit. 2019-03-08]. Dostupné na:<http://www.books24x7.com/marc.asp?bookid=62388>
9. MANN, I. *Hacking the human: social engineering techniques and security countermeasures*.
10. MILLS, E. 2011. *Attack on RSA used zero-day Flash exploit in Excel. CNET*. [online]. [cit. 2019-03-08]. Dostupné na:<https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/>
11. MUSA, S. 2014. *Advanced Persistent Threat-APT | Dr. Sam Musa - Academia.edu*. [online]. [cit. 2019-03-06]. Dostupné na: <https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT>
12. NIST. 2012. *NIST Special Publication 800-30 Guide for Conducting Risk Assessments*. [online]. [cit. 2019-03-06]. Dostupné na: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>
13. NIST. *Advanced persistent threat (APT) - Glossary | CSRC*. [online]. [cit. 2019-03-06]. Dostupné na: <https://csrc.nist.gov/glossary/term/advanced-persistent-threat>
14. NIST. *Cyber Attack-Glossary | CSRC*. [online]. [cit. 2019-03-06]. Dostupné na: <https://csrc.nist.gov/glossary/term/Cyber-Attack>
15. NIST. *Cyber Threat-Glossary | CSRC*. [online]. [cit. 2019-03-04]. Dostupné na: <https://csrc.nist.gov/glossary/term/Cyber-threat>
16. RADZIKOWSKI, Przemek Shem. 2016. *CyberSecurity: Expanded Look at the APT Life Cycle and Mitigation.* [online]. [cit. 2019-03-08]. Dostupné na: <http://DrShem.com/2016/02/11/cybersecurity-expanded-look-apt-life-cycle-mitigation/>
17. Shodan. [online]. [cit. 2019-02-17]. Dostupné na:<https://www.shodan.io/>
18. SCHNEIER, B. 2011. *Advanced Persistent Threat (APT) - Schneier on Security*. [online]. [cit. 2019-03-04]. Dostupné na: <https://www.schneier.com/blog/archives/2011/11/advanced_persis.html>
19. ŠULC, V. *Kybernetická bezpečnost.* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
20. *Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.*
21. *Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů*
22. ZERODIUM-TheLeading Exploit Acquisition Platform. [online]. [cit. 2019-02-17]. Dostupné na:<http://zerodium.com/>

Kontaktné údaje:

Ing. Vladimír Šulc, Ph.D.
Fakulta bezpečnostného manažmentu
Policajná akadémia v Českej republike v Prahe
sulc@polac.cz

Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom

Kristián Ujváry, Jana Kuchtová

Abstrakt:
Autori v prvej časti príspevku predstavujú okruh používateľov kryptomien ako aj predpokladané účely ich využitia. Venujú sa inštitucionálnej ochrane pred nelegálnym využitím kryptomien, špecificky bitcoinu, ako na národnej, tak aj na medzinárodnej úrovni. Predstavujú legislatívny rámec upravujúci postup pri vzájomnej výmene informácií, ich sprístupnenie oprávneným agentúram a útvarom. V príspevku sa konkretizujú úlohy povinných osôb, vrátane zmenární kryptomien a spoločností poskytujúcich služby online kryptopeňaženiek, ktoré sú v súlade s predmetom svojej činnosti povinní podieľať sa na predchádzaní a odhaľovaní legalizácie príjmov z trestnej činnosti a financovania terorizmu. Nevyhnutnou podmienkou úspešného odhaľovania a vyšetrovania nelegálnych finančných transakcií v bitcoine a schopnosti ich odlíšenia od legitímnych transakcií, je pochopenie princípu ekosystému kryptomien. V poslednej časti príspevku autori poskytujú návody, postupy vyšetrovania a navrhujú využitie softvérových nástrojov, ktoré zvyšujú efektivitu pri vyšetrovaní bitcoin transakcií.
Kľúčové slová:
Bitcoin, BlockChain, Legalizácia príjmu z trestnej činnosti, Europol EC3, Financial Action Task Force (FATF), Informačná sieť finančných spravodajských jednotiek (FIU NET).

Abstract:
In the first part of the paper, the authors present the cryptocurrency users as well as their intended use. The paper is devoted to institutional protection against the illegal use of cryptocurrencies, specifically bitcoin, at both national and international levels. The authors constitute the legislative framework governing the procedure for the mutual exchange of information, making it available to authorized agencies and their responsible units. The paper specifies the roles of liable entities, including bitcoin exchange offices and online cryptowallet services, which are required to participate in the prevention and detection of money laundering and terrorist financing in line with their business. An essential prerequisite for the successful detection and investigation of illegal financial transactions in bitcoins and the ability to distinguish them from legitimate transactions is to understand the principle of the bitcoin ecosystem. In the last part of the paper, the authors provide guidance, investigation procedures and recommend the use of software tools, that increase the effectify of bitcoin investigation.
Keywords:
Bitcoin, BlockChain, Legalization of criminal income, Europol EC3, Financial Action Task Force (FATF), Financial Intelligence Units – FIU.NET.

Úvod

Bitcoin je digitálna decentralizovaná mena, ktorej hodnota je samoregulovaná najmä v závislosti od intenzity dopytu po nej. Protokol bitcoinu je otvorený, tzv. „peer to peer“[1] (zahŕňajúca zdieľanie súborov, alebo iných zdrojov po sieti medzi počítačmi navzájom, namiesto použitia centrálneho servera), umožňujúci nezvratné platby digitálnej meny z jednej kryptograficky podpísanej adresy na inú.

Okruh používateľov bitcoinu

Pseudoanonymný charakter bitcoin ekosystému je atraktívny pre rôzne skupiny používateľov. Jednou najväčších výhod je jeho nezávislosť od zásahov štátnych orgánov do realizovaných transakcií. Druhou je pseudoanonymita systému, t.j. vykonanie každej jednej transakcie je verejne publikované na blockchaine[2] (priebežne narastajúci zoznam záznamov, tzv. blokov, ktoré sú navzájom prepojené prostredníctvom šifrovacích algoritmov. Každý z blokov obsahuje kryptografický hash predchádzajúcich blokov, časovú značku a údaje

---

[1] CAMBRIDGE DICTIONARY. 2019. *Definition - Peer to peer*. [online]. [cit. 2019-05-14]. Dostupné na: <https://dictionary.cambridge.org/dictionary/english/peer-to-peer>

[2] ROSIC, A. 2016. *What is Blockchain Technology? A Step-by-Step Guide For Beginners.* [online]. [cit. 2019-05-14]. Dostupné na:<https://blockgeeks.com/guides/what-is-*blockchain-technology*/>

o transakcii), avšak identita používateľa, ktorému patrí bitcoin adresa[3], zostáva anonymná. Pseudoanynonymnú povahu systému využívajú napríklad aktivisti a lobistické skupiny pri uskutočňovaní prevodov. Burzoví špekulanti ťažia z výrazného kolísania kurzov bitcoinu. Priaznivci nových technológií oceňujú doteraz neexistujúce možnosti a funkcionality pri peňažných transakciách. Záujemcovia o negálny tovar, ako drogy, neregistrované zbrane, nelegálne služby, ako vykonanie počítačových útokov, zabezpečenie nástrojov na spáchanie trestných činov. V neposlednom rade je bitcoin, ako aj iné anonymizačné riešenia, využívaný hackermi pri prijímaní platieb, anonymných pripojeniach na vzdialené počítače a iné.

Zmenárne kryptomien predstavujú uzly, cez ktoré sú bitcoiny distribuované, slúžia na vloženie hotovosti do systému, výber hotovosti zo systému, alebo na prevod veľkých súm v ekosystéme bitcoinu.

Zmenárne sú kľúčovým partnerom orgánov činných v trestnom konaní pri zbere digitálnych dôkazov súvisiacich s platbami realizovanými prostredníctvom kryptomien. Pri otváraní účtu v zmenárni sú od zákazníka vyžiadané zvyčajne tri rôzne údaje potvrdzujúce jeho identitu. Ak zákazník využíva mobilnú aplikáciu, zmenáreň uchováva telefónne číslo, e-mailovú adresu, identifikačné číslo zariadenia, ako aj históriu transakcií peňaženky. V prípade, že okrem výmeny kryptomeny na FIAT menu[4] poskytuje zmenáreň aj možnosť vygenerovania a uloženia online peňaženky, zmenáreň chráni aj súkromný kľúč používateľa.

Zmenárne nepretržite monitorujú a hlásia podozrivé aktivity kompetentným dozorným orgánom. Napríklad v Spojených štátoch amerických je to Sieť na vyšetrovanie finančnej kriminality Ministerstva financií USA (angl. „ Financial Crimes Enforcement Network FinCEN, Department of Treasury).

Existencia jednotného trhu v Európskej únii, ktorá podporuje silnú hospodársku súťaž, ekonomickú prosperitu so sebou prináša aj negatívne aspekty v podobe voľného pohybu zločincov, teroristov, príjmov z trestnej činnosti a finančných zdrojov pre terorizmus. Aby bolo možné týmto hrozbám úspešne čeliť aj na Európskej úrovni, sa Finančné spravodajské jednotky Francúzska, Talianska, Luxemburgu a Spojeného kráľovstva pripojili v roku 2002 k vízii Holandskej finančnej spravodajskej jednotky vytvoriť Informačná sieť finančných spravodajských jednotiek. Legislatívnym základom bolo rozhodnutie Rady č. (2000/642/JHA)[5] Za účelom zníženia možnosti marenia vyšetrovacích úkonov sa v článku 5.4 uvedeného rozhodnutia stanovuje, že FIU „vykonajú všetky potrebné opatrenia vrátane bezpečnostných opatrení s cieľom zabezpečiť, aby informácie predložené podľa tohto rozhodnutia neboli prístupné žiadnym iným orgánom, agentúram alebo útvarom“ než tým, pre ktoré sú určené. FIU NET bol v januári 2016 bol FIU.net začlenený do Europolu. Tento krok zlepšil výmenu finančných informácií dostupných prostredníctvom tejto siete, aj vďaka kombinácii s produktmi a službami Europolu. Vytvorením väčšej synergie medzi finančnou a kriminálnou spravodajskou službou FIU.net v konečnom dôsledku zvyšuje úsilie v boji proti organizovanému zločinu a terorizmu v EÚ.[6]

Nezastupiteľné miesto pri koordinácii opatrení na boj proti legalizácii a financovaniu terorizmu má aj Financial Action Task Force. Bola založená v roku 1989 z iniciatívy štátov G7 v Paríži s cieľom stanoviť normy a podporiť účinné vykonávanie regulačných a právnych

---

[3] UJVÁRY, K. Zneužitie kryptomien na pranie špinavých peňazí a základné metódy jeho vyšetrovania, In *Organizovaný zločin v stredoeurópskom regióne - trendy a výzvy*: zborník príspevkov z medzinárodnej vedeckej konferencie, Bratislava, 2017.

[4] Fiat peniaze. 2017. [online]. [cit. 2019-05-19]. Dostupné na:<http://www.financnytrh.com/definicia-pojmu-fiat-peniaze/>

[5] Rozhodnutie Rady č. (2000/642/JHA) z 17 októbra 2000 upravujúce spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov.

[6] Informačná sieť finančných spravodajských jednotiek. 2018. [online]. [cit. 2019-05-19]. Dostupné na:<https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net>

opatrení zameraných na boj proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu a ďalším ohrozeniam integrity medzinárodného finančného systému. [7]

Ochrana pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu prostredníctvom bitcoinu v Slovenskej republike.

Na území Slovenskej republiky sú bitcoin a ostatné kryptomeny čoraz častejšie používaným platobným a investičným prostriedkom. Vzhľadom na túto skutočnosť je potrebné mať na zreteli aj možnosti zneužitia digitálnych mien páchanie trestnej činnosti. Vo všeobecnosti ochranu pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu tvoria tri vertikálne roviny, a to:

- povinné osoby,
- finančná spravodajská jednotka,
- orgány činné v trestnom konaní.

Povinné osoby sa musia v súlade s predmetom svojej činnosti podieľať na predchádzaní a odhaľovaní legalizácie príjmov z trestnej činnosti a financovania terorizmu.

Hlásenie podozrivých finančných transakcií je legislatívne upravené v § 14 ods. 2 písm. b) zákona č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu.[8] Toto ustanovenie zaväzuje všetky povinné osoby[9] venovať zvýšenú pozornosť transakciám v súvislosti s nákupom a predajom virtuálnej meny a akúkoľvek neobvyklú obchodnú operáciu bezodkladne hlásiť finančnej spravodajskej jednotke národnej kriminálnej agentúry, ktorá je prioritne zameraná na prijímanie, evidovanie, analýzu, vyhodnocovanie a spracovávanie hlásení o neobvyklých obchodných operáciách.[10] Je potrebné, už na začiatku efektívne indikovať možné prípady páchania tejto trestnej činnosti. Na to je nevyhnutný prístup založený na zá kladnej filozofii „poznaj svojho klienta“. Cieľom tejto filozofie je:

- zvýšiť dodržiavanie a plnenie všetkých nariadení a zákonov, ale aj všeobecne zaužívaných praktík,
- znížiť pravdepodobnosť, aby sa povinná osoba stala obeťou protizákon-ných aktivít páchaných jej klientmi,
- ochrániť dobrú povesť povinnej osoby,
- zabrániť narušeniu vzťahov povinnej osoby s dobrými klientmi,
- zvýšiť pravdepodobnosť odhalenia aktivít klienta vymykajúcich sa jeho doterajším zvyklostiam a obchodnej činnosti.

Cieľom posudzovania pripravovaných a realizovaných obchodných operácií je rozpoznať neobvyklé obchodné operácie, ktoré povinné osoby hlásia konkrétnemu zákonom určenému subjektu.

Zmenáreň kryptomien, je povinnou osobou v zmysle § 5 ods. (1) písm. b) bodu 14 Zákona č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu ako „*platobná inštitúcia, agent platobných služieb a inštitúcia elektronických peňazí"*. Rozsah zoznamu povinných osôb zodpovedá smernici Európskeho

[7] Financial Action Task Force, FATF. [online]. [cit. 2019-05-20]. Dostupné na:<https://www.fatf-gafi.org/about/>

[8] Zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (ďalej len „preventívny zákon“).

[9] Povinná osoba, Definícia, § 5 Zákona č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[10] Finančná spravodajská jednotka. [online]. [cit. 2019-05-20]. Dostupné na:<https://www.minv.sk/?financna-policia>

parlamentu a Rady EÚ 2015/849.[11] V zmysle § 86 Zákona č. 492/2009 o platobných službách a o zmene a doplnení niektorých zákonov[12] podlieha činnosť inštitúcie elektronických peňazí dohľadu, ktorý vykonáva Národná banka Slovenska. Na efektívne predchádzanie a odhaľovanie prípadov legalizácie príjmov z trestnej činnosti a financovania terorizmu majú povinné osoby zákonom č. 297/2008 Z. z. uložené povinnosti, a to najmä:

- vykonávať identifikáciu a overenie identifikácie klienta,
- identifikovať, hodnotiť, aktualizovať a riadiť riziká legalizácie a financo-vania terorizmu,
- určiť rozsah starostlivosti a jej vykonávanie (základnej, zjednodušenej alebo zvýšenej) vo vzťahu ku klientovi v závislosti od rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu,
- posudzovať obchodné operácie a zisťovať neobvyklé obchodné operácie,
- odmietnuť vykonanie obchodu alebo uzatvorenie obchodného vzťahu,
- zdržať neobvyklú obchodnú operáciu,
- ohlásiť neobvyklú obchodnú operáciu,
- dodržiavať mlčanlivosť,
- spracovávať a uchovávať údaje,
- písomne vypracovať program vlastnej činnosti zameranej proti legalizá-cii príjmov z trestnej činnosti a financovaniu terorizmu,
- poskytovať súčinnosť finančnej spravodajskej jednotke.[13]

NBS je v prípade zistenia nedostatkov v činnosti inštitúcie elektronických peňazí spočívajúcich v nedodržaní podmienok určených v povolení, podmienok alebo povinností vyplývajúcich z iných rozhodnutí Národnej banky Slovenska uložených inštitúcii elektronických peňazí, v nedodržiavaní alebo v obchádzaní ustanovení tohto zákona, právne záväzných aktov Európskej únie vzťahujúcich sa na vydávanie elektronických peňazí, osobitných zákonov alebo iných všeobecne záväzných právnych predpisov, ktoré sa vzťahujú na vydávanie elektronických peňazí, oprávnená v zmysle odseku §86 (2) tohto zákona uplatňovať voči inštitúcii elektronických peňazí sankcie.

Finančná spravodajská jednotka, Predstavuje centrálny orgán, ktorý prijíma, eviduje, ana-lyzuje a využíva ohlásené neobvyklé obchodné operácie od povinných osôb.[14] Finančná spravodajská jednotka je podľa medzinárodnej organizácie na boj proti praniu špinavých peňazí – EGMONT GROUP[15] definovaná ako: centrálna národná agentúra zodpovedná za prijímanie, analyzovanie vyhodnocovanie a spracúvanie finančných informácií týkajúcich sa podozrivých príjmov z trestnej činnosti alebo je poverená národnou legislatívou pre oblasť boja proti legalizácii príjmov z trestnej činnosti.[16] Policajti finančnej spravodajskej jednotky sú po prijatí hlásenia o NOO oprávnení využívať aj ďalšie oprávnenia, ktoré im dáva zákon č. 297/2008 Z. z., a to:

- zdržať neobvyklú obchodnú operáciu[17],

---

[11] Smernica Európskeho parlamentu a Rady EÚ 2015/849.o predchádzaní využívania finančného systému na účely prania špinavých peňazí alebo financovania terorizmu.

[12] Zákon č. č. 492/2009 o platobných službách a o zmene a doplnení niektorých zákonov.

[13] STIERANKA, J. a kol. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu*. Právna a inštitucionálna ochrana v SR, s. 125.

[14] STIERANKA, J., ČENTÉŠ, J. *Právne a inštitucionálne aspekty v boji proti legalizácii príjmov z trestnej činnosti ako integrálnej súčasti organizovanej kriminality*. Záverečná správa z vedeckovýskumnej úlohy. Bratislava: Akadémia Policajného zboru, 2010. s. 82.

[15] EGMONT GROUP. [online]. [cit. 2019-05-20]. Dostupné na:<https://egmontgroup.org/en>

[16] Ustanovenie § 26 ods. 2 písm. a) zákona č. 297/2008 Z. z.

[17] Ustanovenie § 16 zákona č. 297/2008 Z. z.

- žiadať doplňujúce informácie k hláseniu o neobvyklej obchodnej operácii a súvisiace doklady o neobvyklej obchodnej operácii[18]

Z iniciatívy skupiny EGMONT, Interpolu, Europolu sa organizujú stretnutia pracovnej skupiny kryptomien, kde si zástupcovia finančných spravodajských jednotiek, OČTK a súkromného sektora vymieňajú technické zručnosti a skúsenosti v spojitosti s kryptomenami. Stretnutia pracovnej skupiny prispievajú k zvýšeniu informačnej výmeny na poli legalizácie príjmu z trestnej šinnosti a digitálnych mien použitím kanálov ako napríklad Europol, Interpol, Egmont Group a FIU.net. Pripravujú sa návrhy regulácie digitálnych zmenární a poskytovateľov digitálnych peňaženiek, ako aj definície konceptov kryptomien, zmenární kryptomien, poskytovateľov peňaženiek, zmiešavacích služieb kryptomien za účelom zahrnutia do právneho rámca európskej legislatívy. Pracovná skupina má taktiež za cieľ prijať preventívne opatrenia s cieľom zamedziť poskytovaniu služieb zmiešavačov kryptomien, keďže predstavujú prekážku pri odhaľovaní a vyšetrovaní podozrivých transakcií.[19]

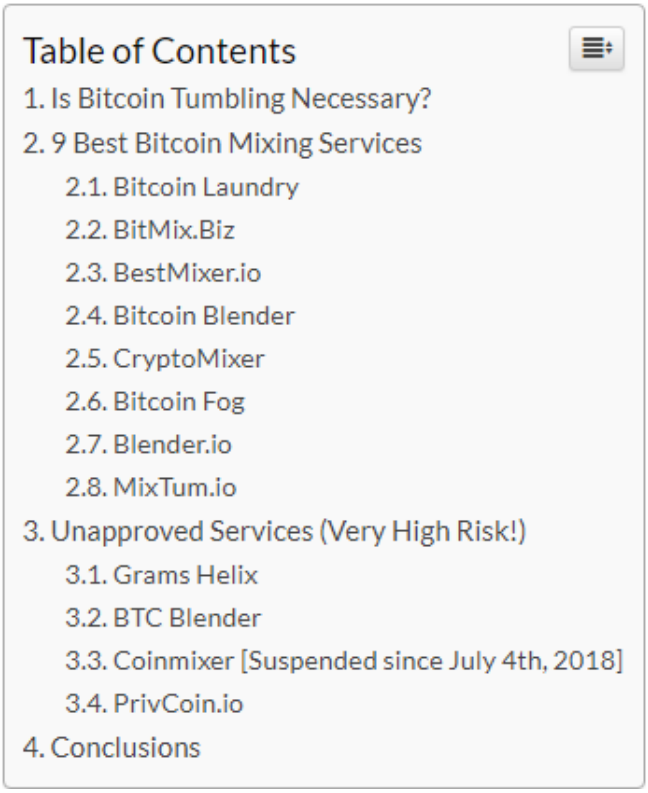


Table of Contents

1. Is Bitcoin Tumbling Necessary?
2. 9 Best Bitcoin Mixing Services
   - 2.1. Bitcoin Laundry
   - 2.2. BitMix.Biz
   - 2.3. BestMixer.io
   - 2.4. Bitcoin Blender
   - 2.5. CryptoMixer
   - 2.6. Bitcoin Fog
   - 2.7. Blender.io
   - 2.8. MixTum.io
3. Unapproved Services (Very High Risk!)
   - 3.1. Grams Helix
   - 3.2. BTC Blender
   - 3.3. Coinmixer [Suspended since July 4th, 2018]
   - 3.4. PrivCoin.io
4. Conclusions

Obr. 1: Table of Contents
Zdroj: https://cryptalker.com/best-bitcoin-tumbler/

Po analýze neobvyklých obchodných operácií u povinnej osoby má FSJ nasledovné možnosti využitia hlásení:

[18] Ustanovenie § 17 zákona č. 297/2008 Z. z.
[19] UJVÁRY, K. Zneužitie kryptomien na pranie špinavých peňazí a základné metódy jeho vyšetrovania, In *Organizovaný zločin v stredoeurópskom regióne - trendy a výzvy: Zborník príspevkov z medzinárodnej vedeckej konferencie*, Bratislava, 2017.

a) odstúpiť vec orgánom činným v trestnom konaní[20], ak výsledky vykonanej analýzy nadobudnú taký charakter, že je možné vyvodiť záver o dôvodnom podozrení zo spáchania konkrétneho trestného činu.
b) odovzdať podklady prí slušnému orgánu činnému v trestnom konaní do prebiehajúceho trestného konania do prebiehajúceho trestného konania, ak sa vykonanou analýzou zistí, že k získaným poznatkom je vedené trestné konanie na niektorom úrade kriminálnej polície alebo Kriminálnom úrade Finančnej správy.
c) postúpiť podklady iným útvarom Policajného zboru [21], najmä službe kriminálnej alebo finančnej polície, ak sa vykonanou analýzou zistí, že informácie získané ohlasovacou povinnosťou sa viažu k osobe alebo osobám, ktoré tieto súčasti PZ preverujú z dôvodu podozrenia páchania inej trestnej činnosti spadajúcej do ich kompetencie.
d) postúpiť podklady prí slušným orgánom členských štátov Európskej únie, a to rešpektujúc medzinárodné zmluvy, ktorými je Slovenská republika viazaná, ak sa vykonanou analýzou zistí, že získané poznatky ku konaniu majú medzinárodný prvok a iný oprávnený orgán iného členského štátu vedie trestné konanie alebo k tomuto konaniu vykonáva iné šetrenie.

Finančnej spravodajskej jednotke je zo zákona č. 297/2008 Z. z. uložená povinnosť vykonávať kontrolu plnenia a dodržiavania povinností povinných osôb, podávať podnety na uloženie pokuty povinnej osobe, podávať podnety na odobranie oprávnenia na zárobkovú činnosť povinnej osobe, atď[22]. Kontrolu môže vykonávať po vzájomnej dohode aj spoločne s Národnou bankou Slovenska alebo ministerstvom financií u tých povinných osôb, ktoré podliehajú ich dohľadu alebo kontrole.

Princíp bitcoin transakcií

Prevod bitcoinu vyžaduje existenciu kľúčového páru, t.j. súkromného a verejného kľúča. Adresa bitcoinu sa skladá z reťazca 27 až 34 alfanumerických znakov, začínajúcich číslicami 1 alebo 3.

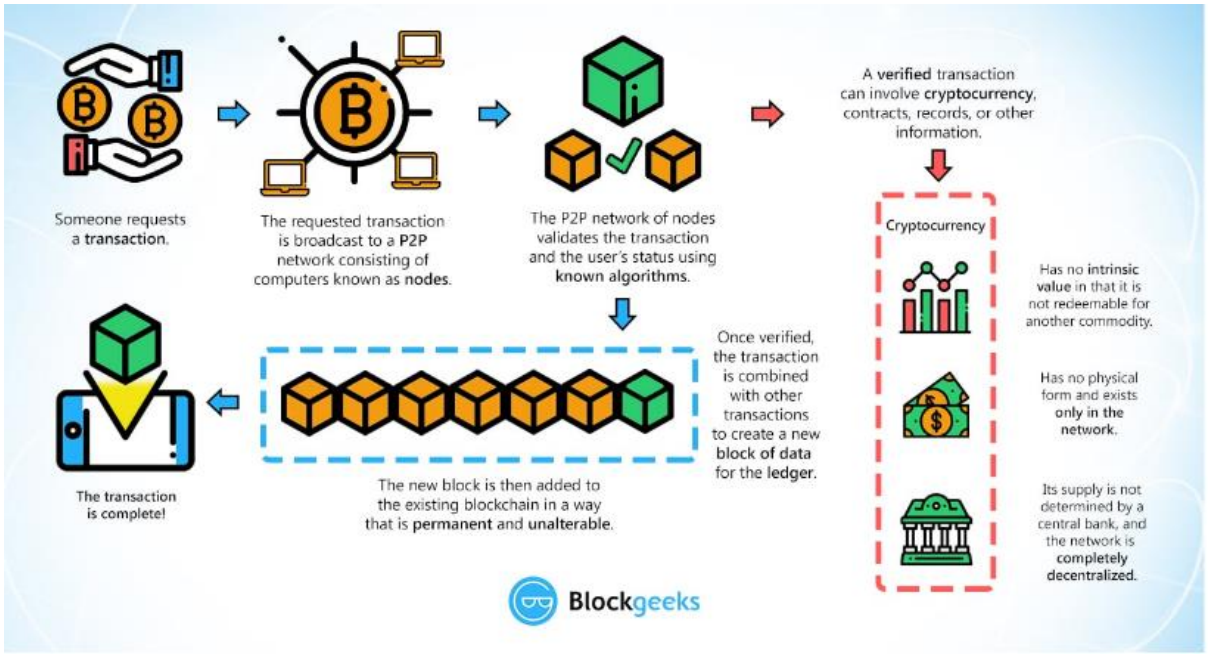
Najmenší fragment bitcoinu definovaný v bitcoin protokole je jeden Satoshi, ktorý predstavuje jednu stomiliónti bitcoinu ,t.j. 1 SATOSHI = 0.00000001 BTC[23]. Keď sa uskutočňuje transakcia určitej sumy v bitcoinoch, výdavok musí byť zaslaný na bitcoin adresu, keďže na rozdiel od platieb v klasických, štátmi riadených, tzv. FIAT menách, neexistuje okrem prevodu iný spôsob na rozdielenie bitcoinu. Z uvedeného vyplýva, že každý prevod časti bitcoinu predpokladá existenciu adresy odosielateľa, adresy prijímateľa, a adresy, na ktorú system pošle výdavok pre odosielateľa. Používateľ pošle dohodnutú sumu príjemcovi a adresu pre zaslanie výdavku.

Údaje o transakcii sú „zahashované“ hodnota hashu je vložená do bloku. Blok je následne pridaný do blockchainu a potvrdený “minermi”. Každá validovaná transakcia nesie so sebou aj informácie o bitcoin adrese odosielateľa aj prijímateľa, počet bitcoinov, datum a čas vykonania transakcie, ako aj poplatok za transakciu. Dáta o transakcii sú reprezentované tzv. “stromom Merkle”. V ľudskej reči je potom transakcia interpretovateľná nasledovne:

Ja (reprezentovaný verejne známou adresou), posielam Prijímateľovi (reprezentovaný verejne známou adresou) XXX BTC, ktoré mám z výpočtovo-dokázanej transakcie dňa DD.MM.RRRR o hh:mm:ss, spolu s poplatkom 0,0001 násobku prevádzanej sumy.

[20] Ustanovenie § 26 ods. 2 písm. b) zákona č. 297/2008 Z. z.
[21] Ustanovenie § 26 ods. 2 písm. l) zákona č. 297/2008 Z. z.
[22] Ustanovenie § 26 ods. 2 písm. c), d), e) zákona č. 297/2008 Z. z.
[23] Konvertor Satoshi a BTC. [online]. [cit. 2019-05-20]. Dostupné na:<http://satoshitobitcoin.co/>

Adresa výdavku na strane odosielateľa je jedným z najdôležitejších zdrojov informácií pre vyšetrovateľa v prípadoch vyšetrovania ekonomickej a finančnej trestnej činnosti. Často je prvým krokom pri výkone vyšetrovacích úkonov na blockchaine.



Obr. 2: Princíp bitcoin transakcie
Zdroj: https://blockgeeks.com/guides/what-is-blockchain-technology/

Výhodou blockchainu je aj jeho odolnosť voči zmene údajov v ňom. Keďže ide o otvorenú technológiu, ktorá dokáže efektívne a overiteľným a trvalým spôsobom zaznamenávať transakcie medzi dvoma stranami. Aby mohol vyšetrovateľ úspešne sledovať platby bitcoinom, je nevyhnutné, aby mal aspoň základné kryptografické znalosti, aby chápal reťazenie binárnych hashov. Bez týchto znalostí je aj napriek možnosti použitia sofistikovaných analytických nástrojov pravdepodobnosť identifikácie platby a prepojenia medzi bitcoin adresami, ako aj ich majiteľmi minimálna.

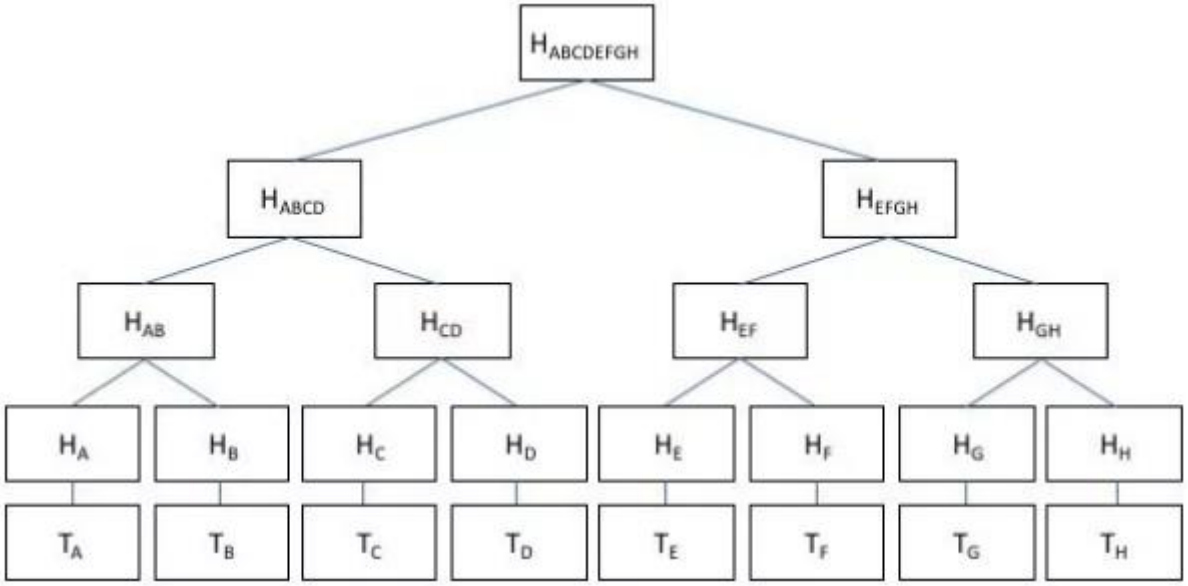
Strom Merkle – princíp efektívneho a bezpečného kódovania dát v blockchaine[24]

Strom Merkle je spomínaný aj ako strom binárneho hashu. Bitcoin blockchain používa Merklov strom na uloženie transakcií v každom bloku, umožňujúce zjednodušené overenie platieb, kde umožňuje stiahnuť reťazec záhlavia blokov, obsahujúci hash predchádzajúcej hlavičky, časové razítko, hodnotu obtiažnosti ťažby , work nonce (cieľ ťažby kryptomeny: nájsť nonce – centrálnu časť proof of work, ktorý vytvorí hash s hodnotou menšou alebo rovnou, ako je nastavená sieťou. Ak ťažiar nájde taký nonce, nazývaný tiež "zlatý nonce", môže takýto blok pridať do blockchainu a získať odmenu vo výške alikvotnej časti v bitcoinoch) a koreňový hash pre strom Merkle obsahujúci transakcie pre daný blok. Nonce je uložený v hlavičke bloku, jeho vložením vytvára v hlavičke bloku nový hash. Hash musí začínať veľkým počtom núl. Ak

[24] MERKLE, R. C. A digital signature based on a conventional encryption function, Advances in Cryptology - CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques, p. 369-378, Santa Barbara, California, USA, August 16-20, 1987, Proceedings, International Association for Cryptologic Research, Elxsi, 2334 Lundy Place, San Jose, CA 951 31.

ich nemá, ťažiar ho zahodí, zoberie nové nonce a generuje nový hash až dovtedy, kým je výsledkom výpočtu hash s hodnotou menšou alebo rovnou ako je nastavená náročnosť. [25]

Na obrázku predstavuje "T" transakciu a "H" hash. Obrázok je demonštračný, v skutočnosti obsahuje priemerný blok vyše 500 transakcií.



Obr. 3: Strom Merkle
Zdroj: Merkle Tree, https://www.investopedia.com/terms/m/merkle-tree.asp

Hashe v spodnom riadku sú označované ako „listy", medziľahlé ako „vetvy", a hash na vrchu ako „koreň". Koreň Merkle daného bloku je uložený v hlavičke. Strom Merkle umožňuje používateľom overiť si konkrétnu transakciu bez toho, aby si stiahli celý blockchain.

Základné ukazovatele podozrivých bitcoin transakcií

Existuje niekoľko spôsobom vyšetrovania, akými je možné identifikovať majiteľa účtu bitcoin. V Blockchaine je zobrazený aspoň jeden vstup a nula alebo viac výstupov pre každú transakciu. Výdavok je zriedkavo zasielaný na pôvodnú adresu. Používatelia môžu mať vygenerovaných veľa adries, dokonca pre každú transakciu môžu mať vygenerovanú novú adresu. Podozrivé transakcie sú v niektorých prípadoch rozpoznateľné pri pohľade na vstupnú, výstupnú adresu a časovú pečiatku transakcie. Napríklad viacvstupové transakcie odhalia, že predchádzajúce vstupy bol i pod kontrolou toho istého vlastníka. Táto transakcia môže byť potom prepojená na iné transakcie , ktoré môžu ustáliť vlastníka kľúča. Podobne, opakované použitie jednej adresy pre viaceré transakcie môže naznačovať, že tá istá osoba používa okrem tejto adresy aj všetky ostatné v tejto transakcii. Konkrétne, za predpokladu, že aj „A" aj „B" sú vstupy do jednej transakcie a „A" aj „C" sú vstupy do druhej transakcie vyplýva, že „A", „B" aj „C" sú pod kontrolou toho istého používateľa.

Množiny bitcoin adries je možné priradiť k jednému regulátorovi, akými sú napríklad služby peňaženiek. Niektoré verejné adresy sú zbierané a označované tretími stranami, alebo používateľskými fórami, čo uľahčuje ich identifikáciu. Používateľ môže transakciu realizovať prostredníctvom QR kódu priradeného k verejnej adrese, využijúc pohodlie platby

[25] Nonce a Proof of Work. [online]. [cit. 2019-05-20]. Dostupné na:<https://coincentral.com/what-is-a-nonce-proof-of-work/>

prostredníctvom mobilných zariadení. Existuje množstvo aplikácií, ako „tumblery“, „mixery“ a „scrumblery“ a „práčovne kryptomien“, ktoré vytváraním veľkých dávok adries anonymizujú transakcie na vstupe. V podstate sú umelo vygenerované adresy vložené medzi legitímne adresy za účelom ochrany príjemcu, alebo za účelom preprania transakcií. [26]Generovanie dávok bitcoin adries nemusí byť nevyhnutne nezákonné, môže slúžiť aj na legitímny účel, napríklad keď webové stránky elektronického obchodu priradia jedinečnú , vopred vygenerovanú adresu každému zákazníkovi, ktorý si za službu alebo tovar vyberie platbu bitcoinom.

Sledovanie bitcoinovej transakcie na blockchaine

Zoberme si napríklad, že výjazdový tím nájde na mieste činu ústrižok s bitcoin adresou , napr.: “15G8SagsD2JqWUpBsIIfcVuvyrQwX3Lq1e.” Prioritne sa v takomto prípade prehľadáva blockchain s cieľom nájsť všetky transakcie spojené s týmto verejným kľúčom, so zreteľom na presný počet odoslaných bitcoinov, dátum a čas odoslania a adresáta. Skúmanie blockchainu a sledovanie toku transakcií späť k známej spoločnosti, alebo majiteľovi konkrétnej bitcoin peňaženky je kľúčom k identifikácií konkrétneho používateľa. Údaje blockchainu sú je možné prehliadať prostredníctvom rôznych web stránok, ktoré poskytujú nasledovné údaje:

- zoznam posledných blokov v blockchaine,
- aktuálne transakcie v konkrétnom bloku,
- odkazy na predchádzajúcu a nasledovnú transakciu zah´ňajúci každý vstup aj výstup,
- zoznam všetkých transakcií zahŕňajúcich konkrétnu adresu, vrátane aktuálneho stavu a historických stavov adresy (balance)
- všetky správy súvisiace s poskytovanou službou k uskutočnenej transakcii.

Ak používateľ vykoná bitcoin transakciu (v tomto prípade nákup) prostredníctvom web stránky, tak je obyčajne IP adresa používateľaa zachytená v logoch a je vystopovateľná. Poskytovateľ internetových služieb používateľa je potenciálne schopný prečítať adresu prislúchajúcu k transakcii, a to prostredníctvom dátumu a času tansakcie zachyteného v blockchaine. V prípade vyšetrovania podozrivej bitcoin transakcie je potrebné identifikovať poskytovateľa internetových služieb (angl. ISP[27]). Dožiadanie vo väčšine prípadov obsahuje dotaz na všetky bitcoin adresy, informácie z log súborov zachytených v rovnakom čase, alebo čase s nepatrou ochýlkou od času transakcie, všetky alfanumerické reťazce, ktoré by mohli byť hashovými hodnotami bitcoin transakcií, alebo súkrmonými kľúčami k bitcoin peňaženke.

Využitie údajov poskytnutých zmenárňami pre vyšetrovanie

Zmenárne kryptomien sú kľúčovými zdrojmi informácií pre vyšetrovanie. Zmenárne bitcoinu obvykle disponujú informáciami, ako emailová adresa, meno a priezvisko, IP adresa, číslo bankového účtu používateľa služby zmenárne. Ked je vykonaná transakcia bitcoinov do zmenárne, vstupná bitcoin adresa je známa, a priamy tok podozrivej transakcie smeruje do zmenárne, môže byť zaslené dožiadanie zaslané do zmenárne. Ak používateľ zamieňa bitcoin za FIAT menu, zaznamenáva sa IP adresa používateľa, zachytávú sa dáta prenášané sieťou. Zmenáreň môže korelovať dve rôzne transakcie, v ktorých sa vyskytuje tá istá bitcoin

[26] UJVÁRY, K. Zneužitie kryptomien na pranie špinavých peňazí a základné metódy jeho vyšetrovania, In *Organizovaný zločin v stredoeurópskom regióne - trendy a výzvy: Zborník príspevkov z medzinárodnej vedeckej konferencie,* Bratislava, 2017.

[27] ISP – Internet Service Provider, je organizácia, ktorá poskytuje služby pre prístup, používanie internetu.

adresa. Používateľ môže anonymizačné technológie ako VPN[28] alebo TOR[29], ktoré síce sťažujú, ale úplne neznemožňujú identifikáciu používateľa. Pri vyšetrovaní sa väčšinou spolieha na znížení obozretnosť a neopatrnosť používateľa, ktorý môže použiť používateľské mená opakovane, ktoré môžu byť identifikované počas manuálneho, alebo automatizovaného vyhľadávania. Pri vyšetrovaní môže pomôcť aj vyplneé poznámkové pole, pretože mnoho používateľov verí v ilúziu úplnej anonymity svojich transakcií, preto nie je vylúčené, že pripoja sprievodnú informáciu k svojim transakciám, čo môže následne vyšetrovateľ použiť ako digitálny dôkaz.

Zoznam použitej literatúry

1. MERKLE, R. C. *A digital signature based on a conventional encryption function, Advances in Cryptology - CRYPTO '87*. A Conference on the Theory and Applications of Cryptographic Techniques, p. 369-378, Santa Barbara, California, USA, August 16-20, 1987, Proceedings, International Association for Cryptologic Research, Elxsi, 2334 Lundy Place, San Jose, CA 951 31.
2. STIERANKA, J. a kol. *Legalizácia príjmov z trestnej činnosti a financovanie terorizmu, Právna a inštitucionálna ochrana v SR*. Wolters Kluwer, 2013. ISBN 978-80-8168-913-0.
3. STIERANKA, J., ČENTÉŠ, J. *Právne a inštitucionálne aspekty v boji proti legalizácii príjmov z trestnej činnosti ako integrálnej súčasti organizovanej kriminality*. Záverečná správa z vedeckovýskumnej úlohy. Bratislava: Akadémia Policajného zboru, 2010.
4. UJVÁRY, K. Zneužitie kryptomien na pranie špinavých peňazí a základné metódy jeho vyšetrovania. In *Organizovaný zločin v stredoeurópskom regióne - trendy a výzvy*. Zborník príspevkov z medzinárodnej vedeckej konferencie, Bratislava : Akadémia Policajného zboru v Bratislave, 2017. s. 188-195. ISBN 978-80-8054-720-2.
5. Rozhodnutie Rady č . (2000/642/JHA) z 17 októbra 2000 upravujúce spoluprácu pri výmene informácií medzi finančnými informačnými jednotkami členských štátov.
6. Smernica Európskeho parlamentu a Rady EÚ 2015/849 o predchádzaní využívania finančného systému na účely prania špinavých peňazí alebo financovania terorizmu.
7. Zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.
8. Zákon č. č. 492/2009 o platobných službách a o zmene a doplnení niektorých zákonov.
9. BlockChain. [online]. [cit. 2019-05-14]. Dostupné na: <https://blockgeeks.com/guides/what-is-blockchain-technology/>
10. Ciphertrace. [online]. [cit. 2019-06-10]. Dostupné na:<https://ciphertrace.com/financial-investigations-and-blockchain-forensics/>
11. EGMONT GROUP. [online]. [cit. 2019-05-19]. Dostupné na: <https://egmontgroup.org/en>
12. Financial Action Task Force, FATF. [online]. [cit. 2019-05-20]. Dostupné na:<https://www.fatf-gafi.org/about/>
13. Fiat peniaze. [online]. [cit. 2019-06-03]. Dostupné na:<http://www.financnytrh.com/definicia-pojmu-fiat-peniaze/>
14. Finančná spravodajská jednotka. [online]. [cit. 2019-05-16]. Dostupné na: <https://www.minv.sk/?financna-policia>

[28] VPN, Virtual Private Network, Rozširuje súkromnú sieť cez verejnú sieť a umožňuje používateľom odosielať a prijímať údaje v rámci zdieľaných alebo verejných sietí, ako keby boli zariadenia priamo pripojené k súkromnej sieti. [online]. [cit. 2019-06-10]. Dostupné na:<https://en.wikipedia.org/wiki/Virtual_private_network>

[29] TOR, Smeruje internetovú prevádzku cez sieť dobrovoľníkov, aby zakryla polohu a činnosť používateľa a znemožnila monitorovanie siete aanalýzu dátového prenosu. [online]. [cit. 2019-06-10]. Dostupné na:<https://www.torproject.org/>

15. Informačná sieť finančných spravodajských jednotiek. [online]. [cit. 2019-05-16]. Dostupné na: <https://www.europol.europa.eu/about-europol/financial-intelligence-units-fiu-net>
16. Konvertor Satoshi a BTC. [online]. [cit. 2019-05-14]. Dostupné na: <http://satoshitobitcoin.co/>
17. NEUTRINO. [online]. [cit. 2019-06-10]. Dostupné na:<https://www.neutrino.nu/>
18. Nonce a Proof of Work. [online]. [cit. 2019-06-05]. Dostupné na: <https://coincentral.com/what-is-a-nonce-proof-of-work/>
19. Peer to peer. [online]. [cit. 2019-05-14]. Dostupné na: <https://dictionary.cambridge.org/dictionary/english/peer-to-peer>
20. TOR - Smeruje internetovú prevádzku cez sieť dobrovoľníkov, aby zakryla polohu a činnosť používateľa a znemožnila monitorovanie siete analýzu dátového prenosu. [online]. [cit. 2019-06-10]. Dostupné na:<https://www.torproject.org/>
21. Virtual Private Network. [online]. [cit. 2019-06-10]. Dostupné na:<https://en.wikipedia.org/wiki/Virtual_private_network>

Kontaktné údaje:
RNDr. Kristián Ujváry
Ministerstvo vnútra SR
kristian.ujvary@minv.sk

Mgr. Jana Kuchtová
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
jana.kuchtova@minv.sk

Využitie znakov digitálnej stopy pri riešení problematiky blockchain

Štefan Zachar

Abstrakt:
Autor príspevku má v úmysle vysvetliť problematiku technológie blokchain v kontexte digitálnych stôp. V rámci príspevku objasňuje aplikovateľnosť všeobecne definovaných špecifík digitálnych stôp na jednotlivé funkcie a vlastnosti technológie blockchain.
Kľúčové slová:
Blockchain, kryptomena, digitálna stopa, ,hash algoritmus, konsenzus.

Abstract:
Author of this article intends to explain the issue of blockchain technology in context with digital evidences. The article describes applicability ordinary defined specifications of digital evidences in functions and properties blockchain technology
Key words:
Blockchain, cryptocurrency, digital evidence, hash algorithm, consensus.

Blockchain v kyberpriestore

Kybernetický priestor sa neustále zväčšuje a s ním narastá aj miera zločinov páchaných jeho prostredníctvom alebo priamo v jeho prostredí. Súčasťou kyberpriestoru sú aj služby založené na technológii blockchain ako sú napríklad:

- kryptomeny, ktoré môžu byť cieľom páchania trestnej činnosti, alebo jej platidlom,
- databázy verejnej alebo štátnej správy,
- databázy poskytujúce služby v súkromnom sektore.

V súvislosti s uvedeným, je potrebné zamyslieť sa nad možnosťami evidencie digitálnych stôp v technológii blockchain.

Rozšírenie problematiky blockchain v informačných technológiách je sprievodným javom expanzie kryptomien vo svete. Blockchain ako technológia bol definovaný už pred zavedením prvej kryptomeny, avšak do popredia sa dostal hlavne svojím využitím ako účtovnej knihy pre kryptomenu Bitcoin. V súčastnosti je technológia blockchain využívaná v širokom spektre aplikácií a služieb.

Blockchain a špecifiká digitálnych stôp v odbornej literatúre

V kontexte technológie blockchain, sa môžeme na problematiku digitálnych stôp pozrieť ako na informáciu uloženú v prostredí tejto technológie. Touto informáciou môže byť finančná transakcia, elektronický dokument či informácia s multimediálnym obsahom. Digitálne stopy majú určité špecifiká, ktoré sú definované v odbornej literatúre.

„Špecifiká digitálnych stôp[1]*:*

- *Nehmotnosť digitálnych stôp,*
- *Latentnosť digitálnych stôp,*
- *Časová trasovateľnosť digitálnych stôp,*
- *Vysoká obsažnosť digitálnych stôp,*
- *Veľmi nízka životnosť digitálnych stôp,*
- *Uchovávanie a kvalita digitálnych stôp je ovplyvnená radom subjektívnych faktorov,*
- *Veľký dátový objem digitálnych stôp,*

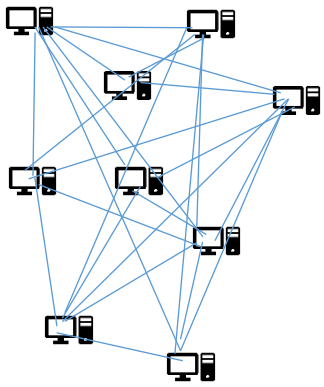
[1] METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej criminality*. Akadémia PZ SR v Bratislave, 2004. s. 168.

- *Dátová hustota digitálnych stôp, v čase a s rozvojom nových technológií neustále klesá,*
- *Extrémna dynamickosť prostredia digitálnych stôp,*
- *Heterogénnosť a komplexnosť prostredia digitálnych stôp,*
- *Veľký geografický rozsah priestoru s digitálnymi stopami,*
- *Vysoký stupeň ochrany dát sťažuje alebo znemožňuje prácu s digitálnymi stopami,*
- *Digitálna stopa je špecializovanými prostriedkami automaticky identifikovaná a spracovateľná,*
- *Vysoká úroveň zahladzovania digitálnych stôp, kvalifikovanými páchateľmi,*
- *Reštaurovateľnosť zničených digitálnych stôp,*
- *Originálnosť digitálnych stôp,*
- *Súčasne nízka úroveň súdnej akceptácie digitálnych stôp v právnej praxi.“*

Nakoľko blockchain je distribuovaná databáza, nemôžeme k nemu pristupovať ako ku klasickému hmotnému médiu určenému na ukladanie údajov. S tým sú spojené aj možné rozdiely medzi všeobecnými špecifikami digitálnych stôp a špecifikami digitálnych stôp v súvislosti s technológiou blockchain. Komparáciou vlastností definovaných v jednotlivých špecifikách budeme hľadať spoločné alebo rozdielne prvky. Výsledkom bude porovnanie súboru špecifík určených na popisovanie digitálnych stôp v súvislosti s technológiou blockchain. Pre jednoduchosť, špecifiká ktoré vykazujú určitú podobnosť v zlúčime do skupín.

Nehmotnosť digitálnych stôp

Informácie vo forme dát sú nehmotné[2] avšak na svoju existenciu potrebujú hmotné médium, v ktorom sú uložené. Blochchain nie je hmotné médium, ale technológia, využívajúca hmotné médiá. Ak používateľ vloží informáciu do blockchainu, z pohľadu používateľa sa javí ako jedinečný záznam v databáze. Z pohľadu technológie však tento záznam existuje ako niekoľkonásobná identická kópia, kde počet týchto kópií sa rovná počtu uzlov v počítačovej sieti vytvárajúcej blockchain. Z tohto dôvodu pracovník skúmajúci informácie uložené v blockchaine nepotrebuje aby bol zaistený fyzicky konkrétny hardvér, stačí mu prístup do konkrétneho blockchainu. Výnimku môžu tvoriť krypto-peňaženky určené na „uloženie krypto mincí“. V skutočnosti však obsahujú personálne šifrovacie kľúče, ktoré sprístupňujú tie záznamy v blockchaine, ktoré sa týkajú používateľa. Tieto krypto-peňaženky môžu byť fyzické zariadenia vo forme USB flash kľúčov, ako aplikácia pre rôzne operačné systémy, alebo ako web aplikácia. Zaistenie krypto-peňaženky a prístupu do jej obsahu môže byť kľúčové v prípade dokazovania spojitosti medzi záznamom v blockchaine a jeho vlastníkom.



Obr. 1: Distribuovaná databáza
Zdroj: vlastné spracovanie

Latentnosť, vysoký stupeň ochrany dát a zahladzovania digitálnych stôp

Viacnásobná latentnosť digitálnych stôp vyplýva z princípu ich existencie (informácia je vo forme binárneho zápisu uložená na záznamovom médiu), spôsobu uloženia (využitie atribútov na skrytie súborov, používanie rôznych súborových formátov), šifrovanie, prípadne zmazanie či prepísanie binárneho zápisu iným binárnym zápisom.

[2] METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej criminality*. Akadémia PZ SR v Bratislave, 2004. s. 169.

V prípade blockchainu nemusíme skúmať zmazané, či prepísané informácie, keďže to nie je možné z dôvodu jeho funkčnosti. Avšak pri skúmaní blockchainu rozoznávame dve možné varianty.

- Otvorený blockchain, kde sú jednotlivé informácie priradené konkrétnym transakciám s jednoznačne určenými používateľmi. Sem môžeme zaradiť aj systémy využívajúce pseudoanonymitu[3],
- Šifrovaný blockchain využívajúci niektorú z technológií znemožňujúcu identifikáciu konkrétnych užívateľov čiže vytvárajúci anonymné prostredie.

Napríklad systém „ring signatures“ v technológii CryptoNote[4] znemožňuje pozorovateľovi zistiť kto komu a čo posiela v rámci blockchainu. Táto technológia je využívaná proof-of-work algoritme CryptoNight, ktorý si osvojilo a modifikovalo niekoľko krypromien. Tieto sú často využívané/zneužívané na DarkNete na platby za trestnú činnosť. Asi najznámejšou anonymnou kryptomenou bolo v čase písania článku „Monero“5.

Obr. 2: Ring signature
Zdroj: https://cryptonote.org/inside#untraceable-payments

So šifrovaným blockchainom súvisí aj špecifikum vysokého stupňa ochrany dát. Rovnako ako u iných digitálnych stôp, aj v blockchaine šifrovanie spôsobuje sťaženie a vo väčšine prípadov znemožnenie práce s takýmito stopami. Pokiaľ teda predpokladáme, že skúmaný blockchain obsahuje potenciálne digitálne stopy, no nemáme mechanizmy na jeho dešifrovanie nemá pre nás žiadnu informačnú hodnotu.

Tak ako vysoký stupeň ochrany dát, súvisí s latentnosťou aj zahladzovanie digitálnych stôp. V tomto prípade závisí od použitej technológie. Nešifrovaný blochchain je v mnohých ohľadoch transparentný systém bez možnosti spätných úprav jednotlivých záznamov, čo z neho robí systém odolný voči zahladzovaniu stôp. Na druhej strane, páchatelia skôr využívajú šifrovaný blockchain, ktorý im svojou šifrovou ochranou vytvára anonymné prostredie, v ktorom nie je potrebné stopy zahladzovať. Prudkým vývojom informačných technológií a snahou o nadadenie užívateľsky prívetivého prostredia do každej oblasti informatiky často nie je potrebné aby bol páchateľ špecialista – informatik, postačí ak bude postupovať podľa pripravených návodov, ktoré sú dostupné na internete.

[3] To znamená, že používateľ síce uviedol nepravdivé, alebo upravené identifikačné údaje, no stále je možné jednoznačne určiť ktorú transakciu takýto používateľ vykonal.

[4] Ring signatures: Untraceable payments. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://cryptonote.org/inside#untraceable-payments>

[5] What is Monero (XMR)? [online]. [cit. 19. 03. 2019]. Dostupné na:<https://ww.getmonero.org/get-started/what-is-monero/>

Časová trasovateľnosť digitálnych stôp

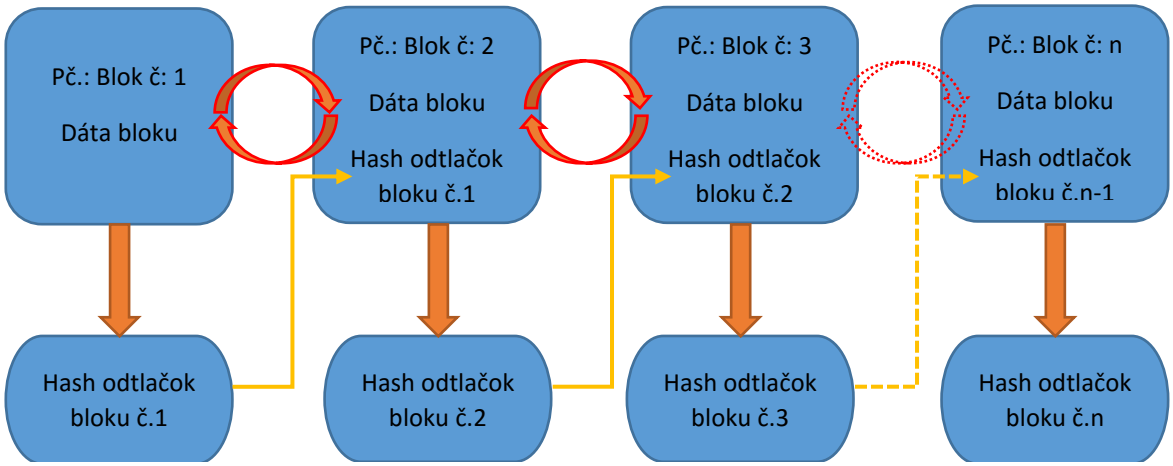
Z princípu funkčnosti databázy založenej na technológii blockchain nie je možné upravovať už zapísané údaje ale len pridávať nové. Tým pádom môžeme údaje ktoré sú v nej uložené považovať za relevantné aj s odstupom času. Každý vygenerovaný blok má niekoľko identifikátorov z nich sa minimálne jeden týka času, presnejšie časovej pečiatky (timestamp) ktorá presne určuje kedy bol blok vytvorený a pripojený do blockchainu. Tým pádom, ak vieme presný čas transakcie, vieme zistiť v ktorom bloku sa nachádza a opačne.

Vysoká obsažnosť digitálnych stôp

Informácie uložené na blockchaine môžu obsahovať veľmi cenné údaje o používateľovi. V závislosti od účelu, na ktorý bol blockchain spustený môžeme napríklad v blockchainoch kryptomien získať informácie o transakciách používateľa či adresy krypto-peňaženiek osôb s ktorými obchoduje, v blockchainoh subjektov (či už štátnych alebo súkromných) môžeme získať podrobné a citlivé osobné informácie týkajúce sa konkrétnych používateľov. Avšak vždy to závisí od spôsobu ukladania informácií do blochchainu. V prípade že sú použité otvorené metódy bez šifrovania údaje sú voľne prístupné. V opačnom prípade je potrebné poznať súkromný kľúč používateľa.

Životnosť digitálnych stôp, ich uchovávanie, kvalita a reštaurovateľnosť.

Na rozdiel od iných digitálnych stôp, kde je životnosť spravidla závislá od kvality použitého záznamového média, v prípade blockchainu je životnosť digitálnych stôp závislá na jeho existencii. Úroveň či mieru bezpečnosti uchovania by bolo možné vyjadriť veľkosťou siete teda počtom nódov, ktoré tvoria blockchain. Čím je sieť väčšia, tým je bezpečnejšia. Platí to ajmä pri kryptomenách založených na konsenze proof-of-work. Zaťiaľ je známych len niekoľko zraniteľností[6], no najznámejšou je útok „51 %“[7]. To znamená, že ak vlastním 51 % a viac výpočtového výkonu celej blockchain siete môžem vykonávať falošné transakcie



Obr. 3: Blockchain
Zdroj: vlastné spracovanie

a zapisovať ich do blockchainu, respektíve nahradiť pôvodný blockchain jeho modifikovanou verziou. Kryptomeny založené na tomto konsenze ale počítajú s tým, že je získanie takéhoto

[6] Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors> „útok 51“, „DDoS“, Transaction malleability attack, timejacking“, „routing attack“, „Sybil attack“. Útok 51 môže mať vplyv na celý blockchain, pričom ostatné útoky sa zameriavajú skôr na proces pri vytváraní nových blokov.

[7] 51% Attack. [online]. [cit. 19. 03. 2019]. Dostupné na: <https://learncryptography.com/cryptocurrency/51-attack>

výkonu je oveľa drahšie, či náročnejšie ako potenciálny zisk. V minulosti boli vykonané útoky 51% na viacero kryptomien avšak tie mali veľmi nízky sieťový hashrate teda pre útočníkov bolo jednoduchšie získať nadvládu nad blockchainom napríklad prostredníctvom bot-net vírusov inštalovaných na zariadeniach internetu vecí.

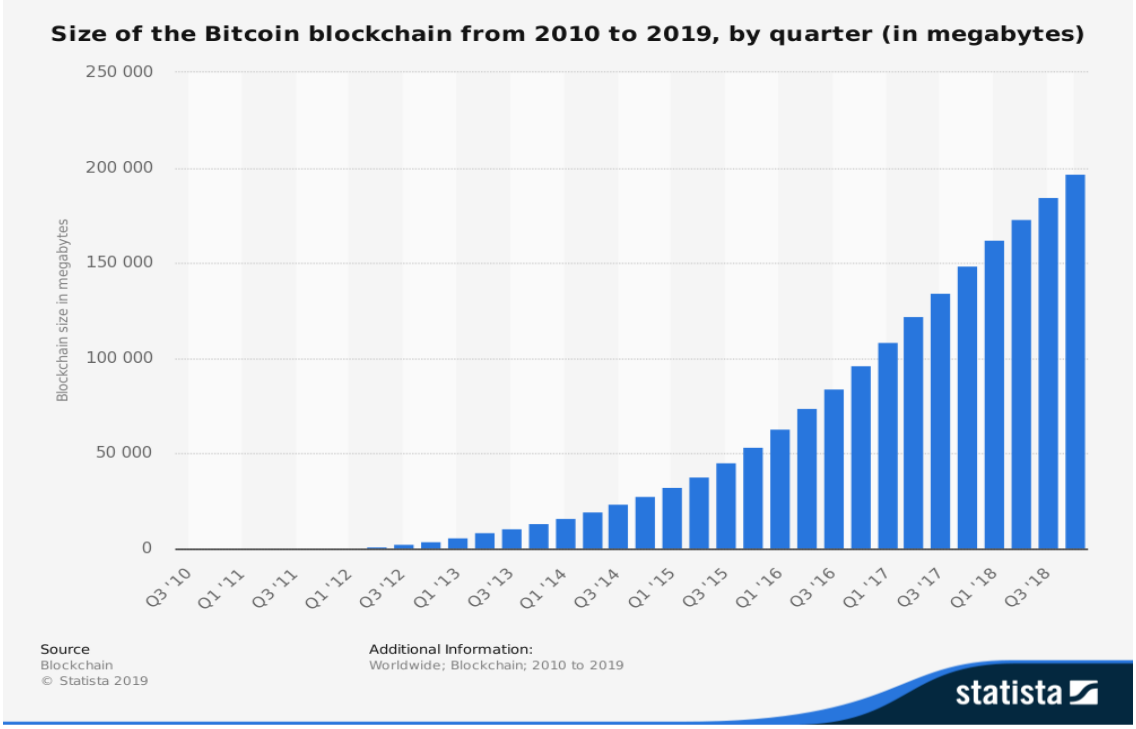
Uchovávanie blockchainu a kvalita rovnako závisí od funkčnosti a veľkosti siete nódov. Pokiaľ je sieť v stave on-line a má aspoň minimálny počet nódov[8], môžeme povedať že informácia je bezpečne uložená a dáta sú konzistentné. Ak by boli všetky nódy vypnuté a bola by k dispozícii len jedna kópia blockchainu, bola by relevancia informácií sporná nakoľko by nebolo možné porovnávať hash pečiatky jednotlivých blokov s inými kópiami blockchainu.

S tým súvisí aj reštaurovateľnosť blockchainu. Pokiaľ by došlo k zničeniu či zmazaniu blockchainu, obnova by znamenala reštaurovanie niekoľkých nódov, nakoľko reštaurovanie len jedného by nám neposkytovalo požadovanú validitu informácií.

Dátový objem a dátová hustota digitálnych stôp

Blockchainové databázy vo svojej podstate neustále narastajú. Keďže jednotlivé bloky na seba nadväzujú zväčšovanie databázy je nevyhnutnosť. Napríklad Bitcoin blockchain po 10 rokoch existencie dosiahol v januári 2019 veľkosť 197 gigabytov[9].

So zväčšovaním databázy bude narastať aj doba odozvy pri vyhľadávaní konkrétnych transakcií, čím sa bude predlžovať doba spracovávania či forenzného vyšetrovania informácií uložených v blockchaine ako potenciálnej digitálnej stopy. Z uvedeného vyplýva, že rovnako ako u iných typoch digitálnych stôp dochádza k poklesu ich dátovej hustoty v čase. Okrem nárastu dátového objemu ukladaných dát má na to vplyv ak skutočnosť, že „Množstvo zanechaných digitálnych stôp páchateľmi nemusí narastať rovnakým tempom“[10].



Obr. 4: Veľkosť blockchainu kryptomeny Bitcoin od vzniku po január 2019
Zdroj: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

[8] Minimálny počet nódov závisí od použitej blockchainovej technológie.

[9] Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes). [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>

[10] METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej criminality.* Akadémia PZ SR v Bratislave, 2004. s. 174.

Extrémna dynamickosť prostredia digitálnych stôp

Podľa opisu špecifík[11] je toto špecifikum typické pre sieťové prostredie, s tokom veľkého množstva dát. Sú to teda siete subjektov, so zväčša centralizovaným bodom riadenia a uskladnenia dát. Nakoľko je veľká pravdepodobnosť, že tieto systémy pracujú v nepretržitej prevádzke a v reálnom čase spracúvajú a ukladajú dáta veľkého množstva užívateľov, je z dôvodu potenciálneho vzniku veľkých škôd takmer nemožné ich úplné odstavenie a skúmanie systému v stave offline. Expertízy sú z tohto dôvodu vykonávané buď to na živých systémoch, alebo na ich záložných offline kópiách.

V prípade vykonávania expertíz v blockchaine, je situácia sčasti podobná. Blockchain je distribuovaná databáza, a jej prechod do stavu offline je veľmi nepravdepodobný. V prípade blockchain databáz využívaných štátnym či verejným sektorom môžu byť na ňom závisle systémy potrebné pre chod štátu či spoločností. V prípade kryptomien je by prechod blockchainu do stavu offline z praktického hľadiska takmer nemožný, keďže jeho jednotlivé nódy môžu byť rozmiestnené kdekoľvek vo svete. Na druhú stranu, prechod do režimu offline nie je v prípade blockchainu potrebný. Prístup do blockchainu je možný z ktoréhokoľvek bodu počítačovej siete, v ktorej je spustený. Jednotlivé bloky sa po pridaní do blockchainu nedajú jednoduchým spôsobom zmeniť[12]. Z toho vyplýva, že na rozdiel od iných digitálnych stôp je forenzné skúmanie blockchainu ohrozené dodatočnou aktivitou páchateľov len v minimálnej až zanedbateľnej miere v závislosti od veľkosti blockchainovej siete. Takže napríklad pokus o zmazanie záznamu, či jeho prepísanie iným záznamom nie je možný a to ani v prípade, že by bol páchateľ vo funkcii admministrátora, či superužívateľa. Pri akomkoľvek pokuse o zmenu v zapísanom bloku by kvôli zmenenému hash odtlačku došlo k porušeniu integrity celého blockchainu.

Heterogénnosť a komplexnosť prostredia digitálnych stôp

Pri špecifiku heterogénnosti a komplexnosti sa na blockchain môžeme pozrieť ako z hardverového, tak aj softvérového hľadiska. Zdrojové kódy blockchainu sú spravidla písané v programovacom jazyku[13], ktorý je možné kompilovať na počítačoch s rôznou architektúrou a pod rôznymi operačnými systémami. Vo všeobecnosti ale väčšina uzlov beží na niektorej z distribúcií linuxu a klientske aplikácie sú spustiteľné pod linuxom, MS Windows, či Androidom. Na vytvorenie nódu nie je potrebný špeciálny hardvér, zväčša postačuje bežný počítač, alebo server, no niektoré projekty sú schopné fungovať aj na SBC[14] počítačoch ako napríklad raspberry pi. V prípade kryptomien, sú istým špecifikom minery teda zariadenia, ktoré výpočtami hash funkcií udržiavajú v činnosti blockchainy založené na konsenze typu proof of work. Typ hardwaru závisí od použitej blockchain technológie. Môžu to byť obyčajné počítače, asic[15] minery, či GPU Rig[16].

V prípade, že za digitálnu stopu považujeme informáciu obsiahnutú v blockchaine, na jej extrahovanie je potrebný operátor, ktorý je danú informáciu schopný nájsť teda ovláda klientsky softvér, prípadne vie pracovať s block explorerom ak ho daný blockchain má verejne prístupný.

---

[11] METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej criminality*. Akadémia PZ SR v Bratislave, 2004. s. 168.

[12] Až na útok 51 popísaný vyššie.

[13] Napríklad blockchain Bitcoinu je písaný v jazyku „C++“.

[14] Single board computer (jednodoskový počítač).

[15] Application-specific integrated circuit – počítače zložené z veľkého množstva špecifických obvodov, ktoré sú schopné veľmi rýchlo počítať nejaký konkrétny druh algoritmu.

[16] Počítač obsahujúci viac, ako dve grafické karty určený na výpočty prostredníctvom grafických čipov.

Veľký geografický rozsah priestoru s geografickými stopami

Z pohľadu forenzného skúmania, nemá geografický rozsah pre prístup k potenciálnym digitálnym stopám v blockchaine až taký vplyv ako je tomu u iných digitálnych stôp. Ako bolo spomínané vyššie, blockchain je distribuovaná databáza, kde každý nód má vlastnú identickú kópiu databázy. Takže prístup k potenciálnym stopám je síce ohraničený veľkosťou siete ale prístup k nim je možný z ktoréhokoľvek bodu siete.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Thu Mar 21 2019 09:58:45 GMT+0100 (stredoeurópsky štandardný čas).

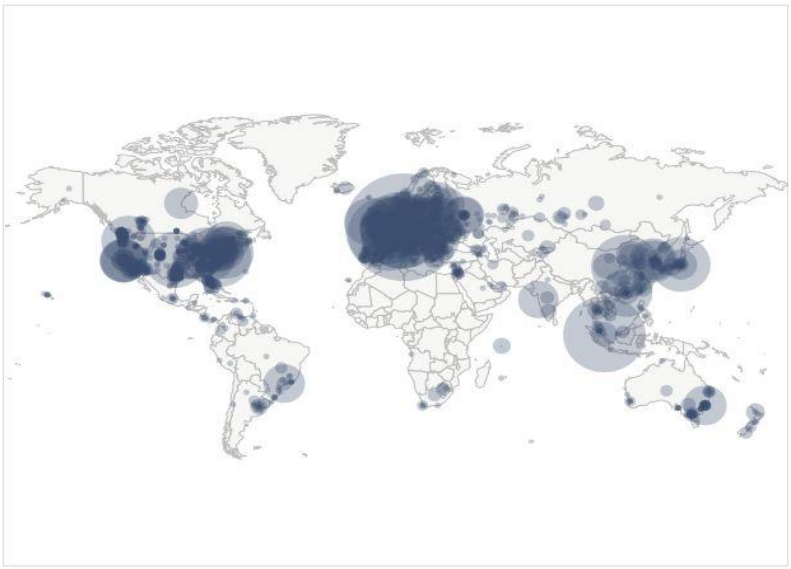
10299 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2585 (25.10%)
2	Germany	1947 (18.90%)
3	France	661 (6.42%)
4	Netherlands	517 (5.02%)
5	Canada	407 (3.95%)
6	United Kingdom	363 (3.52%)
7	Singapore	322 (3.13%)
8	China	321 (3.12%)
9	n/a	263 (2.55%)
10	Russian Federation	253 (2.46%)

More (100) »



Obr. 5: zobrazenie globálnej siete Bitcoin nódov
Zdroj: https://bitnodes.earn.com/

Automatické identifikovanie a spracovanie

V prípade blockchainu je táto identifikácia zatiaľ možná len v prípade, že ide o nešifrovaný blockchain, alebo dešifrovaný blockchain. Jednou z prvých automatizovaných metód je FIFO analýza[17] spätne trasujúca históriu bitcoinov a identifikujúca bicoiny použité pri trestnej činnosti.

Originálnosť digitálnych stôp

Blockckchain je vo svojom princípe databáza s vysokou mierou validity. Zabezpečená je hash funkciami, ktoré sú spätne previazané s jednotlivými blokmi databázy. Keďže vývoj technológií však nie je možné zastaviť ani na jednej strane, tak v súčasnej dobe existuje niekoľko typov útokov[18], ktoré môžu kompromitovať obsah blockchainu. Medzi najznámejšie patrí „útok 51“, „DDoS“, Transaction malleability attack, timejacking“, „routing attack“, „Sybil attack“. Takmer všetky sú využívané pri kradnutí kryptomien a najčastejšie využívajú zraniteľmosti konsenzu „proof of work“.

Na druhej strane sú neustále vyvíjané riešenia ako obmedziť alebo zamedziť potenciálnym útokom. Dôležitá je tiež voľba konsenzu. Konsenzus „proof of work“ patrí do skupiny takzvaných „loterry-based“ konsenzov využívaných hlavne u kryptomien. Nevýhodou je neustále narastajúca energetická náročnosť spolu s narastajúcou sieťou. Druhá skupina konsenzov „voting-based“ je založená na skupine pravidiel a je implementovaná

[17] A 200-year-old idea offers a new way to trace stolen. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.wired.com/story/bitcoin-blockchain-fifo-dirty-coins/>

[18] Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors>

v blockchainoch, ktoré sú využívané štátnymi či verejnými sektormi. Ako príklad môžeme uviesť konsenzus „hyperledger indy“.

Nízka úroveň súdnej akceptácie digitálnych stôp v právnej praxis v súčasnosti

S informatizáciou spoločnosti sa postupne eliminuje nedôvera súdnictva v relevantnosť digitálnych stôp. V tejto oblasti je priekopníkom pravdepodobne Čína[19] so zriaďovaním internetových súdov. Ďalším krokom je vyjadrenie Najvyššieho súdu Číny[20] zo 7. septembra 2019, ktorým oznamujú, že internetové súdy uznávajú ako dôkazy digitálne údaje, ktoré predkladajú príslušné strany ak boli zozbierané a uložené prostredníctvom blockchainu s digitálnymi podpismi, spoľahlivými časovými pečiatkami a overovaním hašovacej a môžu preukázať pravosť použitej technológie. To znamená, že pre čínske súdnictvo je technológia blockchain dostatočne dôveryhodná.

Rovnako právna komisia Veľkej Británie vo svojej výročnej správe[21] poukazuje na potrebu preskúmania smartkontraktov a technológie blockchain za účelom zachovania konkurencieschopnosti britského súdnictva.

Uvedené príklady naznačujú, že prijatie informačných technológií ako nositeľov digitálnych stôp v podobe informácií je nezvratné a je len otázkou času kedy bude akceptované plošne.

Záver

Technológia blockchain nie je nový prvok v prostredí komunikačno-informačných technológií, avšak jeho popularizáciou vďaka rozširovaniu kryptomien si našiel uplatnenie v mnohých oblastiach života. Mnohé štáty, či organizácie prechádzajú z klasických databázových systémov na komplexné blockchainové riešenia. Vďaka bezpečnosti a transparentnosti uložených údajov sa stal blockchain fenoménom pre ukladanie informácií dnešnej doby. Práve informácie v ňom uložené môžu slúžiť ako digitálne stopy pri dokazovaní a vymáhaní spravodlivosti.

Zoznam použitej literatúry:

1. METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. Akadémia PZ SR v Bratislave, s. 356. ISBN 80-8054-336-4.
2. Ring signatures: Untraceable payments [online]. [cit. 19. 03. 2019]. Dostupné na:<https://cryptonote.org/inside#untraceable-payments>
3. What is Monero (XMR)? [online]. [cit. 19. 03. 2019]. Dostupné na:<https://ww.getmonero.org/get-started/what-is-monero/>
4. 51% Attack. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://learncryptography.com/cryptocurrency/51-attack>
5. Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes). [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>
6. A 200-year-old idea offers a new way to trace stolen. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.wired.com/story/bitcoin-blockchain-fifo-dirty-coins/>

[19] Internetový súd v Hangzhou (*https://www.netcourt.gov.cn*) v Číne založený v roku 2017 bol prvým pilotným súdom v Číne, ktorý sa zameriava na vypočutia týkajúce sa prípadov súvisiacich s internetom. V čase písania tohto článku boli zriadené ďalšie tri podobné súdy.

[20] Provisions of the Supreme People's Court on Several Issues in the Trial of Cases in Internet Courts. 2019. [online]. [cit. 19. 03. 2019]. Dostupné na:<http://www.court.gov.cn/zixun-xiangqing-116981.html>

[21] The Law Commission Annual Report 2017-18 Courts. [online]. [cit. 19. 03. 2019]. Dostupné na: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727386/6.4475_LC_Annual_Report_Accounts_201718_WEB.PDF>

7. Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology. [online]. [cit. 19. 03. 2019]. Dostupné na:<https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors>
8. Provisions of the Supreme People's Court on Several Issues in the Trial of Cases in Internet Courts. [online]. [cit. 19. 03. 2019]. Dostupné na:<http://www.court.gov.cn/zixun-xiangqing-116981.html>
9. The Law Commission Annual Report 2017-18 Courts. [online]. [cit. 19. 03. 2018]. Dostupné na:<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727386/6.4475_LC_Annual_Report_Accounts_201718_WEB.PDF>

Kontaktné údaje:
Mgr. Štefan Zachar
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
stefan.zachar@akademiapz.sk

Recenzné posudky

doc. Ing. Anna Hamranová, PhD.
Katedra informačného manažmentu
Fakulta podnikového manažmentu
Ekonomická univerzita v Bratislave

Recenzný posudok na Zborník príspevkov z vedeckej konferencie
s medzinárodnou účasťou
**„AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI
(v podmienkach bezpečnostných zložiek)"**
konanej dňa 4.6.2019

1. Aktuálnosť a prínos riešenej problematiky

V súčasnosti rozvoj informačno - komunikačných technológií ovplyvňuje väčšinu oblastí pracovného i súkromného života každého človeka. Prináša nové príležitosti a nástroje, ale aj zvyšuje zraniteľnosť. Ťažisko nášho života a informácií postupne presúva do digitálne spravovaného sveta, preto je pochopiteľné, že to priťahuje aj snahy o zneužitie možností, ktoré digitálna éra prináša. Existuje množstvo atakov, od jednoduchých vírusových infiltrácií, cez rôzne cielené metódy a postupy na získanie citlivých dát a prístupových údajov, až po komplexné systémové útoky s cieľom ovládnuť a v prípade potreby zničiť cieľový systém. Hrozby v kybernetickom priestore sa postupne stávajú jednou zo zásadných hrozieb nielen pre jednotlivcov a organizácie, ale pre štát ako taký. Preto je problematika kybernetickej bezpečnosti celosvetovo riešená na najvyššej úrovni každého štátu a prirodzene aj na úrovni Európskej únie.

Na Slovensku od 1. apríla 2018 nadobudol účinnosť zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NIS). Narastajúce kybernetické hrozby, ako aj skutočnosť, že široká verejnosť využívajúca informačno - komunikačné technológie túto problematiku v mnohých prípadoch podceňuje, vyžadujú venovať jej zvýšenú pozornosť zo strany vedeckých pracovníkov a odborníkov na IT a bezpečnosť.

Z týchto dôvodov hodnotím Zborník príspevkov z vedeckej konferencie s názvom „Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)" ako vysoko aktuálny.

Zborník je výsledkom vedeckej činnosti pracovníkov Akadémie PZ v Bratislave, odborníkov zaoberajúcich sa kybernetickou bezpečnosťou z Českej republiky (Univerzita obrany v Brne, Policejní akademie ČR v Prahe), z viacerých slovenských univerzít (FEI STU v Bratislave, Prešovská univerzita, Žilinská univerzita, UMB v Banskej Bystrici), ako aj z odbornej praxe. Pozitívne hodnotím spoluprácu viacerých autorov nielen z jedného

pracoviska, ale predovšetkým spoluprácu autorov z akademického prostredia s autormi z odbornej praxe.

2. Obsahová a formálna stránka zborníka

Problematika kybernetickej bezpečnosti je v zborníku riešená z viacerých aspektov. Obsahuje 21 vedeckých a odborných príspevkov, ktoré sa zaoberajú:

- charakteristikou a špecifikáciou jednotlivých oblastí kybernetickej bezpečnosti
- bezpečnosťou občana, prevenciou a vzdelávaním v oblasti kybernetickej bezpečnosti,
- úlohami bezpečnostných zložiek v tejto oblasti,
- analýzou a zdokumentovaním digitálnych stôp,
- princípmi kybernetickej meny a finančnými transakciami
- prístupmi k ochrane osobných údajov,...

Významný prínos jednotlivých príspevkov a prípadné poznámky sú uvedené v nasledujúcom texte posudku.

Charakteristika a špecifikácia jednotlivých oblastí kybernetickej bezpečnosti

Príspevok R. Ivančíka s názvom KYBERNETICKÝ BOJ AKO JEDEN Z NEKONVENČNÝCH SPÔSOBOV BOJA, považuje kybernetický priestor za jednu z dimenzií pre vedenie vojny. V závere autor uvádza dve možnosti vývoja, a to buď modifikáciu vojenských doktrín, alebo realizáciu nekonvenčných operácií v rámci špeciálnych operácií a vznik špecializovaných jednotiek, zložiek, organizácií a inštitúcií ktoré sa budú podieľať na boji, ale nebudú mať status armády.

R. Ivančík a Ľ. Baričičová v príspevku s názvom KYBERNETICKÉ HROZBY AKO SÚČASŤ ASYMETRICKÝCH BEZPEČNOSTNÝCH HROZIEB V 21. STOROČÍ sa zameriavajú na charakteristiku kybernetických hrozieb, ako sú kyberterorizmus, kybernetická špionáž, kybernetické útoky, kybernetická kriminalita a kybernetické vojny. Keďže zaistenie bezpečnosti je považované za jednu zo základných funkcií štátu, tlak na vytváranie čo najbezpečnejších informačných sietí a rozvoj metód, postupov, prostriedkov a zariadení obrany, ochrany a bezpečnosti kyberpriestoru v budúcnosti ešte viac vzrastie a dostane sa na jedno z popredných miest v ďalšom vývoji komunikačných a informačných technológií.

Problematika podvodov v kyberpriestore je riešená v príspevkoch PODVOD – JEDNO Z NAJVÄČŠÍCH BEZPEČNOSTNÝCH RIZÍK, autorov A. Korauša, S. Backu a M. Bártu, a v príspevku RIADENIE RIZIKA PODVODU Z POHĽADU BEZPEČNOSTI A VČASNÉHO ODHALENIA, autorov A. Korauša, P. Kelemena, S. Backu a J. Poláka. Prvý z týchto príspevkov charakterizuje rizikovú skupinu úverových odvodov, ich prevenciu a softvér na včasné odhalenie podvodov. Druhý príspevok zdôrazňuje dôležitosť odhaľovania podvodov predovšetkým v podnikoch a organizáciách, ako aj jednotlivé kroky zdokonalenia prevenčného systému na zamedzenie výskytu podvodov.

Kolektív týchto autorov rieši ďalej problematiku kybernetických mien v príspevku ALTERNATÍVNE KYBERNETICKÉ MENY V SÚČASNOSTI, autorov A. Korauša, P. Kelemena,

S. Backu a J. Poláka a v spolupráci s J. Kuchtovou aj problematiku implementácie procesného riadenia v príspevku PROCESNÉ RIADENIE – FIREMNÝ NÁSTROJ BEZPEČNOSTI, OCHRANY MAJETKU A NEŽELANEJ MANIPULÁCIE S ÚDAJMI.

Bezpečnosť občana, prevencia a vzdelávanie v oblasti kybernetickej bezpečnosti

Dôležitosť riešenia problematiky prevencie a vzdelávania je podčiarknutá príspevkami zaoberajúcimi sa prevenciou a vzdelávaním od základných až po vysoké školy, ako aj vzdelávaním používateľov informačných systémov v praxi.

Do oblasti bezpečnosti občana a prevencie môžeme v prvom rade zaradiť príspevky Z. Dobrovanov Šimovej PROBLEMATIKA SEXTINGU U DETÍ A MLÁDEŽE a S. Šišuláka a M. Cíchovej „FAKE NEWS" A PROPAGANDA V KYBERNETICKOM PRIESTORE, ktoré riešia aktuálne témy ovplyvňujúce výchovu a budúce správanie sa detí mládeže.

F. Lenko v príspevku VYBRANÉ ASPEKTY VZDELÁVANIA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI NA ZÁKLADNÝCH ŠKOLÁCH rieši problematiku kyberšikanovania, uvádza jeho základné znaky, typy a formy. Na základe zrealizovaného dotazníkového prieskumu na základných školách v okrese Čadca konštatuje, že kyberšikanovanie sa na základných školách vyskytuje často a stretávajú sa s ním už deti vo veku 10 rokov. Z tohto dôvodu je potrebné zvýšiť mieru informovanosti u mladistvých o šikanovaní a kyberšikanovaní ako aj ďalších oblastiach, ktorými sa zaoberajú preventívne aktivity.

Autor P. Hrůza v príspevku VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI uvádza prehľad vzdelávania v oblasti kybernetickej bezpečnosti na Univerzite obrany v Brne. Okrem zamerania študijných programov v oblasti kybernetickej bezpečnosti, zdôrazňuje aj osvetu kybernetickej bezpečnosti pre študentov, ktorí neštudujú špecializáciu týkajúcu sa informačných technológií.

L. Mariš a V. Šoltés v príspevku PRÍPRAVA BEZPEČNOSTNÝCH MANAŽÉROV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI - VÝSLEDKY TESTOVANIA publikovali výsledky phishingového testu študentov Fakulty bezpečnostného inžinierstva Žilinskej univerzity v predmete aplikovaná informatika v rámci témy „kybernetická bezpečnosť". Na vykonanie phishingového testu autori zvoli odporúčaný test jednotky CSIRT na Úrade podpredsedu vlády SR pre investície a informatizáciu, dostupného na stránke csirt.sk, ktorý pozostával zo 17 otázok. Výsledky testu sú pomerne stručné, uvedené sú len počty správnych odpovedí, otázky s najväčším počtom nesprávnych odpovedí a porovnanie s opätovným testovaním. Keďže test obsahoval len 17 otázok, žiadúce by bolo okomentovať úroveň testu, príp. navrhnúť vylepšenia pre zrealizovanie vlastného testovania v budúcnosti. Súčasne chýbajú závery z testovania aplikovateľné vo vyučovanom predmete. Navrhujem aj úpravu názvu príspevku napr. na TESTOVANIE ŠTUDENTOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI (do názvu nedávať slovo „výsledky" – tie by mali byť v texte).

Príspevok K. Murdzu ÚLOHA SOCIOLÓGIE V ROZVOJI DIGITÁLNYCH KOMPETENCIÍ ŠTUDENTOV AKADÉMIE PZ V BRATISLAVE, zdôrazňuje okrem digitálnych kompetencií, ktoré sú kľúčovou zručnosťou 21. storočia, aj úlohu sociológie, ktorá umožňuje lepšie pochopiť zložité spoločenské javy a procesy, podporuje schopnosti kritického myslenia vo vyhľadávaní

sociálnych informácií a overovaní sociálnych faktov. Učí hľadať pravdu a zároveň ju odlišovať od rôznych dezinformácií, ktoré ovplyvňujú kybernetickú bezpečnosť spoločnosti.

Autori V. Šoltés a A. Šiser v príspevku POŽIADAVKY NA VZDELÁVANIE POUŽÍVATEĽOV INFORMAČNÝCH SYSTÉMOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI riešia aktuálnu situáciu v oblasti kybernetickej bezpečnosti na Slovensku a aktuálny stav vzdelávania v tejto oblasti. Navrhujú systém vzdelávania v oblasti informačnej bezpečnosti v SR pre rôzne kategórie používateľov digitálneho priestoru a popisujú znalostné štandardy pre oblasť informačnej bezpečnosti stanovené MF SR.

Kybernetická bezpečnosť a úlohy bezpečnostných zložiek v tejto oblasti

Kybernetická bezpečnosť je v zborníku riešená z viacerých hľadísk. A. Hambalík v príspevku s názvom CIELE KYBERÚTOKOV SA ROZŠIRUJÚ NA MENEJ CHRÁNENÉ ZARIADENIA SIETÍ sa zameral na ochranu bežne využívaného hardvéru, pripojeného na internet, predovšetkým tlačiarní.

L. Réveszová v príspevku KYBERPRIESTOR, KYBERNETICKÁ KRIMINALITA A KOMPARÁCIA JEJ NÁRASTU VZHĽADOM NA DYNAMIKU JEJ VÝVOJA rieši špecifiká kybernetickej kriminality.

J. Kuchtová sa zaoberá digitálnou stopou vo vzťahu k sociálnemu inžinierstvu v príspevku DIGITÁLNA STOPA AKO ZÁKLAD KYBERNETICKEJ BEZPEČNOSTI.

Autori P. Nečas a R. Ivančík v príspevku AKTUÁLNY POHĽAD NA VÝVOJ V OBLASTI ZAISŤOVANIA KYBERNETICKEJ BEZPEČNOSTI A OCHRANY INFORMÁCIÍ NA NÁRODNEJ A NADNÁRODNEJ ÚROVNI charakterizujú nové kybernetické bezpečnostné hrozby a riziká z globálneho pohľadu na základe dokumentov prijatých NATO a EÚ, ako aj na národnej úrovni. Autori konštatujú, že napriek existencii viacerých stratégií, koncepcií a právnych úprav, v SR absentuje kvalitná všeobecná právna úprava v tejto oblasti čo bude potrebné urýchlene riešiť.

Autor V. Šulc sa v príspevku ROLE MANAŽERA KYBERNETICKÉ BEZPEČNOSTI V PROCESU ŘÍZENÍ HROZEB zaoberá identifikovaním a charakteristikou generických hrozieb, ktorým je vystavený každý informačný systém. Autor navrhuje vytvoriť jednotnú taxonómiu hrozieb a určiť relevantné zdroje na určenie kategórií hrozieb, konkrétne vyšpecifikovanie hrozieb, ktorým organizácia čelí a posúdiť jej pripravenosť a odolnosť voči týmto hrozbám.

K. Ujváry a J. Kuchtová v príspevku ŠPECIFIKÁ OBJASŇOVANIA FINANČNÝCH TRANSAKCIÍ V SÚVISLOSTI S BITCOINOM sa venujú inštitucionálnej ochrane pred nelegálnym využitím kryptomien, špecificky bitcoinu, na národnej, tak aj medzinárodnej úrovni. V závere poskytujú návody, postupy vyšetrovania a navrhujú využitie softvérových nástrojov, ktoré zvyšujú efektivitu pri vyšetrovaní bitcoin transakcií.

Š. Zachar sa v príspevku VYUŽITIE ZNAKOV DIGITÁLNEJ STOPY PRI RIEŠENÍ PROBLEMATIKY BLOCKCHAIN zaoberá problematikou technológie blockchain, služieb založených na tejto technológii (napr. kryptomeny, databázy verejnej alebo štátnej správy, databázy poskytujúce služby v súkromnom sektore) a možnosťami evidencie digitálnych stôp v technológii blockchain, ktorá môže slúžiť pri dokazovaní a vymáhaní spravodlivosti.

Príspevok M. Kostreca OCHRANA OSOBNÝCH ÚDAJOV - VÝSLEDKY VÝSKUMOV VYKONANÝCH VO FRANCÚZSKU, NA SLOVENSKU A V ČESKEJ REPUBLIKE má praktický charakter (zrealizovaný dotazníkový prieskum), porovnáva a vyhodnocuje prístup k ochrane osobných údajov v krajinách uvedených v názve. Navrhujem zvážiť úpravu názvu tak, aby neobsahoval slovo „výsledky", napr. na OCHRANA OSOBNÝCH ÚDAJOV – VÝSKUM ZREALIZOVANÝ VO FRANCÚZSKU, NA SLOVENSKU A V ČESKEJ REPUBLIKE (pretože výsledky výskumu sú obsahom príspevku). Samotné výsledky považujem za veľmi cenné a do budúcnosti navrhujem prieskum zopakovať, aby bolo možné identifikovať vývoj v oblasti ochrany osobných údajov skúmaných krajinách v (možno aj vo vzťahu ku GDPR).

3. Záver

Celkovo je možné Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou „AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI (v podmienkach bezpečnostných zložiek)" hodnotiť ako aktuálny a veľmi kvalitný publikačný výstup.

Keďže problematika kybernetickej bezpečnosti a prevencie nadobúda s rozvojom IKT, zvyšovaním množstva elektronických údajov a informácií a implementáciou prvkov znalostnej spoločnosti stále väčší význam, môže byť predložený zborník vhodným námetom pre ďalšie skúmanie a implementáciu prvkov bezpečnosti a prevencie počítačovej kriminality v práci jednotlivcov i organizácií.

Záverom konštatujem, že zborník pod názvom „AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI (v podmienkach bezpečnostných zložiek)" po odstránení drobných nedostatkov má všetky potrebné atribúty, preto **o d p o r ú č a m** jeho schválenie a publikovanie.

V Bratislave, 13.8.2019

doc. Ing. Anna Hamranová, PhD.

Recenzný posudok

Titul, meno a priezvisko autora: Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou

Názov príspevku: Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)

Titul, meno a priezvisko recenzenta: RNDr. Eva Kostrecová, PhD.

Hodnotenie príspevku:

1. **Zaradenie príspevku** (Charakterizujte jednoznačne, či sa jedná o vedeckú štúdiu, vedeckú prácu alebo odborný článok). Posúďte konkrétnu nadväznosť štúdie ako výstupu projektu alebo vedeckovýskumnej úlohy a splnenie stanovených cieľov štúdie.

   - **uverejniť ako vedeckú štúdiu,**

   Príspevky, ktoré sú predmetom recenzovaného zborníka, spĺňajú vzhľadom na vedecký charakter medzinárodnej konferencie, kritériá vedeckej štúdie, aj napriek tomu, že ich zameranie a ciele sú rôznorodé. Tento fakt vyplýva zo skutočnosti, že účastníkmi konferencie boli akademickí, vedeckí i expertní pracovníci Univerzitných pracovísk, špecializovaných inštitúcií so zameraním na kybernetickú a informačnú bezpečnosť, ako aj špecialisti z policajnej praxe.

2. **Dostatočný rozsah príspevku** (pozn. nevhodné prečiarknite)

   Vedecká štúdia (minimálny rozsah 1 AH, 36 000 znakov vrátane medzier).
   ~~Vedecká práca (minimálny rozsah 0,5 AH, 18 000 znakov vrátane medzier).~~
   ~~Odborný článok (minimálny rozsah 0,5 AH, 18 000 znakov vrátane medzier).~~

   - áno, obsahuje stanovený rozsah strán,
   - ~~nedosahuje minimálny rozsah strán, podľa názoru recenzenta je potrebné príspevok dopracovať,~~
   - ~~nedosahuje minimálny rozsah strán, ale podľa názoru recenzenta vzhľadom na spracovanie príspevku je počet strán dostačujúci,~~
   - príspevok obsahuje viac strán, ako je odporúčané, ale recenzent vzhľadom na spracovanie príspevku nepovažuje za potrebné rozsah strán zúžiť,
   - ~~príspevok obsahuje viac strán, ako je odporúčané, recenzent považuje za potrebné rozsah strán zúžiť.~~

Vzhľadom na typ publikácie, ktorým je zborník z vedeckej konferencie, a ktorý obsahuje až 21 príspevkov, považujem jeho rozsah za dostatočný.

3. **Odborná úroveň** (pozn. nevhodné prečiarknite)

   a) **aktuálnosť témy**
   - téma je nová,
   - téma je bežná, ale aktuálna,
   - ~~téma je neaktuálna.~~

   Kybernetická a informačná bezpečnosť je v oblasti ochrany súkromia, aj v súlade s GDPR - nariadenia EÚ o ochrane osobných údajov, síce už legislatívne bežne ošetrenou témou, ale napriek tomu vysoko aktuálnou. Jej skutočná realizácia v praxi je v mnohých oblastiach (najmä pri ochrane IT infraštruktúry, pri spracúvaní dát občanov EÚ mimo územia EÚ, pri publikovaní príspevkov na sociálnych sieťach a prostredníctvom informatických nástrojov pre publikovanie a šírenie informácií – napr.: Google, Wikipédia, a pod., pri vyšetrovaní a posudzovaní porušení pravidiel GDPR, atď.) novou témou, s nedostatočne implementovanými ochrannými mechanizmami a s nedostatočnou úrovňou osvety a vzdelávania občanov EÚ. Z uvedených dôvodov považujem publikovanie recenzovaného zborníka za veľmi aktuálne a prínosné.

   b) **citácie** (pozn. nevhodné prečiarknite)
   - pôvod prevzatých časti sa cituje v súlade s normou,

   Napriek skutočnosti, že som označila alternatívu, že citácie sú súlade s normou, žiadam zostavovateľov zborníka o formálnu úpravu textov citácií a použitých zdrojov a ich zosúladenie, pretože napr. už v prvom príspevku nie je pri názve použitých zdrojov použitá „Kurzíva", tak ako je tomu pri väčšine príspevkov.

   V príspevku „Digitálna stopa ako základ kybernetickej bezpečnosti" autorky Jany Kuchtovej, sú referencie na citované texty v texte formálne vyznačené nejednotne. Je nutné ich zosúladiť so štandardom. Obdobná pripomienka platí aj pre príspevok „Vybrané aspekty vzdelávania v oblasti kybernetickej bezpečnosti na základných školách", autora Filipa Lenka.

   - ~~pôvod prevzatých častí sa cituje nedostatočne alebo vôbec.~~

Pripomienky:

4. **Úroveň spracovania** (pozn. nevhodné prečiarknite)

   a) **jazyková úroveň:**
   - ~~má požadovaný štandard, bez výhrad,~~
   - má drobné nedostatky,

   V príspevku „Alternatívne kybernetické meny v súčasnosti" autorov: Antonín Korauš, Pavel Kelemen, Stanislav Backa, Jozef Polák, sú už v Abstrakte príspevku drobné preklepy a použité nespisovné slová („Vznikajú nezávisle od vlád a bankách, sú buď ťažené prostredníctvom počítačov, alebo vydávané ich autormi.").

V príspevku „Kyberpriestor, kybernetická kriminalita a komparácia jej nárastu vzhľadom na dynamiku jej vývoja“ autorky Liliany Réveszovej, je niekoľko formálnych gramatických preklepov a nesúladov (napr. už v abstrakte je uvedené: „V uvedenom príspevku sa v jej prvej časti venujeme definícii kybernetickej kriminality“).

V príspevku „Špecifiká objasňovania finančných transakcií v súvislosti s bitcoinom“ autorov Kristiána Ujváry, Jany Kuchtovej, je niekoľko sémantických preklepov (napr.. už v abstrakte v texte: „Venujú sa inštitucionálnej ochrane pred nelegálnym využitím kryptomien, špecificky bitcoinu, ako na národnej, ako aj medzinárodnej úrovni.)

- ~~má zásadné nedostatky.~~

b) odborná terminológia:

- rešpektuje v plnej miere,

Aj napriek skutočnosti, že som označila alternatívu, že je v príspevkoch zborníka odborná terminológia rešpektovaná v plnej miere, mám drobnú výhradu k pojmu „dotazníkový prieskum“ v príspevku „Vybrané aspekty vzdelávania v oblasti kybernetickej bezpečnosti na základných školách“ autora Filipa Lenka, a navrhujem ho v celom príspevku preformulovať na pojem „dotazníkový výskum“.

V príspevku „Problematika sextingu u detí a mládeže“ autorky Zuzany Dobrovanov Šimovej, je potrebné bližšie vysvetliť pojem „revenge porn“, ktorého skutočný význam je „pomsta formou uverejnenia porna osoby, bez jej vedomia“.

V príspevku „Využitie znakov digitálnej stopy pri riešení problematiky blockchain“ autora Štefana Zachara, je nesúlad v Kľúčových slovách v slovenskej a anglickej verzii.
„Kľúčové slová: Blockchain, kryptomena, digitálna stopa, ,hash algoritmus, konsenzus.“
„Key words: Cyber security, communication and information technologies, information protection.“

- ~~rešpektuje čiastočne,~~
- ~~nerešpektuje.~~

Pripomienky:

5. **Súlad názvu príspevku s obsahom** (pozn. nevhodné prečiarknite)

- je výstižný a korešponduje s obsahom,
- ~~dostatočne nevystihuje obsah príspevku,~~
- ~~nie je v súlade s jeho názvom.~~

6. **Odporúčanie recenzenta** (pozn. nevhodné prečiarknite)

- ~~príspevok odporúčam publikovať v pôvodnej verzii,~~
- príspevok odporúčam publikovať po odstránení menej závažných nedostatkov,

~~– článok nie je vhodný na publikovanie.~~

Zborník odporúčam publikovať po odstránení vyššie uvedených formálnych nedostatkov.

7. **Ďalšie pripomienky recenzenta:**

Zostavovateľom zborníka a organizátorom konferencie odporúčam pri organizácii ďalších konferencií požadovať od autorov príspevkov jednotnú jazykovú formu ich vizitiek, najmä ak ide o viacerých autorov jedného príspevku z rôznych akademických inštitúcií.

(napr. Vizitky autorov príspevku „Riadenie rizika podvodu z pohľadu bezpečnosti a včasného odhalenia", pôsobia veľmi nesúrodo tak jazykovo, ako aj obsahovo).

„Kontaktné údaje:

Doc. Ing. Antonín Korauš, PhD., LL.M, MBA
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
antonín.koraus@minv.sk

Mgr. Pavel Kelemen
University of Prešov in Prešov
Faculty of Management,
Konštantínova 16, 080 01 Prešov, Slovakia
kelemen.pavel@gmail.com

Mgr. Štefan Zachar
Katedra informatuiky a manažmentu
Akadémia PZ v Bratislave
stefan.zachar@minv.sk; stefan.zachar@akademiapz.sk"

dátum

podpis

Hlavní partneri:

FORTINET®

Microsoft

SOITRON

INSPIRUJEME K NAROCNOSTI

ASBIS®

SUCCESS THROUGH FOCUS

Mediální partneri:

PC REVUE

TOUCHIT

Partneri:

RCTT COMMUNICATION

veri2

DOKUMENTA

INTERWAY

SPOJNET

virtė

DELL EMC

veracomp

we inspire IT

Názov: **AKTUÁLNE VÝZVY KYBERNETICKEJ BEZPEČNOSTI (v podmienkach bezpečnostných zložiek)**

Vydala: Akadémia Policajného zboru v Bratislave
Sklabinská 1, 835 17 Bratislava

Pracovisko: Katedra informatiky a manažmentu

Zostavil: Mgr. Štefan ZACHAR
npor. Bc. Mgr. Liliana RÉVESZOVÁ

Technická redakcia: plk. doc. Ing. Ľubica BARIČIČOVÁ, PhD.
Mgr. Štefan ZACHAR
npor. Bc. Mgr. Liliana RÉVESZOVÁ

Recenzenti: doc. Ing. Anna HAMRANOVÁ, PhD.
RNDr. Eva KOSTRECOVÁ, PhD.

Rozsah: 214 strán

Rok vydania: 2019

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori.
Rukopis neprečiel jazykovou úpravou.

ISBN 978-80-8054-819-3
EAN 9788080548193