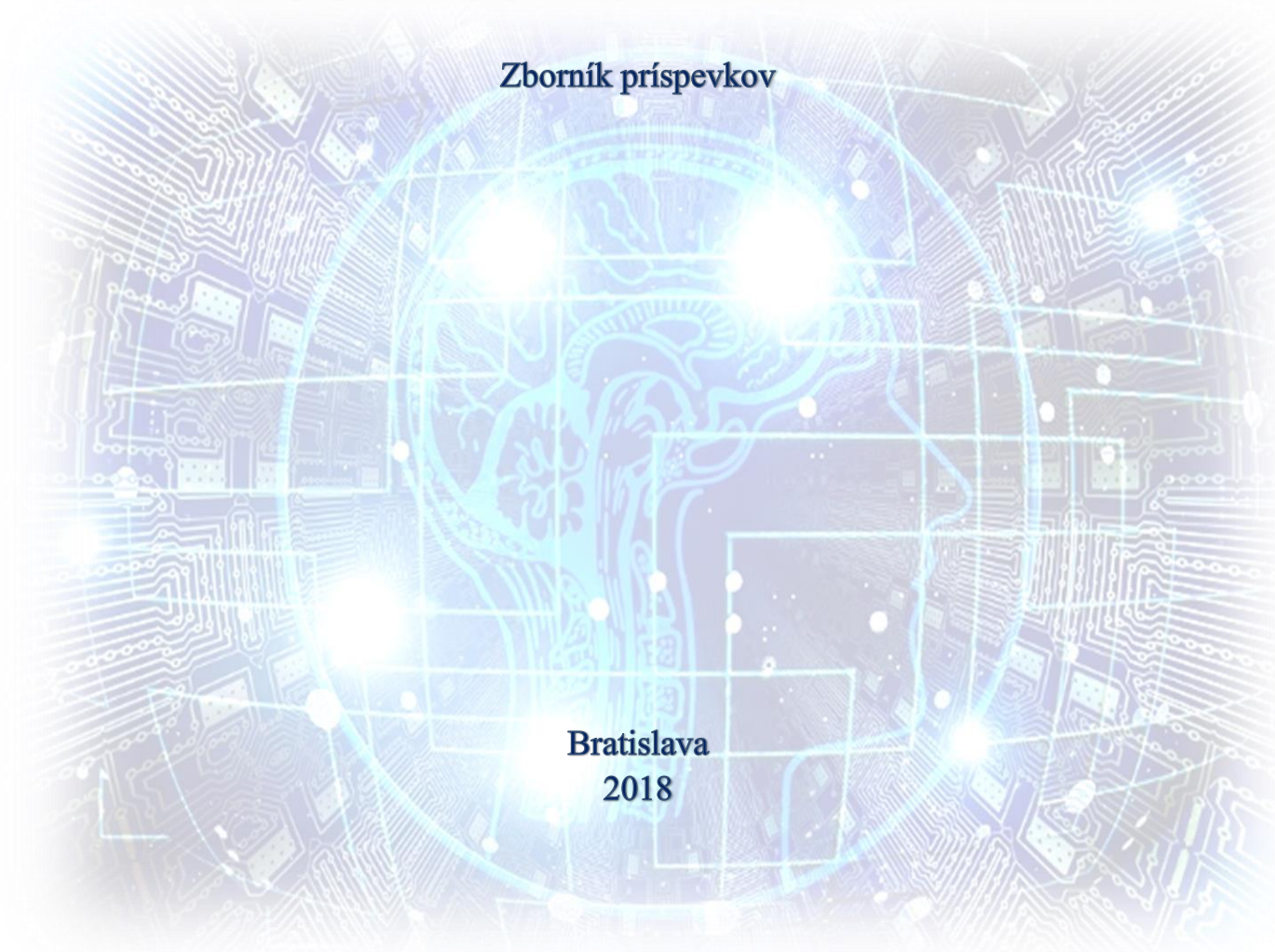
Akadémia Policajného zboru v Bratislave
Katedra informatiky a manažmentu

Vedecká konferencia s medzinárodnou účasťou

AKTUÁLNE VÝZVY PREVENCIE POČÍTAČOVEJ KRIMINALITY

Zborník príspevkov



Bratislava
2018

AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE
Katedra informatiky a manažmentu

ZBORNÍK PRÍSPEVKOV

z vedeckej konferencie s medzinárodnou účasťou

Aktuálne výzvy prevencie počítačovej kriminality

konanej dňa 21. 3. 2018

pod záštitou rektorky Akadémie Policajného zboru v Bratislave
Dr. h. c. doc. JUDr. Lucie Kurilovskej, PhD.
a s podporou Rady vlády SR pre prevenciu kriminality

Bratislava 2018

Vedecká konferencia bola organizovaná v rámci realizácie projektu zameraného na prevenciu páchania počítačovej kriminality s názvom „Buď bezpečný!“

Vedecký výbor konferencie:

Dr. h. c. doc. JUDr. Lucia KURILOVSKÁ, PhD. (APZ)
Ing. Stanislav ŠIŠULÁK, PhD. (APZ)
prof. Ing. Miroslav LISOŇ, PhD. (APZ)
prof. Ing. Jozef STIERANKA, PhD. (APZ)
doc. Ing. Ľubica BARIČIČOVÁ, PhD. (APZ)
doc. RNDr. Ľudmila GREGUŠOVÁ, PhD. (APZ)
doc. PhDr. Magdaléna ONDICOVÁ, PhD. (APZ)
JUDr. Miroslav BRVNIŠŤAN, PhD. (BMSEC)
doc. RNDr. Josef POŽÁR, CSc. (PA ČR)
doc. JUDr. Štěpán KALAMÁR, Ph.D. (PA ČR)
Ing. Jozef HALCIN (MV SR)
Mgr. Stanislav ŠPANKO (P PZ)
Ing. Ondrej LACIAK, PhD. (KEÚ)
Mgr. Rastislav JANOTA (NBÚ)

Organizačný výbor konferencie:

JUDr. Matej KOSTREC, PhD. (APZ)
RNDr. Tatiana HAJDÚKOVÁ, PhD. (APZ)
Mgr. Jana KUCHTOVÁ (APZ)
Mgr. Štefan ZACHAR (APZ)
Mgr. Linda PIVÁČKOVÁ (APZ)
Mgr. Katarína JUNASOVÁ (APZ)
Ing. Igor PAVLOVIČ (APZ)

Recenzenti:

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

Zostavili:

JUDr. Matej KOSTREC, PhD.
Mgr. Jana KUCHTOVÁ

Technická redakcia:

doc. Ing. Ľubica BARIČIČOVÁ, PhD.
Mgr. Jana KUCHTOVÁ
Mgr. Štefan ZACHAR

© Akadémia Policajného zboru v Bratislave

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori. Rukopis neprešiel jazykovou úpravou.

ISBN 978-80-8054-774-5
EAN 9788080547745

Obsah

Úvodné slovo

Vážené dámy, vážení páni,
ctení zástupcovia akademickej obce, aplikačnej praxe,
milé študentky a študenti, vzácni hostia!

Dovoľte mi, aby som Vás v mene svojom ako aj v mene katedry informatiky a manažmentu čo najsrdečnejšie privítala na pôde Akadémie PZ v Bratislave, kde sa spoločne stretávame pri príležitosti konania vedeckej konferencie s medzinárodnou účasťou **„Aktuálne výzvy prevencie počítačovej kriminality“.**

Dnešné podujatie je organizované ako súčasť projektu ***Buď bezpečný!*** zameraného na prevenciu páchania počítačovej kriminality. Preto niet divu, že sa táto skutočnosť premieta aj do obsahového zamerania konferencie, ktorá sa cielene koncentruje na vymedzenie a analyzovanie aktuálnych problémov spojených s páchaním počítačovej kriminality, zovšeobecnenie teoretických prístupov a praktických skúseností zúčastnených subjektov ako základného predpokladu pre vytvorenie systematického prístupu k oblasti prevencie počítačovej kriminality nielen na národnej ale aj medzinárodnej úrovni. K ďalším cieľom konferencie patrí identifikácia predpokladov na prepojenie teórie s aplikačnou praxou, ako aj zabezpečenie transferu relevantných poznatkov do praxe subjektov štátnej a verejnej správy potrebných pre skúmanie špecifických problémov a aktuálnych potrieb bezpečnostnej praxe v oblasti zvyšovania úrovne kybernetickej bezpečnosti SR.

Som veľmi rada, že na dnešnom podujatí môžem osobne privítať viacerých vzácnych hostí na čele s pani rektorkou APZ v Bratislave **Dr. h. c. doc. JUDr. Luciou KURILOVSKOU, PhD.,** pod záštitou ktorej sa táto konferencia koná.

Ďalej medzi nami vítam:

- **Ing. Jozefa HALCINA** - riaditeľa odboru prevencie kriminality MV SR,
- **Mgr. Rastislava JANOTU** - zástupcu riaditeľa útvaru SK-CERT a predsedu výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR,
- **Mgr. Stanislava ŠPANKA** - riaditeľa odboru počítačovej kriminality úradu kriminálnej polície PPZ,
- **Ing. Stanislava ŠIŠULÁKA, PhD.** - prorektora pre informatizáciu a koordináciu s policajnou praxou APZ v Bratislave,
- **JUDr. Miroslava BRVNIŠŤANA, PhD**. - manažéra projektu Buď bezpečný a konateľa spoločnosti BMSEC Bratislava.

Dnešným podujatím nás v roli moderátora bude sprevádzať môj kolega z katedry informatiky a manažmentu **JUDr. Matej KOSTREC, PhD.**

Vážení prítomní,

dovoľte mi z tohto miesta Vám zaželať príjemný deň a načerpanie mnohých zaujímavých a potrebných poznatkov z tejto oblasti.

doc. Ing. Ľubica BARIČIČOVÁ, PhD.
vedúca Katedry informatiky a manažmentu
Akadémie PZ v Bratislave

Ciele a tematické zameranie konferencie

Konferencia bola organizovaná ako súčasť projektu „Buď bezpečný!“, ktorý je prioritne zameraný na prevenciu páchania počítačovej kriminality. Preto hlavným cieľom konferencie bolo vymedzenie a analyzovanie základných problémov týkajúcich sa počítačovej kriminality, vytvorenie predpokladu pre systematický prístup k oblasti prevencie počítačovej kriminality zo strany zúčastnených subjektov nielen na národnej ale aj medzinárodnej úrovni, prepojenie teórie s aplikačnou praxou prostredníctvom workshopu zameraného na zvýšenie úrovne kybernetickej bezpečnosti.

V zmysle vytýčených cieľov a obsahového zamerania vedeckej konferencie boli jednotlivé prezentované príspevky koncentrované najmä na nasledovné okruhy:

- vedecké základy vzťahu ľudského faktora a kybernetickej kriminality,
- teoretické východiská riešenia prevencie kybernetickej kriminality,
- východiská skvalitňovania spolupráce Akadémie PZ v Bratislave s ostatnými vysokými škola doma i 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.

Program konferencie

08.00 – 08.30 – **prezentácia účastníkov**

08.30 – 08.45 – **otvorenie konferencie, úvodné slovo**
Dr. h. c. doc. JUDr. Lucia Kurilovská, PhD., rektorka A PZ v Bratislave
Ing. Jozef Halcin, riaditeľ odboru prevencie kriminality MV SR

08.45 – 09.10 – **Projekt „Buď bezpečný!“ a jeho realizácia v praxi**
JUDr. Miroslav Brvnišťan, PhD., BMSEC s.r.o. Bratislava

09.10 – 09.25 – **Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky**
JUDr. Veronika Marková, PhD., vedúca KTP A PZ v Bratislave

09.25 – 09.45 – **Počítačová kriminalita z pohľadu policajnej praxe**
Mgr. Stanislav Španko, riaditeľ odboru počítačovej kriminality UKP PPZ

09.45 – 10.05 – **Rola polície pri boji s kriminalitou v kybernetickom prostredí – pohľad nezávislej odbornej spoločnosti na možnosti vyšetrovania a dokumentovania kybernetickej kriminality**
Corpus Solution, a.s. Praha

10.05 – 10.25 – **Riziká a nevýhody sociálnych sietí**
Michal Dragan, odborník na sociálne siete

10.25 – 10.40 – **prestávka, občerstvenie**

10.40 – 11.00 – **Zákon o kybernetickej bezpečnosti**

Mgr. Rastislav Janota, zástupca riaditeľa SK-CERT a predseda výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR

11.00 – 11.20 – **Budovanie proaktívneho bezpečnostného dohľadu na úrovni štátnej inštitúcie**
Fidelis Cybersecurity s.r.o. Praha

11.20 – 11.40 – **Digitálna identita v kontexte počítačovej kriminality**
Ing. Marek Laššák, vedúci oddelenia analýzy dát OPSKA KEÚ PZ P PZ MV SR

11.40 – 11.50 – **Možnosti stanovenia výšky škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov**
doc. JUDr. Peter Polák, PhD., Mgr. Bc. Tomáš Trúsik, ProtoWay s.r.o., Fakulta práva Paneurópskej vysokej školy n.o.

11.50 – 12.00 – **Etický hacking v organizácii v zmysle smernice o kybernetickej bezpečnosti**
PhDr. Peter Veselý, PhD. MBA, Mgr. Vincent Karovič, PhD., Fakulta manažmentu Univerzity Komenského v Bratislave

12.00 – 12.30 – **diskusia a prijaté závery**

12.30 – 13.30 – **obed**

13.30 – 15.00 – **workshop zameraný na praktické ukážky**
„Najlepší pomocník experta Security Operations Center alebo ako spoľahlivo detekovať, efektívne vyšetrovať a účinne eliminovať množstvo bezpečnostných incidentov."
Cieľ workshopu: Na konkrétnych praktických ukážkach predstaviť unikátne nástroje určené na detekciu a prevenciu pred sofistikovanými kybernetickými útokmi, ktoré vďaka svojim jedinečným vlastnostiam umožňujú veľmi hlbokú okamžitú aj retrospektívnu analýzu na sieti i koncových bodoch. Vysoká miera automatizácie detekčných, vyšetrovacích a remediačných postupov prináša významnú úsporu času i zefektívnenie činností vyšetrovateľov bezpečnostných incidentov. Názornú časť prezentácie bude tvoriť praktická živá ukážka stopovania útočníka a vyšetrenie incidentu.

Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti

Ľubica Baričičová

Abstrakt:
Dnešná doba prináša so sebou mnoho nových očakávaní, možností a výziev vo všetkých sférach spoločnosti. Zvlášť výrazne sa to odráža v oblasti rýchleho rozvoja informačno-komunikačných technológií. Súvisí to so samotnou podstatou informačnej spoločnosti, ktorá predstavuje objektívnu realitu súčasnosti. Z tohto aspektu je potrebné manažment informácií vnímať nielen ako tok informácií založený na technologickom základe ale hlavne na informačnom ponímaní. Dosiahnutie požadovanej úrovne informačnej kompetencie, ktorá zodpovedá aktuálnym požiadavkám doby, si prirodzene vyžaduje dôslednú aplikáciu nových prístupov, nového obsahu a procesov vzdelávania všetkých členov spoločnosti, policajných manažérov, či ostatných príslušníkov Policajného zboru nevynímajúc.
Kľúčové slová:
Informačná spoločnosť, informačná kompetencia, informačná bezpečnosť, katedra informatiky a manažmentu, predmety skupiny Informatika

Abstract:
Present time brings many new expectations, opportunities and challenges in all spheres of society. This is particularly noticeable in the area of rapid development of information and communication technologies. It is related to the essence of the information society, which represents the objective reality of the present. From this point of view, management of information needs to be perceived not only as a flow of information based on technology but mainly on information. Achieving the required level of information competence according to current requirements naturally requires the consistent application of new approaches, new content and learning processes for all members of the society, includes of the police managers, or other members of the Police Force.
Key words:
Information society, information competence, information security, Department of Informatics and Management, subjects of the Informatics

Úvod

Nástup tretieho tisícročia priniesol vo všetkých oblastiach života prehĺbenie pôsobenia mnohých významných faktorov, ktoré sa spájajú s rozvojom modernej spoločnosti založenej na celosvetovej globalizácii, ktorá úzko súvisí s informačnou spoločnosťou.

Názory viacerých renomovaných odborníkov zaoberajúcich sa problematikou informačnej spoločnosti sa zhodujú v tom, že informačnú spoločnosť označujú ako spoločnosť, v ktorej kvalita života aj perspektíva sociálnych zmien a ekonomického rozvoja stále viac závisí od informácií a ich efektívneho využitia. Z uvedenej charakteristiky jednoznačne vyplýva rastúci význam informácií, ktoré zohrávajú kľúčové postavenie z pohľadu rozvoja spoločenského života. Práve informácie sú totiž - popri personálnych zdrojoch - najcennejším zdrojom fungovania každej organizácie. Bez zveličenia možno povedať, že v dnešnej spoločnosti zohrávajú úlohu najhodnotnejšieho a najziskovejšieho tovaru.

Preto niet divu, že stále viac do popredia sa dostávajú otázky spojené s ich ochranou a bezpečnosťou. Dôkazom toho je aj prijatie viacerých strategických a legislatívnych dokumentov, ako napríklad:[1]

- Národná stratégia pre informačnú bezpečnosť v Slovenskej republike,
- Koncepcia šifrovej ochrany informácií,
- Návrh systému vzdelávania v oblasti informačnej bezpečnosti/kybernetickej bezpečnosti v Slovenskej republike,

[1] Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.

- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – CSIRT.SK,
- Legislatívny zámer zákona o informačnej bezpečnosti,
- Stratégia Európskej únie pre kybernetickú bezpečnosť: Otvorený, bezpečný a chránený kybernetický priestor,
- Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy,
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020,
- Zákon o kybernetickej bezpečnosti,
- Nariadenie EÚ na ochranu osobných údajov (GDPR) a podobne.

Vychádzajúc z uvedeného možno konštatovať, že informačná spoločnosť si vyžaduje nové prístupy, nový obsah a procesy vzdelávania, ktoré v podmienkach SR vychádzajú hlavne z rastúceho záujmu obyvateľstva o využívanie informačno-komunikačných technológií vo všetkých oblastiach života.

Informačná spoločnosť potrebuje ľudí, ktorí budú vzdelaní a budú disponovať potrebnými zručnosťami a návykmi. Ako vyplýva z európskeho referenčného rámca[2] stanovujúceho kľúčové kompetencie pre celoživotné vzdelávanie v podmienkach modernej spoločnosti, *informačná kompetencia*, *zručnosť v informačno-komunikačných technológiách* patrí medzi hlavné priority vzdelávania podporujúce všetky ostatné vzdelávacie činnosti.

Informačná spoločnosť a jej odraz v spoločnosti

Informačnú spoločnosť charakterizuje značné využívanie digitálneho spracovávania, uchovávania a prenosu informácií. Technologickou základňou tejto zmeny je využívanie prvkov moderných informačných a komunikačných technológií. Motorom tohto rastu a neustálych inovácií je rýchle tempo technologického pokroku v konštrukcii počítačov. V tejto súvislosti napríklad Yoneji Masuda svoje predstavy o informačnej spoločnosti pre 21. storočie nazval *Computopia* (počítačová utópia).

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 (network society), 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. [3]

Spoločnosť založená na informáciách so sebou prináša isté všeobecne platné kladné ale i záporné dôsledky. K hlavným pozitívam informačnej spoločnosti možno priradiť predovšetkým:[4]
- dostupnosť, aktuálnosť a úplnosť informácií,
- okamžitý prenos informácií,

[2] Rámec stanovuje osem kľúčových kompetencií, medzi ktoré patria: komunikácia v materinskom jazyku, komunikácia v cudzích jazykoch, kompetencie v matematike a základné kompetencie v oblasti prírodných vied a techniky, informačná kompetencia, učenie sa ako sa učiť, sociálne a občianske kompetencie, zmysel pre iniciatívu a podnikanie, kultúrne povedomie a vyjadrovanie.

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

[4] VYMĚTAL, J., DIAČIKOVÁ, A., VÁCHOVÁ, M. *Informační a znalostní management v praxi*. Praha: LexisNexis CZ, 2005, s. 231-235.

- slobodu pri práci s informáciami,
- zvýšenie informovanosti vo všetkých sférach spoločenského života,
- pomerne lacnú výmenu informácií v celosvetovom meradle,
- nové formy vzdelávania,
- nové formy obchodu (e-business), virtuálne podnikanie,
- globálnu spoluprácu.

Na druhej strane negatívom takejto spoločnosti je hlavne to, že zapríčiňuje napríklad:
- stratu súkromia spôsobenú interpersonálnou komunikáciou prostredníctvom elektronických médií,
- stratu sociálnych väzieb,
- nebezpečenstvo informačného pohltenia vyvolaného informačnou explóziou,
- existenciu informačnej vojny, či informačného „smogu“ so snahou o šírenie dezinformácií,
- zvýšený rozmach počítačovej kriminality s prvkami veľmi nebezpečnej trestnej činnosti organizovanej v kyberpriestore,
- možnú selekciu spoločnosti na informačne bohatých a chudobných z pohľadu ich počítačovej gramotnosti, či dostupnosti nových informačno-komunikačných technológií,
- rôzne filozofické, etické i zdravotné problémy.

Aj keď všetky zmeny súvisiace s informačnou spoločnosťou majú v konečnom dôsledku prispieť k zdokonaleniu manažérskej práce, v mnohých prípadoch to tak nie je. Dôvodov zo strany samotných manažérov môže byť hneď niekoľko. Zvyčajne sa prezentujú nasledovné príčiny:[5]

1. Sklon k rutine, pohodlnosť meniť zaužívané návyky. Ide o psychologický moment, ktorý sa dá očakávať, nakoľko býva v mnohých prípadoch sprievodným javom inovačných procesov.
2. Malá dôvera k moderným informačným technológiám vyplývajúca z neznalosti až neschopnosti ich správneho využívania.
3. Strach, obava z informácií. Manažéri radšej alibisticky zatvárajú oči pred nepríjemnými skutočnosťami a odvolávajú sa na rôzne objektívne príčiny, než aby urobili dôslednú analýzu javu na zlepšenie stavu.
4. Obava, že zlepšený tok informácií zabezpečený prostredníctvom informačných technológií by mohol vyvrátiť doposiaľ konštruované závery a koncepcie, za ktoré je zodpovedný príslušný manažér.

Uvedené skutočnosti sa v mnohých aspektoch dotýkajú aj iných ľudí, u ktorých zmeny súvisiace so zavádzaním informačno-komunikačných technológií do aplikačnej praxe prinášajú pocit neistoty a určité sociálne napätie. Historické skúsenosti totiž naznačujú istú tendenciu v prehlbovaní sociálnych rozdielov medzi členmi spoločnosti v závislosti od úrovne ich kvalifikácie, od úrovne tzv. počítačovej gramotnosti, ktorú je jej nositeľ schopný v novom prostredí využiť. Preto nosným cieľom informačnej spoločnosti je vytvorenie podmienok pre vznik racionálnej spoločnosti, v ktorej sa informácie využívajú na rozumné riešenie nielen individuálnych ale hlavne globálnych problémov.

Adaptácia jednotlivcov, či organizácií, resp. celej spoločnosti na toto nové informačné prostredie si nevyhnutne vyžaduje posilnenie požadovanej úrovne informačnej kompetencie, ktorá zodpovedá aktuálnym požiadavkám dnešnej doby. Zvládnutie a využitie informácií v rôznych oblastiach spoločenského života je pomerne zložité, pretože informácia má mnoho

[5] PORVAZNÍK, J. *Celostný manažment. Piliere kompetentnosti v riadení*. Bratislava: Sprint, 1999, s. 219-220.

foriem, líši sa rozmanitosťou zdrojov i technológií potrebných na jej spracovanie. Niekedy sa nielen ťažko kvantifikuje a meria, ale aj vyhodnocuje efektívnosť informačných systémov.[6]

Potreba informačnej kompetentnosti policajných manažérov

Dôležitosť otázok významu informačnej kompetentnosti policajných manažérov sa odráža a vychádza z viacerých nielen všeobecných ale aj špecifických faktorov, ktoré bez nároku na úplnosť možno argumentačne oprieť o nasledovné skutočnosti:[7]

Informačná podstata manažmentu

Manažment predstavuje informačné usmerňovanie a informačná charakteristika je jednou zo základných charakteristík procesu manažmentu. Informácie v procese manažmentu plnia v zásade dve úlohy, jednak umožňujú prípravu optimálneho rozhodnutia, jednak zabezpečujú jeho samotnú realizáciu.

Tendencie vo vývoji manažmentu

Pre manažment v informačnej spoločnosti nepostačuje aplikácia informačných technológií a zvládnutie spôsobov práce s nimi. Podstatne náročnejšia je potreba komplexného pochopenia úlohy informácií a s nimi prepojených vplyvov, ktoré menia podmienky našej existencie. Menia sa úlohy manažérov a spôsoby vykonávania doterajších činností. To podnietilo vznik informačného manažmentu, ktorý z manažérskych a systémových hľadísk skúma, projektuje a využíva kvalitatívne nové možnosti práce s informáciami. [8]

Informatizácia polície

Proces informatizácie štátnej správy sa v plnom rozsahu týka aj polície. Dôležité je pochopiť úlohu informačných technológií. Ako už bolo uvedené, to si vyžaduje zmenu spôsobu myslenia. Zásadnou chybou je nazerať na informačné technológie optikou svojich doterajších procesov: „Ako môžeme využiť tieto nové možnosti na zlepšenie, na zdokonalenie toho, čo robíme?“ Naopak, aplikácia informačných technológií vyžaduje zmenu procesov, ktoré v organizácii prebiehajú. Preto aj v polícii je potrebné klásť si správnu otázku, ktorou je: „Ako môžeme využiť informačné technológie na to, aby sme robili veci, ktoré sme doteraz nerobili?“

Zabezpečenie pozitívneho vývoja policajnej organizácie, útvaru

Úlohou policajného manažéra nie je iba zabezpečiť bezchybné fungovanie policajnej organizácie, ale aj byť iniciátorom zmien a motorom jej rozvoja, čo samozrejme bez efektívneho využívania informácií nie je možné.

Informačná podstata policajnej práce

Podstatou policajnej práce je práca s informáciami. Informácie sú pre políciu dôležitejšie ako čokoľvek iné. To akcentuje všeobecný poznatok o prínose informačných systémov a informačných technológií na skvalitnenie činnosti v akejkoľvek oblasti spoločenského života.

Tvorba a kultivácia informačných systémov

V neposlednom rade je informačná kompetentnosť potrebná aj z hľadiska tvorby a ďalšej kultivácie informačných systémov organizácie. Len informačne kompetentný manažér je schopný dať kvalifikované zadanie projektantom a realizátorom informačných systémov, a tým prispieť k vytvoreniu účelného, kvalitného a efektívneho informačného systému organizácie.

---

[6] LUKÁŠ, L., HRŮZA, P., KNÝ, M. *Informační management v bezpečnostních složkách*. Praha: MO ČR – AVIS, 2008, s. 11.

[7] BARIČIČOVÁ, Ľ., KRÁČMAR, J. Informačná kompetentnosť policajných manažérov. In: *Aktuální problémy managementu veřejné správy a metodologické předpoklady jeho rozvoje*. Sborník příspěvků z mezinárodní konference. Praha: PA ČR, 2004, s. 70-72.

[8] VODÁČEK, L., ROSICKÝ, A. *Informační management. Pojetí, poslání a aplikace*. Praha: Management Press, 1997, s. 7.

Efektívne fungovanie a využívanie informačných systémov

Z hľadiska efektívneho fungovania informačných systémov musí policajný manažér v rámci svojej pôsobnosti prioritne zabezpečiť nielen korektné vstupné údaje, ich korektné spracovanie ale aj správnu interpretáciu informácií.

Informačná autonómia

Súčasné informačné systémy a schopnosť manažéra priamo s nimi pracovať podstatne zvyšujú jeho informačnú autonómiu. Niektorí autori hovoria o informačnej samostatnosti manažéra.

Objektívna informovanosť

Informačné systémy zvyšujú objektívnu informovanosť policajného manažéra, nakoľko je podstatne menej závislý od informačného servisu svojich podriadených. To platí nielen pre rozhodovanie, ale aj pre ostatné manažérske funkcie.

Informačná kriminalita[9]

Informačné systémy a informačné technológie sú spojené s rizikom, že môžu byť zneužité pre kriminálne činy vrátane ohrozenia osobnosti i spoločnosti. To ale znamená, že musia byť vytvárané individuálne a spoločenské predpoklady pre minimalizáciu naznačených rizík.

V súvislosti s rozvojom informačných systémov a informačných technológií sa objavujú stále nové formy ich zneužívania, ktoré sú často vysokosofistikované a ich vyšetrovanie a dokazovanie je veľmi náročné. Počítačová kriminalita sa totiž od tzv. „klasickej" kriminality odlišuje celým radom osobitných charakteristík a zvláštností.[10] O to viac jej preto musí polícia a policajní manažéri venovať zvýšenú pozornosť.

Aj keď by bolo možné hľadať ďalšie argumenty podporujúce význam informačnej kompetentnosti policajných manažérov, všeobecne možno konštatovať, že v podmienkach modernej spoločnosti policajná organizácia potrebuje takých riadiacich pracovníkov, u ktorých nestoja v popredí len odborné vedomosti, ale hlavne 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]

Informačná kompetencia a jej odraz vo vzdelávacej a vedeckej činnosti katedry

Katedra informatiky a manažmentu Akadémie Policajného zboru v Bratislave sa v súlade s profilom absolventa akadémie zameriava na dôležité stránky všeobecnej prípravy špecialistov a riadiacich pracovníkov tak Policajného zboru a iných bezpečnostných služieb, ako aj verejnej správy. Patrí k nim najmä schopnosť využívať dostupné informácie a informačné systémy s využitím výpočtovej techniky a jej programového vybavenia, poznanie hlavných manažérskych činností a metód riadenia s dôrazom na vedenie ľudí, osvojenie si základných manažérskych kompetencií v oblasti riadenia jednotlivých úsekov policajných/ bezpečnostných služieb, resp. organizácií v pôsobnosti verejnej správy.

---

[9] V policajnej terminológii sa udomácnil pojem počítačová kriminalita. Otázkami tejto trestnej činnosti sa na pôde Akadémie Policajného zboru už v roku 1996 vôbec po prvýkrát zaoberal odborný seminár „Počítačová kriminalita a počítačová bezpečnosť", ktorý organizovala Katedra managementu a informatiky APZ v spolupráci s výskumným centrom počítačových nehôd HT Computers s. r. o. Bližšie viď zborník zo seminára. Bratislava: APZ, 1996, 103 s.

[10] HAJDÚKOVÁ, T., HRUŠKA, P. Pohľad na pripravenosť príslušníkov Policajného zboru na odhaľovanie a vyšetrovanie počítačovej kriminality. In: *Polícia ako garant bezpečnosti*. Zborník z medzinárodnej vedeckej konferencie. Bratislava: APZ, 2018, s. 88.

[11] BARIČIČOVÁ, Ľ. *Kompetencie policajných manažérov*. Bratislava: APZ, 2011, s. 88.

Vychádzajúc z hlavných zámerov moderného vzdelávania pre informačnú a znalostnú spoločnosť členovia katedry zaradení v skupine predmetov Informatika kladú dôraz na rozvoj informačnej kompetencie študentov potrebnej na podporu manažérskych rozhodnutí. Cieľom výučby v tejto oblasti je poskytnúť študentom ucelený systém vedomostí a intelektuálnych schopností, výsledkom ktorých je zvládnutie nielen základného pojmového aparátu z informatiky a príbuzných vied (teórie algoritmov, teórie informácií, všeobecnej teórie systémov, štatistiky a i.) nevyhnutných pre prostriedky či metódy zberu, spracovania a ochrany informácií, ale aj z problematiky informačnej bezpečnosti, auditu bezpečnosti informačných systémov a legislatívnych noriem upravujúcich predmetnú oblasť. Absolvovaním jednotlivých predmetov si študenti osvoja potrebné praktické návyky a zručnosti vo využívaní prostriedkov informačných technológií, ako aj vybraných policajných informačných systémov aktuálne používaných v odbornej činnosti špecialistu či riadiaceho pracovníka v podmienkach verejnej/štátnej správy.

Tomu logicky zodpovedá štruktúra predmetov, výučbu ktorých katedra aktuálne garantuje vo všetkých formách a stupňoch vysokoškolského vzdelávania. Ide o nasledovné povinné a povinne voliteľné predmety - *Informatika 1, Informatika 2, Praktická informatika, Moderné metódy spracovania informácií, Informačná bezpečnosť, Štatistické metódy, Informatika, Informačné systémy PZ.*

V rámci uvedených predmetov sa problematikou počítačovej bezpečnosti a ochrany pred kybernetickými hrozbami vyučujúci prioritne zaoberajú v predmete Informačná bezpečnosť v rozsahu 24 hodín v dennom magisterskom štúdiu (z toho 12 hodín prednášok a 12 hodín cvičení) a 12 hodín v externom magisterskom štúdiu (6 hodín prednášok a 6 hodín cvičení). Obsahová náplň predmetu sa všeobecne koncentruje na tie poznatky, ktorými by študenti ako budúci absolventi akadémie bez ohľadu na ich špecializáciu mali disponovať. Jednotlivé témy tvoria harmonický celok vychádzajúci v prvom rade z požiadaviek manažérskej praxe v rámci rezortu vnútra, resp. aj súkromnej sféry a plne reflektujú štandardy a normy platné pre túto oblasť (ako napríklad bezpečnostná politika, organizácia bezpečnosti, klasifikácia a riadenie aktív, personálna bezpečnosť, fyzická bezpečnosť a bezpečnosť prostredia, správa počítačov a sietí, systém riadenia prístupu, vývoj a údržba systémov, plány kontinuity činností a súlad požiadaviek bezpečnostnej politiky). Študenti po absolvovaní predmetu nadobudnú znalosti z problematiky informačnej bezpečnosti, auditu bezpečnosti informačných systémov a legislatívnych noriem. Aktuálne je tento predmet zaradený do ponuky povinne voliteľných predmetov s ambíciou stať sa v budúcnosti povinným predmetom, ktorý by následne absolvovali všetci študenti akadémie.

Do obsahu predmetu Informatika 1 v 1. ročníku bakalárskeho štúdia s časovou dotáciou 36 hodín v dennom štúdiu a 20 hodín v externom štúdiu je okrem iného zaradená problematika bezpečnosti dát a informačných technológií s cieľom priblížiť študentom otázky spojené s ochranou a bezpečnosťou súborov, zabezpečením dát v prostredí MS Windows, bezpečnosťou počítača a bezpečnou prácou vo virtuálnom prostredí prostredníctvom počítačových sietí.

Súčasťou predmetu Informatika 2 v 3. ročníku bakalárskeho štúdia je jedna prednáška na tému Informačná bezpečnosť z pohľadu manažérov s cieľom podporiť rozhodovacie kompetencie manažéra pri praktickom výkone riadiacej činnosti.

Čo sa týka špecializácie Vyšetrovanie v rámci špecializovaného policajného štúdia sú z celkovej dotácie predmetu Informačné systémy polície (8 hodín) na problematiku informačnej bezpečnosti vyčlenené 2 hodiny prednášky.

Okrem toho spomenúť treba aj riešenie danej problematiky v rámci semestrálnych prác študentov, ale hlavne v rámci katedrou vypísaných a študentom pridelených záverečných prác (či už bakalárskych alebo diplomových), ako napríklad:

- Neoprávnené prieniky do informačných systémov,
- Bezpečnosť počítačových sietí,
- Digitálne stopy,
- Bezpečnostné hrozby smart-zariadení,
- Sociálne inžinierstvo,
- Etický hacking,
- Osobné údaje v e-svete z hľadiska bezpečnosti a ochrany súkromia,
- Právne aspekty zneužívania anonymného prístupu do darknetových sietí na nelegálnu činnosť,
- Programy využívané pri riadení síl a prostriedkov PZ prostredníctvom operačného strediska,
- Komunikačné prostriedky v rezorte MV SR,
- Nežiaduce elektromagnetické vyžarovanie,
- Dieťa ako obeť trestnej činnosti páchanej online,
- Mediálna výchova detí ako spôsob prevencie proti negatívnym dopadom používania internetu,
- Riziká používania moderných komunikačných technológií deťmi a mládežou a podobne.

V rámci predmetov zaradených do skupiny Manažment sú otázky ochrany pred kybernetickými hrozbami a počítačovou kriminalitou sprostredkovane riešené v predmete Bezpečnostný manažment (8.3.1 Ochrana osôb a majetku) a Informačný manažment (8.3.2 Bezpečnostné verejno-správne služby).

V predchádzajúcom období boli na katedre úspešne obhájené 2 čiastkové vedeckovýskumné úlohy, ktoré sa či už priamo alebo nepriamo zaoberali otázkami počítačovej bezpečnosti a aktuálnymi hrozbami v kybernetickom priestore (*Ochrana detí vo virtuálnom prostredí* – zodpovedná riešiteľka mjr. RNDr. T. Hajdúková, PhD.; *Metódy ochrany policajne relevantných informácií* - zodpovedný riešiteľ mjr. JUDr. M. Kostrec, PhD.) Plnenie prvej úlohy naďalej pokračuje v rámci riešenia vedecko-výskumnej úlohy Výsk. 161 „Metódy spracovania policajne relevantných informácií“ s cieľom zisťovania hodnotovej orientácie detí a mládeže v spojitosti s informačnými technológiami a Internetom. Na plnení výskumných úloh v oblasti sexuálneho zneužívania detí online participujú aj pracovníci Prezídia Policajného zboru. Významným praktickým prínosom pre problematiku bezpečnosti online prostredia a kyberšikanovania je realizácia viacerých odborných prednášok spojených s besedami so žiakmi vybraných základných a stredných škôl, na ktorých študenti akadémie (prevažne z radov príslušníkov PZ) aktívne diskutujú o nebezpečenstvách spojených s prácou s modernými informačnými technológiami. S obdobným cieľom sa uskutočnili aj dve náučno-preventívne aktivity počas minuloročných letných prázdnin v rámci pobytu detí zamestnancov rezortu MV SR v letnom tábore organizovanom MV SR v Krupine a na Duchonke, ktoré boli cielene orientované na oblasti vhodného a bezpečného používania moderných informačných a komunikačných technológií deťmi. Na uvedenej akcii sa v rámci svojej odbornej praxe zúčastnili dvaja študenti 1. ročníka APZ - príslušníci PZ.

Záver

Jednou z najvýznamnejších výziev modernej informačnej spoločnosti je prevencia a boj proti počítačovej kriminalite. Preto je viac ako dôležité venovať týmto otázkam zvýšenú pozornosť tak na národnej ako aj medzinárodnej úrovni. V budúcnosti je možné predpokladať

vznik ďalších medzinárodných dokumentov dotýkajúcich sa rôznych prejavov počítačovej trestnej činnosti. Na účinný boj s nimi by bola potrebná globálna zmluva, ktorá by tak zaviedla nielen účinné nástroje a postupy v boji proti tejto kriminalite, ale zjednocovala by tiež trestné činy, ktoré by jednotlivé štáty museli implementovať do svojich právnych poriadkov.[12]

Zásadný obrat by takisto priniesla predovšetkým kvalitná príprava a posilnenie systému vzdelávania príslušníkov Policajného zboru v oblasti informačnej kompetentnosti, ktorá je nevyhnutná na zvládanie a praktické riešenie náročných a často neštandardných úloh delegovaných spoločnosťou pri zaisťovaní informačnej/počítačovej bezpečnosti, resp. ochrane života, zdravia a majetku občanov všeobecne.

Zoznam použitej literatúry:

BARIČIČOVÁ, Ľ. *Koncepcia rozvoja Katedry informatiky a manažmentu Akadémie PZ v Bratislave.* Bratislava: KIM, 2013. 16 s.

BARIČIČOVÁ, Ľ. *Kompetencie policajných manažérov*. Bratislava: APZ, 2011. 160 s. ISBN 978-80-8054-514-7

BARIČIČOVÁ, Ľ., KRÁČMAR, J. Informačná kompetentnosť policajných manažérov. In: *Aktuální problémy managementu veřejné správy a metodologické předpoklady jeho rozvoje*. Sborník příspěvků z mezinárodní konference. Praha: PA ČR, 2004, s. 70-72. ISBN 80-7251-174-2

HAJDÚKOVÁ, T., HRUŠKA, P. Pohľad na pripravenosť príslušníkov Policajného zboru na odhaľovanie a vyšetrovanie počítačovej kriminality. In: *Polícia ako garant bezpečnosti*. Zborník z medzinárodnej vedeckej konferencie. Bratislava: APZ, 2018, s. 86-96. ISBN 978-80-8054-751-6

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

LUKÁŠ, L., HRŮZA, P., KNÝ, M. *Informační management v bezpečnostních složkách*. Praha: MO ČR – AVIS, 2008, 214 s.

PORVAZNÍK, J. *Celostný manažment. Piliere kompetentnosti v riadení*. Bratislava: Sprint, 1999, 493 s. ISBN 80-8884-836-9

VODÁČEK, L., ROSICKÝ, A. *Informační management*. *Pojetí, poslání a aplikace*. Praha: Management Press, 1997, 146 s. ISBN 80-8594-335-2

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020

Odporúčanie Európskeho parlamentu a Rady Európskej únie o kľúčových kompetenciách pre celoživotné vzdelávanie (návrh) : Kľúčové kompetencie pre celoživotné vzdelávanie – európsky referenčný rámec (príloha). Brusel : Európsky parlament a Rada EÚ, 2006

Kontaktné údaje:

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

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

Vývoj informačnej bezpečnosti v Slovenskej republike – výsledky prieskumu 2006-2017

Benita Beláňová

Abstrakt:
Článok sa venuje problematike riadenia bezpečnosti informačných systémov v malých a stredných podnikoch Slovenskej republiky. Na základe celoštátneho prieskumu, uskutočneného v rokoch 2006,2008, 2012, 2015 a 2017 mapuje vývoj informačnej bezpečnosti v podnikoch SR, identifikuje najvážnejšie hrozby ohrozujúce bezpečnosť informačných systémov, a zároveň poukazuje na najzávažnejšie prekážky presadzovania bezpečnostnej politiky a bezpečnostných opatrení v oblasti IS/IT z pohľadu riadiacich pracovníkov podnikov.
Kľúčové slová:
Bezpečnosť, IT systémy, Internet, bezpečnostný incident, bezpečnostná politika, malé a stredné podniky

Abstract:
The article is devoted to the issue of the management of the security of information systems in small and medium-sized enterprises of the Slovak Republic. On the basis of a national survey, conducted in 2006, 2008, 2012, 2015 and 2017, charts the development of information security in the Slovak Republic, the most serious threat of endangering the safety of information systems, and identifies points on the most serious obstacles to the enforcement of the security policy and the security measures in the area of IS/IT from the perspective of managers of enterprises.
Key words:
Security, IT systems, Internet, Security incident, Security policy, Small and Medium-sized

Úvod

V dnešnej dobe sú informačné a komunikačné systémy tak zložité, rozsiahle a vzájomne poprepájané systémy, že ich bezproblémový chod musí byť zabezpečený vysoko odborným personálom. S týmito systémami však častokrát pracujú laickí používatelia, ohrozujú ich ľudské chyby a omyly, technické poruchy, prírodné živly, ale aj cielené útoky, či už zo strany nespokojných zamestnancov z vnútra organizácie, alebo hackerov a zlodejov z vonka. Podniky spracúvajú väčšinu svojich informácií, ktoré potrebujú pre vykonávanie svojej činnosti, pomocou informačných systémov. Viaceré z týchto informácií spadajú pod správu niektorej právnej normy legislatívy SR, takže i keby samotnej organizácii na svojich dátach až tak nezáležalo, sú povinní ich chrániť, aby neprišli do konfliktu so zákonom.

Z ohľadom na vplyv veľkých organizácií na národné hospodárstvo sa malé a stredné podniky javili ako nie príliš zaujímavý objekt skúmania a implementácie vedeckých poznatkov. Zmenu tohto prístupu spôsobili nové trendy, ktoré so sebou priniesla globalizácia a informatizácia. Informatizácia so sebou priniesla zároveň novú oblasť, ktorú je potrebné systematicky riadiť, a to bezpečnosť informačných systémov v podniku.

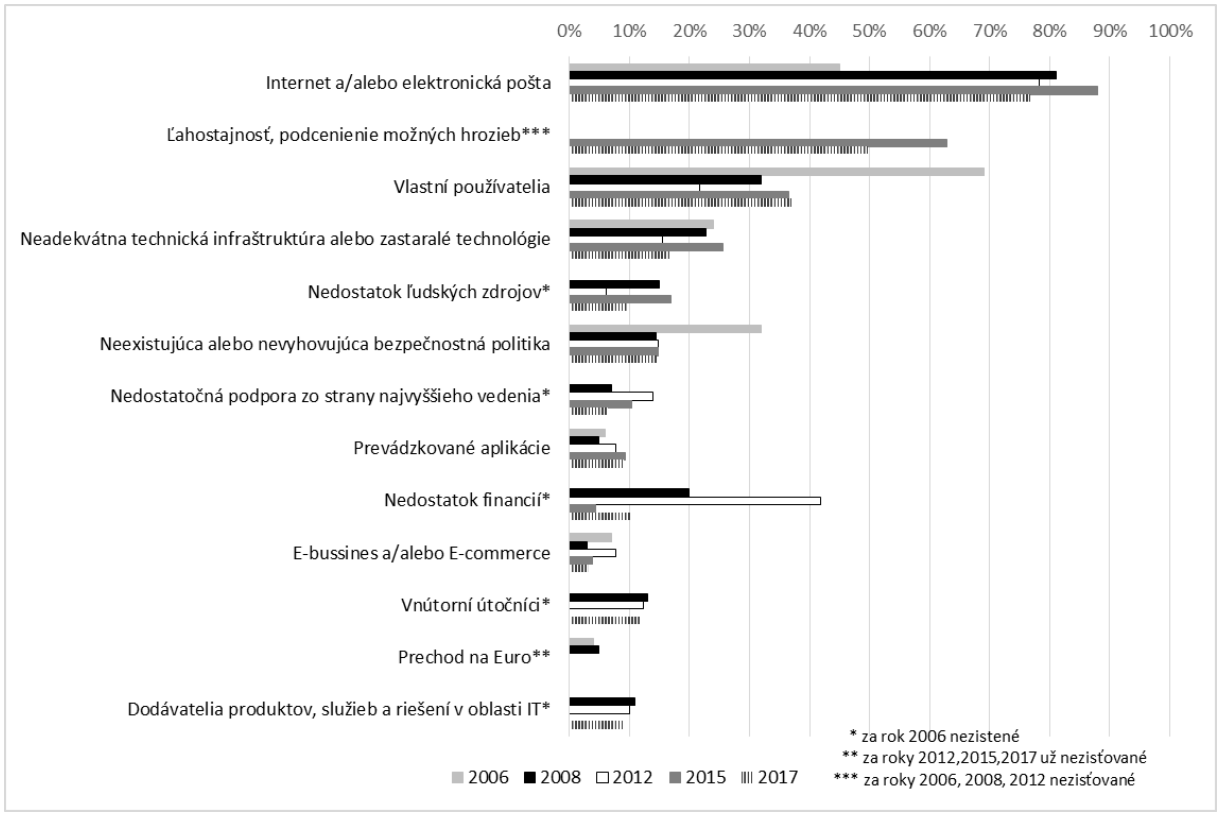
Bezpečnosť informačných systémov sa vo všeobecnosti zameriava najmä na ochranu informácií, prevenciu a detekciu neautorizovanej činnosti používateľov a počítačov, ale aj ochranu súkromia používateľov. S rozšírením moderných informačných a komunikačných technológii do všetkých oblastí života vzrástol význam riešenia bezpečnosti dát pri ich zbere, prenose, spracovaní a archivácii. Do povedomia riadiacich pracovníkov sa táto problematika dostala najmä vďaka zákonu č. 122/2013 Z. z. o ochrane osobných údajov (v informačných systémoch) a zákonu č. 215/2004 Z. z. o ochrane utajovaných skutočností a ich neskorších doplnení. Táto problematika je však oveľa širšia. O význame, ktorý je informačnej bezpečnosti prisudzovaný, svedčí aj stále rastúci záujem spoločností o koncipovanie, presadzovanie a implementáciu bezpečnostnej politiky. Aby sme si ju priblížili a zároveň overili stav informačnej bezpečnosti v podmienkach malých a stredných podnikov SR, uskutočnili sme prieskum, ktorého hlavným cieľom bolo identifikovať hrozby číhajúce na informačné systémy, spôsoby riešenia informačnej bezpečnosti a najzávažnejšie prekážky presadzovania bezpečnostnej politiky.

Charakteristika skúmanej vzorky

Prieskum bol realizovaný na vzorke náhodne vybraných malých a stredných podnikoch v Slovenskej republike. Dotazník bol vytvorený podľa vzoru prieskumu stavu informačnej bezpečnosti v podnikovej sfére v SR, ktorý vykonal Národný bezpečnostný úrad SR, v spolupráci s časopisom DSM – data security management a spoločnosťou Ernst & Young v rokoch 2006 a 2008.[1] Prieskum formou momentkového pozorovania a náhodného výberu má v porovnaní s cieleným oslovením vopred vybranej skupiny podnikov isté nedostatky, no objektívnosť výsledkov zvyšuje veľký počet podnikov a ich značná odvetvová rozmanitosť. V roku 2006 to bolo 387 podnikov, 2008 - 247 podnikov, 2012 – 129 podnikov, 2015 – 209 podnikov a v roku 2017 – 219 podnikov. Podľa právnej formy mali najväčšie zastúpenie spoločnosti s ručením obmedzeným. Podľa štruktúry vlastníkov prevládali podniky s výlučne domácim vlastníkom, resp. prevažujúcim domácim vlastníkom.

Najväčšie hrozby z hľadiska informačnej bezpečnosti

Najzraniteľnejšie miesta informačných systémov predstavujú komunikačné cesty najmä pri používaní otvorených prenosových systémov s možnosťami pripojenia do verejnej siete Internet alebo pri používaní mobilnej rádiovej siete. Toto neznižujúce sa riziko zo strany Internetu súvisí s rýchlym rozmachom tohto média.



Obrázok 1 Najväčšie hrozby z hľadiska informačnej bezpečnosti

Môžeme dokonca povedať, že Internet je najrýchlejšie sa rozvíjajúcim moderným médiom, ktoré oproti tradičným, ako sú televízia, rozhlas alebo tlač, disponuje mnohými výhodami a navyše stále novými technickými vylepšeniami. Pole pôsobnosti a šírka využitia Internetu sú takmer neobmedzené a na rozdiel od iných médií, dosahuje celosvetovú

[1] *PSIB SR ´08*, Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia. ISBN 978-80-969747-1-9 [cit. 2012-12-06] Dostupné na internete: < http://www.dsm.tate.cz/cz/psib-sr-2008/>

pôsobnosť. S narastajúcim počtom užívateľov sa preto prirodzene zvyšuje riziko prieniku do informačných systémov, k odcudzeniu, zneužitiu alebo poškodeniu dát v týchto systémoch.

Prieskum poskytol zaujímavý poznatok čo sa týka vlastných používateľov. Jedná sa o neúmyselné poškodenie niektorej súčasti informačného systému alebo technického zariadenia, ktoré súvisí s nevedomosťou človeka, či už ide o možné hrozby a dopady útokov na IS, alebo samotnú obsluhu technického zariadenia (v tomto prípade osobného počítača). Kým v roku 2006 predstavovali hrozbu v takmer 70tich percentách podnikov, do roku 2012 mal klesajúcu tendenciu – dostal sa takmer na úroveň 20tich percent, čo svedčilo o narastajúcom povedomí pracovníkov v oblasti informačnej bezpečnosti a o zvyšujúcom sa dôraze manažmentu na túto oblasť. Žiaľ od tohto roku môžeme opäť sledovať postupný mierny nárast, ktorý, ako sa domnievame, spôsobila hospodárska kríza a s ňou spojené šetrenie podnikov aj v oblasti bezpečnosti. Je zrejmé, že zamestnanci si túto skutočnosť uvedomujú, pretože viac ako polovica respondentov v roku 2015 aj 2017 sa domnieva, že k problematike bezpečnosti IS/IT sa pristupuje ľahkovážne a možné hrozby sa podceňujú.

Riešenie informačnej bezpečnosti IS

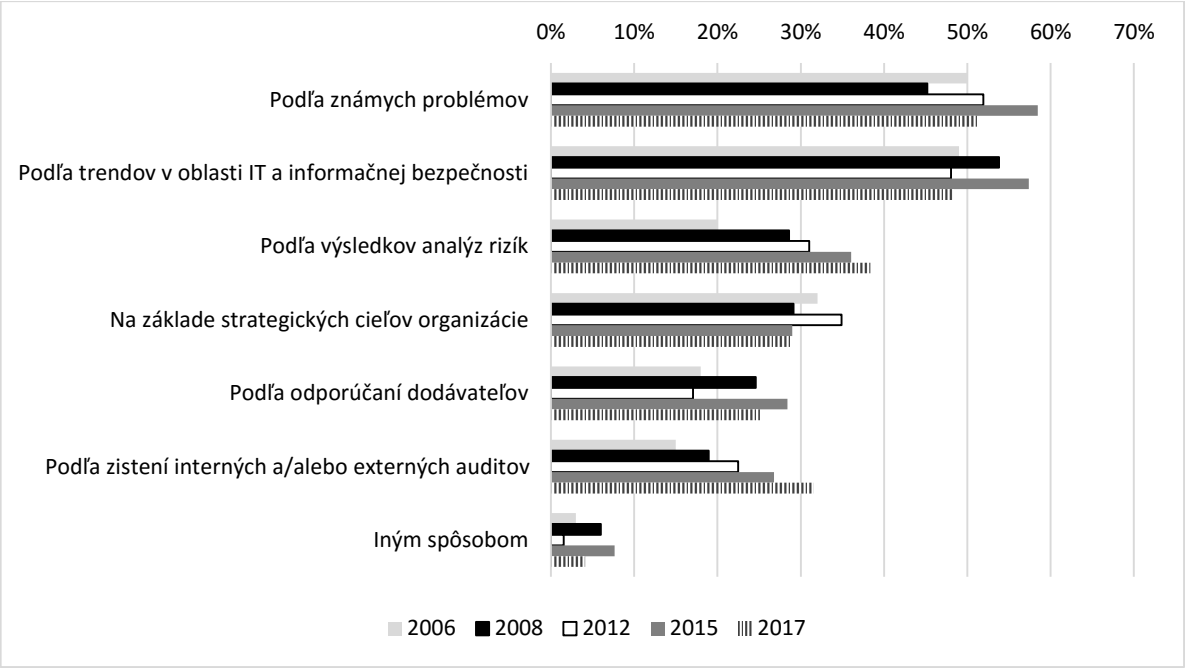
Manažment podnikov sa pri definovaní priorít pre oblasť informačnej bezpečnosti prevažne riadi trendmi v oblasti informačných technológií a informačnej bezpečnosti a podľa známych problémov, ktoré v tom ktorom období rezonujú v spoločnosti. Väčšinou to bývajú nové legislatívne úpravy, ovplyvňujúce najmä dáta a spôsob ich spracovania v informačných systémoch, alebo nové formy tzv. „počítačovej kriminality“, ktoré ohrozujú samotnú podstatu IS. Mohli by sme dokonca povedať, že podniky sa správajú nepredvídavo, pretože väčšinou reagujú až na vzniknutý problém. Potešiteľným faktom je, že k výsledkom zistení z interných alebo externých auditov, prípadne analýzy rizík, prihliada pri riešení informačnej bezpečnosti stále viac malých a stredných podnikov. V ostatných oblastiach sa ich percentuálne zastúpenie významnejšie počas rokov nemení. Ani strategické ciele podniku pri riešení informačnej bezpečnosti, v porovnaní s rokom 2012, výrazne poklesli, čo možno považovať za nebezpečný ukazovateľ, nakoľko by tieto oblasti mali byť úzko prepojené.

Významnú skupinu tvoria podniky, ktoré sa s analýzou rizík IS nikdy nezaoberali, alebo ju neriešili v posledných dvoch rokoch, čo pri rýchlom vývoji v IS/IT oblasti sa prakticky rovná „nule“. Nepostačujúci stav informačnej bezpečnosti si uvedomujú aj samotné podniky. Väčšina sa domnieva, že úroveň informačnej bezpečnosti, v porovnaní zo západoeurópskymi štátmi, je horšia, dokonca v niektorých prípadoch ju hodnotia ako výrazne horšiu. Pozitívom je nárast podielu skupiny podnikov, ktoré hodnotia úroveň rovnako ako v ekonomicky vyspelejších krajinách.

Malé a stredne veľké spoločnosti tvoria špecifické prostredie z pohľadu presadzovania a riadenia informačnej bezpečnosti. Rozdiely oproti veľkým spoločnostiam sú tým väčšie, čím je spoločnosť menšia:[2]

- žiadny alebo minimálny bezpečnostný tím,
- rozpočet na bezpečnosť je súčasťou rozpočtu na IT alebo nie je tvorený vôbec,
- rozsah finančných, časových a ľudských zdrojov pridelených na informačnú bezpečnosť je nižší, z dôvodu minimalizácie výdavkov je potrebné využívať open-source projekty,
- riadenie bezpečnosti býva vykonávané oddelením IT.

[2] DEKÝŠ, P. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti.* In: e-Focus, ISSN 1336-1805, 2010, roč. 10, č. 3, s. 12-13



Obrázok 2 Spôsob definovania priorít pre oblasť informačnej bezpečnosti

Tieto skutočnosti potvrdil aj náš prieskum, ktorý ukázal, že útvar zabezpečujúci výhradne oblasť informačných technológií a systémov vo všeobecnosti, majú väčšinou stredné podniky, u malých je tento podiel len okolo 23%. Väčšinou majú len osobu, ktorá na pozícii tzv. správcu siete, ktorý sa stará o chod informačných systémov v podniku. Podniky, ktoré nemajú takýto útvar alebo správcu, majú tieto služby zabezpečované externou firmou a rovnako ako pri správe siete sa táto forma v podnikoch čoraz viac preferuje. V tejto skupine sú zahrnuté všetky odvetvia, takže nemôžeme povedať, že by to bolo pre niektoré odvetvie špecifické.

Zameranie bezpečnostnej politiky v podniku

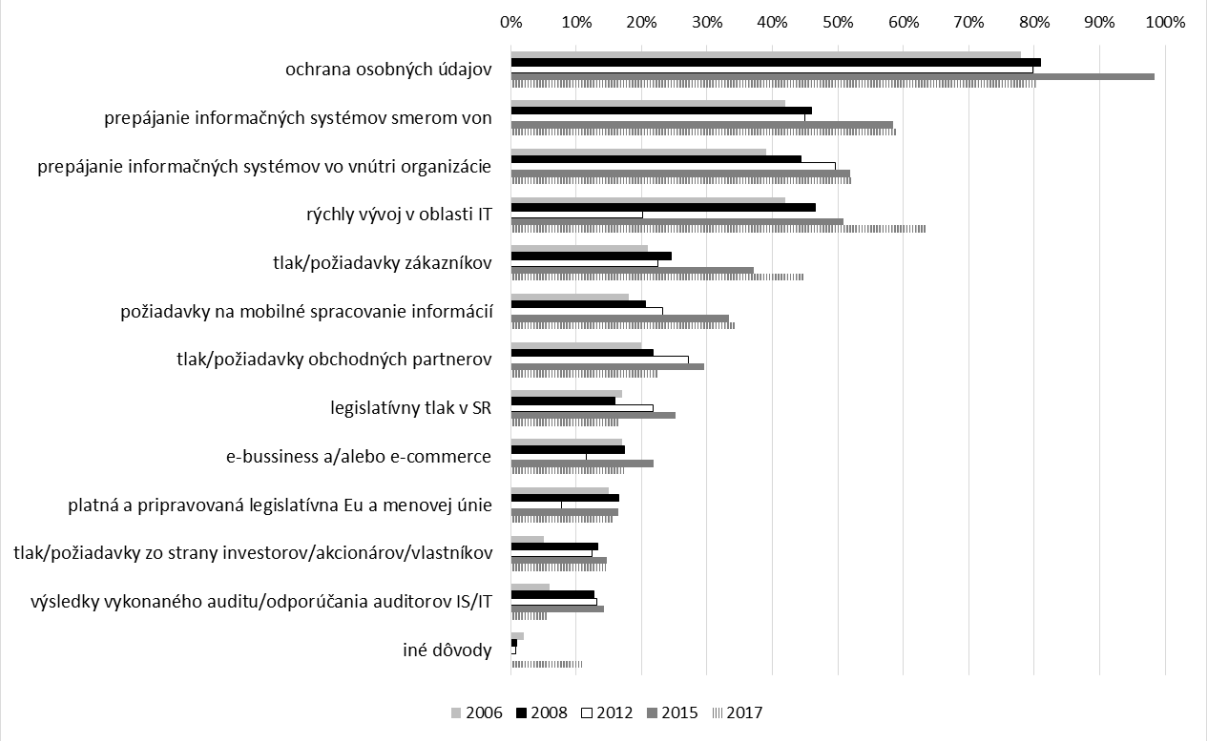
Problematika bezpečnostnej politiky sa chápe ako problém čisto počítačových odborníkov, resp. pracovníkov fyzickej bezpečnosti. Informácie v automatizovaných systémoch sú však len vrcholným stupňom v hierarchii toho, čo je potrebné chrániť. Netreba zabúdať na samotné priestory, v ktorých sú informácie a informačné systémy uložené, tak isto archívne priestory, areál organizácie a pod.

Môže sa stať, že bude dochádzať k stretu dvoch aktivít - bezpečnostné ciele totiž nemusia byť totožné s obchodnými cieľmi a vo všeobecnosti sa ani vzájomne nepodporujú. Napriek tomu musia ciele bezpečnostného riadenia vychádzať v ústrety cieľom obchodným.[3] Taktiež je potrebné si uvedomiť, že bezpečnosť nie je najdôležitejším produktom organizácie, ale je len postupným krokom k stabilizácii obchodných aktivít. Je vhodné, nie povinné, spracovať bezpečnostnú politiku informačných technológií, ktorá bude vychádzať z bezpečnostnej politiky celej organizácie.

Základné bezpečnostné ciele, prípadne globálne bezpečnostné dokumenty organizácie uľahčujú hodnotenie a analýzu bezpečnosti a návrh opatrení. Bezpečnostná politika musí byť chápaná ako súhrn princípov a východísk pre strategické riešenia. Predstavuje základ na zaistenie informačnej bezpečnosti. Politika predstavuje východiskový bod pre návrh a realizáciu všetkých úspešných štandardov, smerníc, procedúr a opatrení. Všetky analýzy sú však zbytočné, ak nenájdu svoje uplatnenie v bezpečnostných opatreniach a nie sú

[3] TVRDÍKOVÁ, M. *Aplikace moderních informačných techologií v řízení firmy*. Praha: Grada Publishing, a.s., 2008. 176 s. ISBN 978-80-247-2728-8

východiskom pre bezpečnostnú politiku. Ako ukázal prieskum, je zarážajúce, že výsledky vykonaného auditu, resp. odporúčania audítorov IS/IT nepovažujú organizácie za významný faktor vplývajúci na informačnú bezpečnosť. Pričom výsledky by mali byť súčasťou tak štúdie informačnej bezpečnosti, ako aj výsledného bezpečnostného projektu.



Obrázok 3 Okolnosti najviac vplývajúce na presadzovanie informačnej bezpečnosti

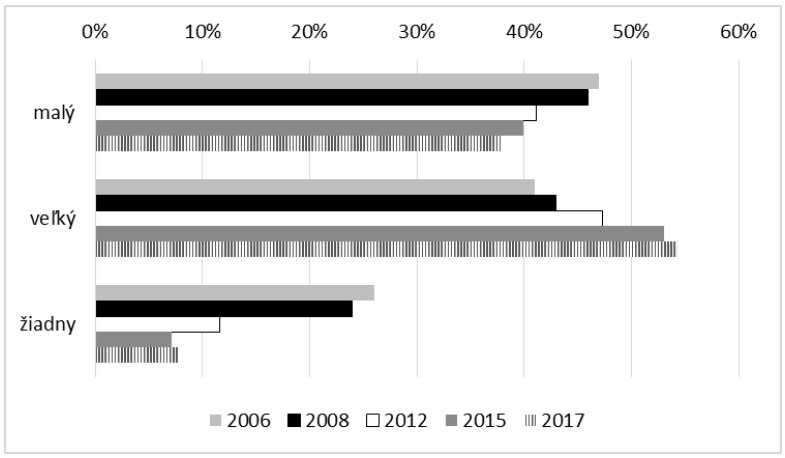
V rámci bezpečnosti IS a ochrany dát v nich uložených musíme tieto dáta rozdeliť do dvoch kategórií:

- informácie a dáta, ktoré tvoria know-how podniku a je v jeho záujme tieto údaje, zvyšujúce konkurenčnú výhodu, chrániť;
- a dáta, ktorých ochrana je zákonom upravená a podnik je povinný ich chrániť.

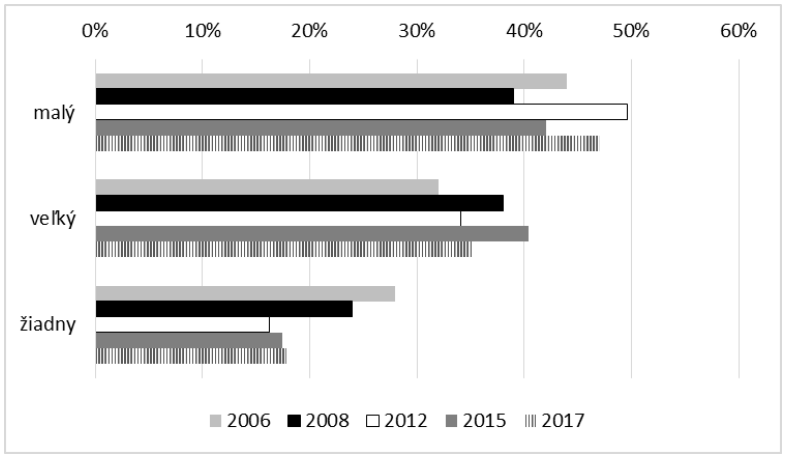
Z dlhodobého hľadiska sa táto skutočnosť odzrkadľuje aj na okolnostiach, ktoré najviac vplývajú na presadzovanie informačnej bezpečnosti. Sú to najmä už spomínané zákony č. 122/2013 Z. z. (resp. 428/2002) o ochrane osobných údajov (v informačných systémoch) a zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a ich neskorších doplnení. Ako môžeme vidieť z nasledujúcich grafov vplyv týchto zákonov na informačnú bezpečnosť z roka na rok narastá. Čiastočne to ovplyvňujú aj legislatívne úpravy týchto zákonov, ktoré ich neustále pritvrdzujú, rovnako aj sankcie za ich porušenie.

Podľa §19 zákona č. 212/2013 Z. z. (resp. §16 zákona č. 428/2002 Z. z.) o ochrane osobných údajov v znení neskorších predpisov, musí organizácia dokonca prijať opatrenia vo forme bezpečnostného projektu informačného systému a zabezpečiť jeho vypracovanie, ak sú v informačnom systéme spracúvané osobitné kategórie osobných údajov (napr. rodné číslo, zdravotné údaje, členstvo v odborových organizáciách) a informačný systém je prepojený na verejne prístupnú počítačovú sieť (Internet), alebo je prevádzkovaný v počítačovej sieti, ktorá je prepojená na verejne prístupnú počítačovú sieť.[4]

[4] Zákon č. 212/2013 Z.z. o ochrane osobných údajov. [cit. 2015-12-06] Dostupné na internete: <http://www.dataprotection.gov.sk/ uoou/sites/default/files/kcfinder/files/ 136_2014.pdf>



Obrázok 4 Vplyv zákona č. 122/2013 Z.z. (resp. č.428/2002) o ochrane osobných údajov na informačnú bezpečnosť



Obrázok 5 Vplyv zákona č. 215/2004Z.z. o ochrane utajovaných skutočností na informačnú bezpečnosť

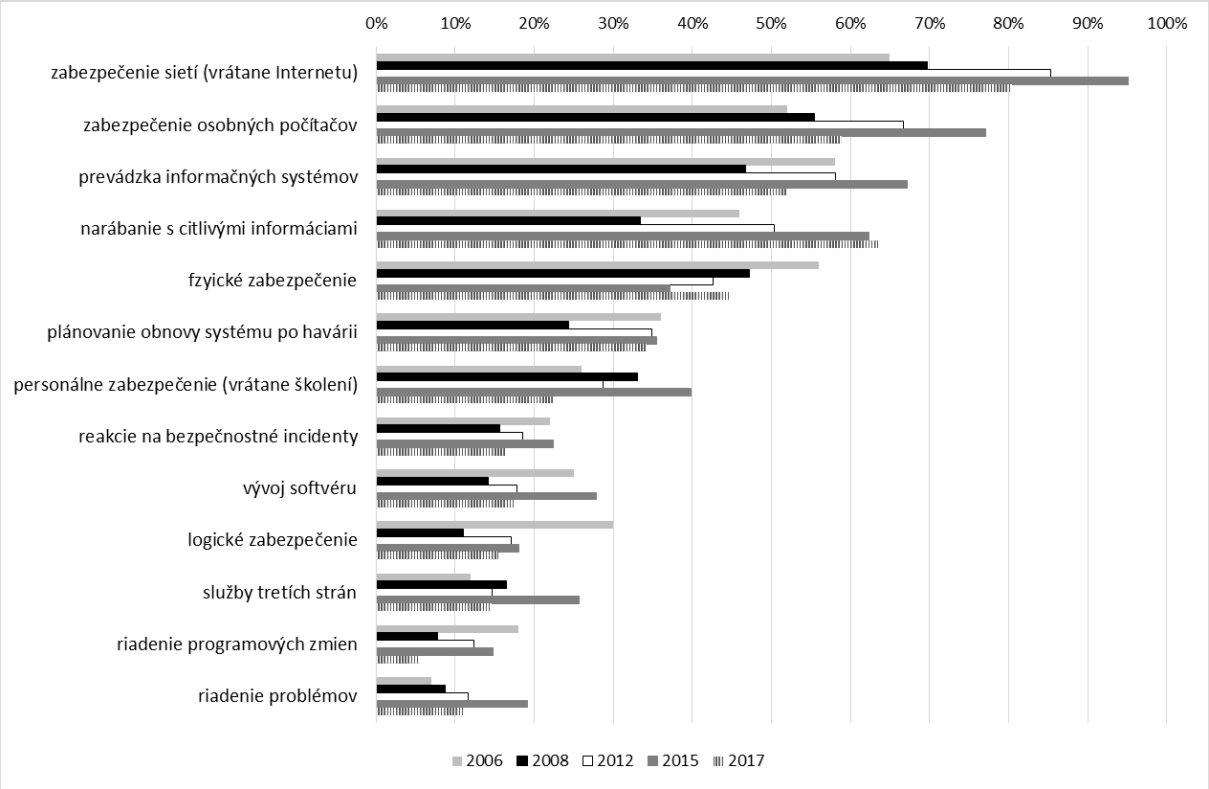
Okolnosti, ktoré najviac vplývajú na informačnú bezpečnosť by sa mali odzrkadľovať v bezpečnostnej politike podniku. Ako môžeme dobre vidieť z obrázku 6, podniky, vzhľadom na zvyšujúce sa riziká plynúce z e-komunikácie a internetu, v rámci zamerania svojej bezpečnostnej politiky upriamili pozornosť hlavne na zabezpečenie sietí, či už vnútorných alebo vonkajších. Významne však pokleslo v rámci bezpečnostnej politiky logické zabezpečenie. Z prieskumov taktiež vyplynulo, že rovnako ako pri identifikácii hrozieb, aj v oblasti bezpečnostnej politiky môžeme konštatovať, že rozsah implementácie výrazne neovplyvňuje odvetvová ani veľkostná štruktúra podniku. Napriek tomu, že bezpečnostná politika reflektuje na rodiace sa hrozby a požiadavky z okolia, konštatujeme, že v súčasnosti len štyri oblasti sú pokryté u viac ako 50% podnikov. Tento stav nemôžeme považovať za dostatočný.

Ak sa manažment spoločnosti rozhodne seriózne zaoberať bezpečnostnou politikovu, je potrebné, aby si ujasnil základné body:[5]

• vymedziť zásadné *ciele, stratégie a politiky* na informačné zabezpečenie organizácie,
• stanoviť *požiadavky* na informačné zabezpečenie organizácie,
• určiť právomoci a zodpovednosti,

[5] LUKÁČ, Ľ. *IT manažment*. Praha: Computer Press, 2011. 208 s. ISBN 978-80-251-3378-1

• identifikovať a analyzovať *hrozby* informačných aktív organizácie,
• identifikovať a analyzovať *riziká* plynúce z prevádzky IS,
• určiť primerané *bezpečnostné opatrenia* znižujúce riziká na prijateľnú úroveň.



Obrázok 6 Rozsah bezpečnostnej politiky

Následne treba zabezpečiť:
• *sledovanie* implementácie bezpečnostných opatrení a prevádzka IS so zavedenými bezpečnostnými opatreniami,
• zavedenie programu na *zvyšovanie kvalifikácie* užívateľov IS v oblasti informačnej bezpečnosti,
• *sledovanie a zaznamenávanie všetkých bezpečnostných incidentov* a pokusov o ne s vyvodením patričných dôsledkov.

Personálne zabezpečenie oblasti informačnej bezpečnosti

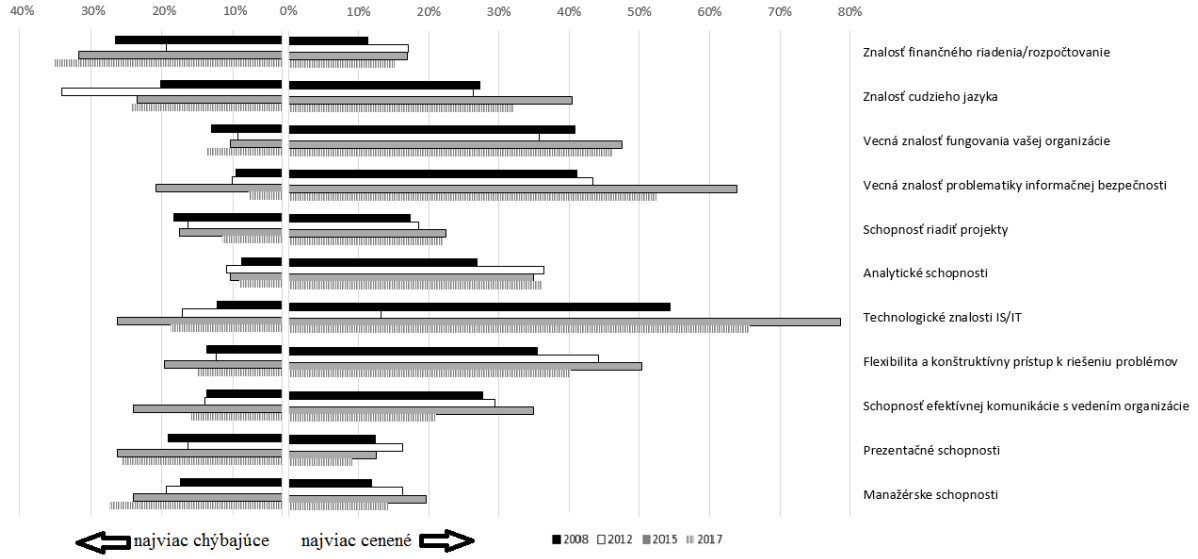
Kvalitné personálne zabezpečenie je jednou zo základných a nevyhnutných podmienok uplatňovania bezpečnostnej politiky IS v podniku, preto je nutné na tento faktor klásť obzvlášť dôraz. Konkrétne na definíciu, vytvorenie a personálne obsadenie rolí, ktoré v spoločnosti zabezpečujú kontinuálny rozvoj informačnej bezpečnosti v súlade s novými legislatívnymi prvkami, organizačnými zmenami resp. rozvojom spoločnosti, zmenami IS a v súlade so samotnou bezpečnostnou dokumentáciou.

Kľúčové role, ktoré v praxi predstavujú primárnu zložku každého systému riadenia informačnej bezpečnosti musia rešpektovať existujúce prvky riadenia v spoločnosti (napr. líniové resp. procesné riadenie, odborná spôsobilosť atď.)[6]. Vytvorenie týchto rolí nemusí nutne vyžadovať vytvorenie a obsadenie nového pracovného miesta, často krát sa priraďuje nová rola existujúcim pracovníkom. Je však dôležité, aby príslušné role zabezpečovali vymáhateľnosť

[6] KOUBEK, J. *Řízení lidských zdrojů*. Praha: Management Press, 2015. 400 s. ISBN 978-80-726-1288-8

pravidiel a zásad špecifikovaných v bezpečnostnej politike a ich praktickú aplikáciu a dodržiavanie.

Útvar zabezpečujúci výhradne oblasť informačných technológií a systémov vo všeobecnosti, majú väčšinou stredné podniky, u malých je tento podiel malý. Väčšinou majú len osobu, ktorá je na pozícii tzv. správcu siete, ktorý sa stará o chod informačných systémov v podniku. Podniky, ktoré nemajú takýto útvar alebo správcu, majú tieto služby zabezpečované externou firmou. Za samotnú bezpečnosť IS najmä u malých podnikov, ktoré využívajú externé IS/IT služby nezodpovedá nikto (žiadny útvar). Podniky využívajúce správcu siete prenášajú zvyčajne zodpovednosť na ekonomický a finančný útvar.



Obrázok 7 Znalosti a schopnosti pracovníkov v oblasti informačnej bezpečnosti - najviac chýbajúce/najviac cenené*

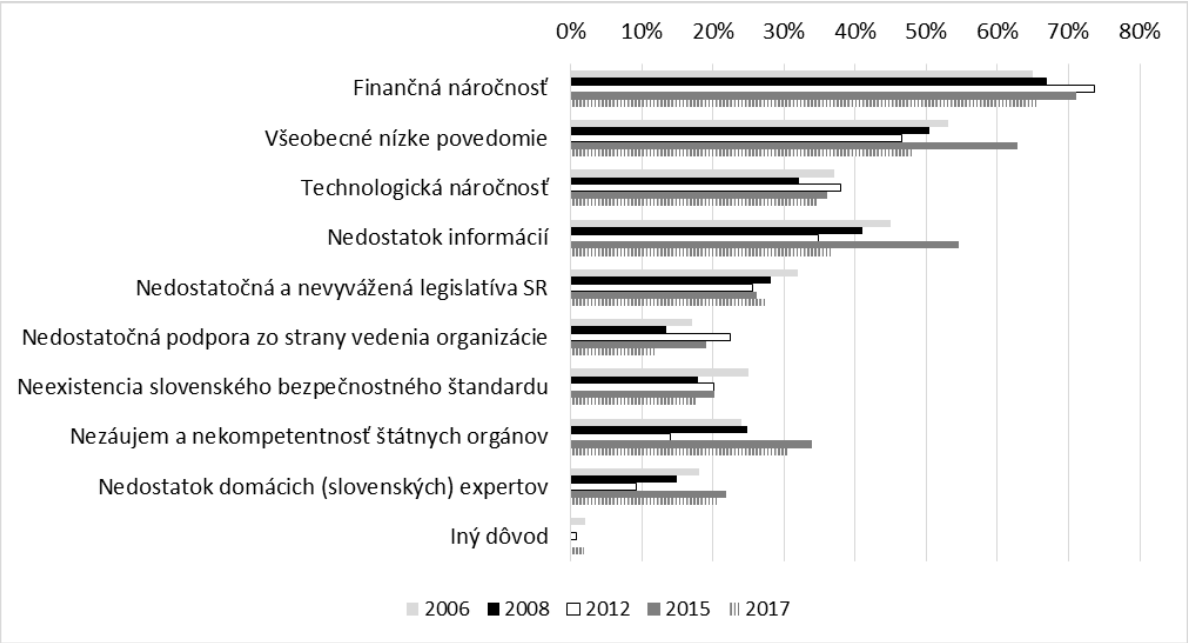
Pri porovnávaní najviac cenených a naopak najviac chýbajúcich znalostí a schopností pracovníkov z oblasti zabezpečenia informačných systémov sme zistili výraznejší nedostatok znalostí a vedomostí pracovníkov z oblasti finančného riadenia podniku, čo však nepovažujeme za tak významný faktor v oblasti IS/IT. Horšie je to v oblasti technologických znalostí IS/IT a znalostí cudzieho jazyka, ktoré patria medzi kľúčové znalosti pracovníkov IS/IT. Čo sa týka počtu takýchto pracovníkov v organizácii, 1/4 podnikov považuje existujúci stav za nepostačujúci. Výrazné zmeny v počte týchto pracovníkov zaznamenalo v priemere len desatina podnikov. Zhoda medzi odbornosťou a požiadavkami je u 2/3 podnikov. Pri ostatných zručnosti zodpovedajú len čiastočne, alebo vôbec nie.

Prekážky presadzovania informačnej bezpečnosti

Zodpovední pracovníci sa domnievajú, že medzi najvýznamnejšie faktory, brzdiace presadzovanie bezpečnostnej politiky v podnikoch, sú - veľmi nízke bezpečnostné povedomie, chýbajúce finančné prostriedky na dôsledné dodržiavanie pravidiel bezpečnostnej politiky, a taktiež by uvítali slovenský bezpečnostný štandard. Naopak z prieskumu vyplynulo, že sa slovenské podniky nemôžu sťažovať na nedostatok kvalifikovaných odborníkov, ktorí by zvládli technologicky náročné a stále sa zdokonaľujúce informačné a komunikačné technológie, i keď podiel tohto faktora stúpol v roku 2015 a 2017 o vyše 10%. So zvyšujúcim sa povedomím o problematike informačnej bezpečnosti sa zvyšuje aj dopyt po informáciách.

* v roku 2006 nezisťované

Neznamená to však, že informácií je menej. Práve naopak. Poukazuje to len na skutočnosť, že ak o probléme nevieme, tak nepátrame po riešení.



Obrázok 8 Najväčšie prekážky presadzovania informačnej bezpečnosti v SR

Záver

Účinné riadenie bezpečnosti informačných systémov je v súčasnom podnikateľskom prostredí čoraz kritickejšia oblasť. S narastajúcou technologickou úrovňou informačných systémov sa priamoúmerne zlepšujú techniky a nástroje narúšajúce tieto systémy, čoho dôsledkom je potreba vyšších investícií do ochranných prostriedkov. Taktiež zvyšujúci sa podiel tzv. neovplyvniteľných hrozieb, ako sú prírodné katastrofy, ktoré čoraz častejšie postihujú územie Slovenskej republiky, ale aj okolitých štátov, kladie na problematiku informačnej bezpečnosti ešte vyšší dôraz. Prieskum odhalil, že úroveň informačnej bezpečnosti v Slovenskej republike je vo vzťahu k západoeurópskym štátom významne horšia.

Každý z veľkých podnikov pôsobiacich na Slovensku disponuje IT oddelením, ktoré sa zaoberá otázkami ochrany informácií podniku, analyzuje a vyhodnocuje hrozby, ktoré sa v tejto oblasti vyskytujú a tvorí súbory opatrení zameraných na ich limitovanie a elimináciu. Malé a stredné podniky v SR však takýmito oddeleniami nedisponujú. Pritom však napadnutie alebo poškodenie ich vnútropodnikového informačného systému je pre ne priam likvidačné. Ako ukazujú výsledky prieskumu, aj malé a stredné podniky musia venovať viac pozornosti otázkam zabezpečovania bezpečnosti informačných technológií, ktoré v rámci vnútropodnikových komunikačných tokov používajú ako aj výberu komunikačných nástrojov, ktoré transfer informácií umožňujú. Ako základné východisko na zachovanie ich informačnej bezpečnosti sa ukazuje ich pripravenosť riešiť aj nepredvídateľné situácie a schopnosť zachovať takú mieru rizika, ktorá je pre podnik znesiteľná.

Príspevok bol spracovaný v rámci riešenia projektu VEGA 1/0309/18 - Sociálne siete v riadení ľudských zdrojov.

Zoznam použitej literatúry:

DEKÝŠ, P. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti*. In: e-Focus, ISSN 1336-1805, 2010, roč. 10, č. 3, s. 12-13

KOUBEK, J. *Řízení lidských zdrojů*. Praha: Management Press, 2015. 400 s. ISBN 978-80-726-1288-8

LUKÁČ, Ľ. *IT manažment*. Praha: Computer Press, 2011. 208 s. ISBN 978-80-251-3378-1

TVRDÍKOVÁ, M. *Aplikace moderních informačných techologií v řízení firmy*. Praha: Grada Publishing, a.s., 2008. 176 s. ISBN 978-80-247-2728-8

PSIB SR ´08, Ernst & Young, NBÚ SR, DSM – data security management, TATE International Slovakia. ISBN 978-80-969747-1-9 [cit. 2012-12-06] Dostupné na internete: < http://www.dsm.tate.cz/cz/psib-sr-2008/>

Zákon č. 212/2013 Z.z. o ochrane osobných údajov. [cit. 2015-12-06] Dostupné na internete: <http://www.dataprotection.gov.sk/ uoou/sites/default/files/kcfinder/files/ 136_2014.pdf>

Kontaktné údaje:

Ing. Benita Beláňová, PhD.
Katedra informačného manažmentu
Fakulta podnikového manažmentu
Ekonomická univerzita v Bratislave
benita.belanova@euba.sk

Kybernetická kriminalita a možnosti prevencie

Miroslav Brvnišťan

Abstrakt:
Kybernetická kriminalita ako novodobý fenomén čoraz výraznejším spôsobom zasahuje do života spoločnosti a štátu. Dôsledky často nie sú priamo identifikovateľné a brániť sa je zložité. Obeť sa nachádza v novej situácii, kedy štandardný bezpečnostný systém a jeho výkonné zložky neposkytujú požadovanú mieru bezpečnosti. Latentnosť kybernetickej kriminality, jej špecifickosť a sofistikovanosť kladú nové požiadavky na činnosť bezpečnostných zložiek. Kybernetická bezpečnosť ako integrálna súčasť prevencie kybernetickej kriminality zároveň redefinuje vzťah štát verzus občan a zvýrazňuje nutnosť spolupráce so súkromným sektorom. Článok analyzuje vybrané aspekty a stav oblasti kybernetickej kriminality, poukazuje na špecifiká oblasti prevencie a navrhuje možnosti riešenia.[1]
Kľúčové slová:
Kybernetická kriminalita, prevencia, latentnosť, kybernetická bezpečnosť, policajný zbor

Abstract:
Cybercrime as a modern phenomenon is increasingly affecting the life of society and the state. Consequences are often not directly identifiable and prevention is being complex. The victim is in a new situation where the standard security system and its executive components do not provide the required security level. The latentness of cybercrime, its specificity and sophistication put new demands on the operation of security components. Cyber security as an integral part of cyber crime prevention redefines the relationship between the citizen and the state and highlights the need for cooperation with the private sector. The article analyzes selected aspects and the state of cyber crime, highlights the specifics of the area of prevention and proposes solutions.
Key words:
Cyber crime, prevention, latentness, cyber security, police corps

Úvod

Nárastom používania moderných informačných a komunikačných systémov (napr. počítače, mobily, tablety) a rastúcou informatizáciou spoločnosti a štátu predstavuje kybernetická kriminalita čoraz väčšiu hrozbu pre používateľov a ochranu ich osobných údajov, citlivých dát a súkromia. Postupne zasahuje do všetkých oblastí života spoločnosti. Práca s počítačmi a informačnými systémami, zdieľanie informácií, osobných údajov a fotografií na sociálnych sieťach, používanie aplikácií, nakupovanie z pohodlia domova, či sledovanie aktuálnych informácií na internete, sa stáva čoraz viac integrálnou súčasťou našich životov. Množstvo bezpečnostných hrozieb narastá úmerne postupujúcej informatizácii.

Bezpečnosť a ochrana pred kybernetickou kriminalitou, ktorá postupne zasahuje do všetkých oblastí života spoločnosti, predstavuje čoraz väčšiu výzvu aj pre bezpečnostné zložky štátu. Bezpečnosť, tak ako sme ju privyknutí vnímať, sa mení a je tomu potrebné prispôsobiť zaužívané nástroje ochrany a prevencie, prípadne vytvoriť a aplikovať nové.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý nadobudol účinnosť dňa 01. 04. 2018 je súčasťou opatrení, ktoré SR prijala v rámci postupných krokov smerujúcich k budovaniu bezpečnosti kybernetického prostredia SR. Zákon nesporne vytvára základ systémového prístupu na úrovni štátu k riešeniu problematiky kybernetickej bezpečnosti. Samotný zákon však bezpečnosť nezaručí. Bude potrebné realizovať množstvo súvisiacich krokov. Niektoré takéto kroky už boli definované v Koncepcii kybernetickej bezpečnosti a v Akčnom pláne realizácie koncepcie kybernetickej bezpečnosti na roky 2015 - 2016[2]. Jednou

[1] Tento príspevok je podporovaný Agentúrou na podporu výskumu a vývoja na základe Zmluvy č. APVV – 16-0521.

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

z dôležitých oblastí, ktorú je potrebné rozpracovať, je bezpečnosť občana v kybernetickom prostredí, čo úzko súvisí so schopnosťami bezpečnostných zložiek odhaľovať a objasňovať trestnú činnosť páchanú v kybernetickom prostredí.

Ako má však postupovať občan, ak je obeťou kybernetickej kriminality?

Štandardné procesy a postupy, vytvorené pre podmienky materiálneho sveta sa javia ako pomalé a neefektívne. Občan je často odkázaný na pomoc súkromných spoločností a fyzických osôb. Ako takýmto situáciám predísť? Prevencia ako oblasť, ktorá môže situácii napomôcť, je v oblasti kybernetickej bezpečnosti zatiaľ systematicky neaplikovaná a nevyužívaná.

Je pritom zrejmé, že charakter kybernetickej kriminality vyžaduje realizáciu špecifických preventívnych opatrení tak, aby bolo možné efektívne predchádzať páchaniu moderných foriem trestnej činnosti v kybernetickom priestore.

Pojmy počítačová kriminalita a kybernetická kriminalita sú pre účely tohto článku používané subsidiárne, rovnocenne, v kontexte situácie, ktorú popisujú. Pod pojmom počítač sa pritom rozumie aj mobilný telefón, tablet a iné zariadenia fungujúce na obdobnom princípe.

Kybernetická kriminalita - charakteristika

Pod pojmom počítačová kriminalita (čoraz viac používaný pojem kybernetická) rozumieme jednak trestné činy zamerané proti počítačom, a jednak nepriamu počítačovú kriminalitu, teda trestné činy páchané pomocou počítača, niektorým z jeho komponentov, prípadne väčšieho množstva samostatných počítačov alebo počítačov prepojených do počítačovej siete.

Samotný pojem počítačová kriminalita nie je explicitne definovaný v Trestnom zákone[3] alebo v obdobnom normatívnom právnom akte. Pre potreby právnej praxe sa preto využívajú termíny a definície vedy trestného práva, kriminalistiky a kriminológie. Platný a účinný Trestný zákon však pozná a definuje skutkové podstaty jednotlivých trestných činov, ktoré spolu tvoria právny rámec pre počítačovú kriminalitu na Slovensku.

Pre účely slovenských trestnoprávnych predpisov sa vychádzalo z definície obsiahnutej v Dohovore rady Európy o počítačovej kriminalite, ktorý dňa 01. 08. 2007 ratifikovala slovenská vláda. Touto normatívnou zmluvou, ktorá je pre Slovenskú republiku záväzná z hľadiska medzinárodného práva a európskeho práva, je počítačová kriminalita (angl. Computer Crime alebo Cyber Crime) vymedzená nasledovne: „Počítačová kriminalita je akékoľvek nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. Ide o veľmi všeobecné definovanie, no vzhľadom na nie celkom jasné hranice oblasti kybernetického priestoru pravdepodobne postačujúce.

Z pohľadu autora tohto článku kybernetickú kriminalitu je možné stručne charakterizovať prostredníctvom činností páchateľov zameraných na:

1. Získanie informácií a dát,
2. Poškodenie informácií a dát,
3. Získanie kontroly nad počítačom za účelom aktivít podľa bodov 1. a 2.

Od klasickej kriminality sa počítačová kriminalita odlišuje viacerými zvláštnosťami a osobitnými charakteristikami, ktoré je potrebné brať v úvahu v procese zameriavania a realizácie opatrení bezpečnostných zložiek a prevencie:

[3]Zákon Národnej rady SR č. 300/2005 Z. z. o Trestnom zákone (Trestný zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

I. Počítačová kriminalita sa vyznačuje veľkou anonymitou páchateľov, vzdialenosťou páchateľa a obete, v mnohých prípadoch aj časovým odstupom medzi konaním a následkom trestného činu, a často presahuje hranice jedného štátu. Trestné činy páchané pomocou počítača možno spáchať za relatívne krátky čas bez toho, aby sa páchateľ nachádzal na mieste činu. Využívaním počítačov a internetu sa zmenili podmienky páchania trestných činov, ako aj typy páchateľov a obetí.

II. Počítačová kriminalita patrí medzi najmenej ohlasované druhy trestnej činnosti, vyznačuje sa vysokou latentnosťou, ktorá sa podľa prieskumov pohybuje až v medziach 90%.

Odhaduje sa, že OČVTK sa dozvedia len o 10 percentách z celého jej množstva. Obete zo súkromného sektora spravidla nemajú záujem nahlásiť možnú trestnú činnosť a riskovať následné zverejnenie skutočnosti, že boli napr. obeťou hackerov alebo kybernetického útoku, alebo sa obávajú škôd na povesti a dobrom mene, zvýšenej nedôvery verejnosti a následných ekonomických škôd (napr. banky).

Sekundárna viktimizácia sa tak stáva rozsiahlejšou než prvotná. Pramení to nielen z dôvodu neochoty obetí tieto trestné činy oznamovať, či z obtiažnosti obete identifikovať a lokalizovať, ale aj z rôznych iných dôvodov. Obete počítačovej kriminality napr. často používajú nelegálny software alebo inak porušujú autorské práva a boja sa odhalenia. Takáto neochota oznamovať trestnú činnosť pritom zvyšuje množstvo páchanej počítačovej kriminality.

III. Obete počítačovej kriminality sa často nedozvedia, že sú alebo boli predmetom útoku páchateľov (napr. ak došlo k odcudzeniu ich osobných údajov) a v niektorých prípadoch je dôvodom aj nedostatok právneho povedomia, čo má za následok, že obeť nevie, že predmetné konanie je trestným činom.

IV. Viktimizácia nemusí byť však v každom prípade zistená, veľké množstvo počítačových útokov je vykonávaných spôsobom, ktorý obmedzuje alebo znemožňuje rozpoznanie (napríklad vo forme rôznych spyware). Zistiť, že sa niekto stal obeťou počítačovej trestnej činnosti je zložité a bez technických znalostí spravidla takmer nemožné. V prípade koncových užívateľov bez základného bezpečnostného povedomia často ani k odhaleniu nepríde. Odhaľovanie páchateľov počítačovej kriminality je v zásade zložité. Túto trestnú činnosť páchajú predovšetkým mladí ľudia, ktorí majú odborné i praktické skúsenosti z oblasti výpočtovej techniky. Ide najmä o mužov vo veku od 15 do 35 rokov, bez záznamu v registri trestov.

V. Špecifikom je aj povaha nástrojov, teda technológií, ktoré sú použité k páchaniu tejto trestnej činnosti, a ktoré sú zároveň aj jej terčom. Sú relatívne ľahko dostupné (najmä pokiaľ uvažujeme o softvérovom pirátstve – CD, DVD, Blu-ray mechaniky s možnosťou zápisu a iné), čím umožňujú páchanie trestnej činnosti bez zložitejšej prípravy každému. Určitým aspektom je nesporne aj nízka kúpyschopnosť obetí, a teda ich neochota (neschopnosť) zaobstarať si bezpečné a originálne produkty. Ochrana a zabezpečenie hardvéru a softvéru, informácií a osobných údajov je finančne nákladná, a teda často zanedbávaná oblasť, čím dochádza k uľahčovaniu páchania počítačovej trestnej činnosti.

VI. Výška prípadnej škody je ťažko zistiteľná a vyčísliteľná. Typickým je nedostatok dôkazného materiálu, spravidla dochádza k okamžitej likvidácii stôp. Dôkazný materiál je špecifický a jeho zaisťovanie znamená vyššie nároky na orgány činné v trestnom konaní. Pri útokoch na vybrané objekty je takmer s istotou možné vylúčiť svedka, a tým sťažiť zisťovanie, odhaľovanie a vyšetrovanie.

VII. Na strane užívateľov, a teda potencionálnych obetí, sa vyskytujú, ako jednotlivé fyzické osoby, tak osoby právnické, korporácie či štátne inštitúcie (známy útok hackerov na Národný bezpečnostný úrad, viacero útokov na bankový, finančný a poisťovací sektor).

Dôvodov, prečo je tomu tak, je viacero. Fungovanie orgánov štátnej a verejnej správy, samosprávy je dnes takmer v celom rozsahu digitalizované, pričom väčšina informácií je aj vysoko dôvernej povahy (vrátane osobných údajov) a je uchovávaná elektronicky.

VIII. S uvedeným súvisí aj možnosť páchať kybernetické trestné činy vo veľmi krátkom časovom intervale - v priebehu niekoľkých sekúnd, bez nutnej prítomnosti páchateľa na mieste činu s tým, že poškodený - obeť spáchanie takéhoto činu ani nemusí postrehnúť. Typickým je aj nedostatok dôkazného materiálu, dochádza spravidla k okamžitej likvidácii stôp. Dôkazný materiál je ťažko dostupný a zaistiteľný, čo znamená vyššie nároky na orgány činné v trestnom konaní. Pri útoku na cielený objekt je možné takmer absolútne vylúčiť svedka, a tým sťažiť zisťovanie, odhaľovanie a vyšetrovanie.

IX. Miesto činu kybernetickej kriminality je často neidentifikovateľné a odlišné od miesta páchania, bez fyzickej prítomnosti páchateľa, vrátane medzinárodných prvkov - tzv. dištančná forma kriminality. Medzinárodná spolupráca orgánov činných v trestnom konaní sa stáva nevyhnutnou - prevažná väčšina kybernetickej kriminality má cezhraničný charakter. Orgány činné v trestnom konaní musia preto prispôsobiť postupy pri vyšetrovaní, štandardné vyžiadanie právnej pomoci z cudziny je viac ako pomalé a je pravdepodobné, že by došlo ku omeškaniu, ktoré by mohlo celé trestné konanie zmariť.

X. Digitálna forma stôp podstatne uľahčuje páchateľovi zahladenie stôp spôsobených spáchaním trestného činu. Zmeny, ktoré spôsobí konanie páchateľa v prípadoch počítačovej kriminality možno veľmi ľahko a jednoducho odstrániť, zmanipulovať alebo skresliť. To znamená, že odhalenie páchateľa počítačovej kriminality je veľmi náročné.

XI. Premisa: Každý bezpečnostný incident v kybernetickom prostredí má potenciál byť trestným činom. Bezpečnosť kybernetického prostredia je oveľa komplexnejšou ako sa na prvý pohľad zdá. Zaužívané postupy bezpečnostných zložiek, ktoré poznáme z fyzického sveta sú nedostatočné a neefektívne. Nahlásenie kybernetického incidentu občanom by malo byť základným právom občana. Povinnosť bezpečnostných zložiek vytvoriť podmienky na efektívne prijímanie takýchto oznámení - berúc v úvahu špecifiká kybernetickej kriminality a takéto podnety preverovať a dokumentovať, by mala byť samozrejmá.

V súčasnosti je možné identifikovať, podľa viacerých kritérií, nasledujúce základné - známe formy počítačovej kriminality, ktoré rámcovo poukazujú na stav v popisovanej oblasti:

- útoky na počítač, program, údaje, komunikačné zariadenia a siete,
- neoprávnené získavanie programov a dát,
- neoprávnené využívanie počítačov alebo komunikačných zariadení,
- neoprávnený prístup k osobným údajom a informáciám,
- získavanie utajovaných informácií,
- zneužívanie sociálnych sietí,
- zmena v programoch a dátach,
- softvérové pirátstvo,
- krádež počítača, programu, údajov a komunikačných zariadení,
- zneužívanie počítačov na páchanie akejkoľvek inej trestnej činnosti,
- šírenie poplašných a nepravdivých správ, šírenie detskej pornografie.

Nejedná sa o konečný výpočet všetkých druhov kybernetickej kriminality, nové formy neustále pribúdajú a súvisia najmä s technologickým a technickým pokrokom. Cieľom je však poukázať na široké spektrum už známych druhov a na základe toho odvodiť, navrhnúť možnosti preventívnych opatrení.

Pri zohľadnení štatistických ukazovateľov počítačovej kriminality SR je zrejmé relatívne nízke percento zistenej (latentnosť) a následne aj objasňovanie počítačovej kriminality. Za rok 2016 bolo zistených približne 230 trestných činov počítačovej kriminality, objasnených bolo približne 40%, pričom v porovnaní z prechádzajúcim obdobím je trendom mierny rast. Tento stav zodpovedá situácii, kedy sa spoločnosť a bezpečnostné zložky nezaoberajú efektívnymi spôsobmi reagovania na zmeny bezpečnostnej situácie a vytváraniu účinných nástrojov na predchádzanie počítačovej kriminality. Štatistiky v rámci SR nezodpovedajú vývojovým tendenciám v medzinárodnom meradle. Dôvodom môže byť väčšia miera latentnosti (neochoty alebo neznalosti obetí o možnostiach nahlasovania kybernetickej trestnej činnosti).

Viaceré prieskumy v oblasti informačnej bezpečnosti naznačujú narastanie významu ochrany osobných údajov, ochrany databáz a citlivých informácií, know-how a pod. Výsledky prieskumov naznačujú, že dôraz bude musieť byť kladený na koncového užívateľa (ľudský faktor), ktorý predstavuje najväčšie bezpečnostné riziko[4]. Na nárast významu vzdelávania a budovania bezpečnostného povedomia zamestnancov (koncových užívateľov) poukazuje aj prieskum stavu informačnej bezpečnosti spracovaný Ministerstvom financií SR v roku 2013[5]. Ako je vo výstupoch prieskumu konštatované, poučenie zamestnancov o pravidlách bezpečného používania informačných systémov by malo byť štandardnou súčasťou bezpečnostných opatrení v každej inštitúcii. Prispieva k budovaniu bezpečnostného povedomia zamestnancov a pomáha predchádzať chybám, neželaným následkom a odvracaniu škôd.

Trendy rastu počítačovej kriminality a dôležitosti jej predchádzania potvrdzuje aj štatistika počítačovej kriminality EÚ, zameraná na obyvateľov EÚ[6], podľa ktorej:

74% obyvateľov EÚ si myslí, že môžu byť obeťou počítačového zločinu,
59% cíti, že nie je informovaná o rizikách kybernetického priestoru,
40% sa obáva zneužitia osobných údajov,
12% bolo podvedených online,
8% bola odcudzená identita,
53% si nezmenilo heslá za posledný rok,
52% používa sociálne siete,
48% využíva online banking.

V kontexte iných medzinárodných štatistík[7] je zrejmé aj nasledovné:

a) Globálne škody spôsobené počítačovou kriminalitou budú narastať a do roku 2019 môžu dosiahnuť až 2 bilióny dolárov.
b) Podstatná časť trestnej činnosti ostane nezistená, a to najmä v oblasti nelegálneho získavania citlivých a utajovaných informácií.
c) Bude narastať množstvo únikov osobných informácií. Celkovo sa odhaduje, že tento druh trestnej činnosti rastie ročne približne o 38%.
d) Narastať budú sofistikované útoky (najmä phishing, ransomware) s cieľom získavať informácie o platobných kartách, prístupové heslá k mailovým kontám, sociálnym sieťam a informačným systémom.

[4] Pozri bližšie napr. Desiaty ročník Globálneho prieskumu spoločnosti Ernst & Young o informačnej bezpečnosti www.efocus.sk/images/archiv/file_1183_0.pdf.
[5] Pozri www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c
[6] Pozri bližšie http://recent-ecl.blogspot.fr/2012/07/cybercrime-new-eu-statistics.html:
[7] Pozri bližšie https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

Vzhľadom na uvedené, je možné konštatovať, že z pohľadu obetí počítačovej kriminality je situácia zložitá. Na jednej strane postupujúca informatizácia spoločnosti, technický a technologický pokrok logicky generujú podmienky pre rast kybernetickej kriminality (modernej kriminality), na druhej strane spoločnosť a bezpečnostné zložky nereagujúce primerane z hľadiska ochrany a budovania bezpečnosti občana.

Je zrejmý čoraz väčší kontrast medzi zaužívanými spôsobmi fungovania a budovania bezpečnostných zložiek a novým, dynamicky sa meniacim bezpečnostným prostredím. Bez zásadných zmien nebude možné efektívne predchádzať, odhaľovať a objasňovať nové moderné formy kriminality, medzi ktoré nesporne možno zaradiť kybernetickú kriminalitu.

Štatistické ukazovateľ potvrdzujú, že potencionálnych obetí pribúda, podstatná časť je neidentifikovaná, a to bez ohľadu na dôvody - obeť nevie čo sa stalo, vie ale neoznámi takýto trestný čin, bojí sa alebo nedôveruje bezpečnostným zložkám. Situáciu dokresľuje stav, kedy na jednej strane máme štatistiky súkromných spoločností, nadnárodných zoskupení (napr. EÚ), ktoré poukazujú na nárast kybernetickej kriminality a tendencie vývoja a na druhej strane, štatistiky bezpečnostných zložiek SR zohľadňujúce len niektoré formy kybernetickej kriminality. Reálny stav v spoločnosti je neznámy, a to najmä s ohľadom na vysokú latentnosť kybernetickej kriminality. Tento pomyselný kruh nie je možné vyriešiť bez prijatia adekvátnych opatrení, a to najmä v oblasti prevencie. Prevencia aj s ohľadom na uvedené bude pravdepodobne vždy účinnejšia ako samotný boj s kybernetickou kriminalitou. Výber vhodných metód prevencie a jej zamerania predstavuje samostatnú výzvu a komplexnú pre kompetentné orgány.

Kybernetická kriminalita a ľudský faktor

V súlade s údajmi v predchádzajúcej kapitole je možné konštatovať, že medzi základné príčiny počítačovej kriminality patrí **nízke bezpečnostné povedomie obetí**, **vysoká anonymita a nízke právne povedomie páchateľov.**

Človek je tým, kto môže najviac v kybernetickom prostredí ohroziť bezpečnosť svoju alebo iných, a to konaním alebo nekonaním. Je potrebné brať primerane v úvahu aj základné technické príčiny kybernetickej kriminality napr. zastaranosť a neaktualizovanie používaných softvérov, nepoužívanie antivírusových programov, nedostatočné bezpečnostné nastavenia, relatívna dostupnosť sofistikovaných technických prostriedkov a iné. Neskúsení užívatelia počítačov v mnohých prípadoch z dôvodu svojej „technologickej a bezpečnostnej negramotnosti“ zanedbávajú ochranu počítačov a informačno-komunikačných nástrojov, prípadne o možných kybernetických hrozbách vôbec nevedia. Ako príklad možno uviesť „smartphony“, o možnostiach relatívne jednoduchého zneužitia ktorých mnoho používateľov často ani netuší.

Je zrejmé, že práve ľudský faktor zohráva kľúčovú úlohu pri páchaní kybernetickej kriminality.

Ľudský faktor je nesporne vo všeobecnosti považovaný za najväčšie bezpečnostné riziko. Nevzdelaný jednotlivec, nerešpektujúci zásady a princípy bezpečnosti je najväčším bezpečnostným rizikom. Kľúčom na zlepšenie bezpečnosti jednotlivcov a v konečnom dôsledku aj kybernetického priestoru je podľa nášho názoru budovanie bezpečnostného povedomia.

Tak ako spoločnosť dokázala vytvoriť systém vzdelávania pre fyzický svet, je potrebné vytvoriť systém vzdelávania pre kybernetický priestor a zohľadniť jeho špecifiká. Je to cesta, akou je možné s primeranými nákladmi efektívne čeliť novodobým bezpečnostným hrozbám a nenechať sa ukolísať falošným pocitom bezpečnosti. Ak nastane bezpečnostný incident, je už spravidla neskoro a škody môžu byť zničujúce. Pre ďalšie úvahy týkajúce sa ľudského faktora budeme vychádzať z platnej premisy, že akýkoľvek bezpečnostný incident má potenciál byť

trestným činom a môže mať trestno-právne dôsledky[8]. Závisí od schopností a stavu bezpečnostného prostredia, či takýto incident vieme zistiť, vyhodnotiť, zaistiť dôkazy a zadokumentovať spôsobom využiteľným v procese trestného konania. Zároveň tu platí, že prevencia kriminality je lepšia než liečba, a jednoznačne je i lacnejšia.

Predchádzanie bezpečnostným incidentom v kybernetickom prostredí je pravdepodobne základným aspektom umožňujúcim predchádzanie kybernetickej kriminality. Máme však za to, že opätovne je potrebné brať v úvahu ľudský faktor - vzdelaný jednotlivec je nápomocný, vie posúdiť dôsledky svojho konania alebo nekonania, vie ako postupovať v prípade bezpečnostného incidentu.

Bezpečnostné povedomie

Pojem bezpečnostné povedomie je historicky najčastejšie spájaný s informačnou bezpečnosťou, bezpečnosťou informačných systémov a bezpečnosťou informácií. V týchto oblastiach ide o proces zavedený s ohľadom na praktické skúsenosti či už súkromného alebo verejného sektora.

Bezpečnostné povedomie je v oblasti informačnej bezpečnosti definované ako: "Poznanie potreby ochrany informácie a informačnej a komunikačnej infraštruktúry, ako aj povinnosti osobne sa na nej podieľať"[9]. Univerzálnejšia definícia bezpečnostného povedomia znie: "Uvedomenie si a postoj členov organizácie vo vzťahu k ochrane rôznych hodnôt organizácie" alebo "Dosiahnutie udržateľného postoja zamestnancov vo vzťahu k bezpečnosti, a zároveň budovanie dôvery vo vlastnú organizáciu"[10]. Vychádzajúc z uvedených definícií je možné zovšeobecniť definíciu bezpečnostného povedomia aj pre účely predchádzania kybernetickej kriminality.

V súlade s uvedenými definíciami mať príslušné bezpečnostné povedomie pre účely predchádzania kybernetickej kriminalite môže znamenať, že jednotlivec:

1. Chápe podstatu bezpečnosti v kybernetickom priestore,
2. Uvedomuje si potencionálne hrozby,
3. Má vedomosť o tom, ako hrozbám predchádzať,
4. V prípade, že takéto okolnosti nastanú, vie ako reagovať.

Praktický výsledok je, že jednotlivec vie ako sa správať pri používaní počítačov. Ak nastane bezpečnostný incident, vie ako má konať - vrátane ohlásenia takejto trestnej činnosti a spolupráce s Policajným zborom.

Bezpečnostné povedomie sa vo všeobecnosti javí ako možný efektívny nástroj na elimináciu moderných bezpečnostných rizík, čo má vo finálnom dôsledku dopad na oblasť páchania kybernetickej kriminality. Primerané bezpečnostné povedomie znamená, že zohľadňuje množstvo aspektov týkajúcich sa určitej (definovanej) skupiny koncových užívateľov počítačov - napr. podľa veku alebo schopností ovládania počítačov.

Vzdelávanie a osveta ako základ prevencie počítačovej kriminality

Postupy ako dosiahnuť primerané bezpečnostné povedomie koncových užívateľov počítačov nie sú stanovené a ani nie sú systematickou súčasťou vzdelávacieho procesu.

V prípade ich vypracovania by tieto mali obsahovať podrobnejšie rozpracovanie oblasti bezpečnostného povedomia, štruktúru a obsahové zameranie bezpečnostného vzdelávania - napr. základné bezpečnostné pravidlá, pravidelné oboznamovanie sa s aktuálnymi hrozbami,

[8] Porovnaj s §3 písm. j) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov - bezpečnostný incident.

[9] Podrobnejšie pozri normu ISO 27001:2013 Systém riadenia bezpečnosti informácií, Organizácia bezpečností informácií, Bezpečnosť z hľadiska ľudských zdrojov - Povedomie, vzdelávanie a príprava.

[10] www.sansecurity.com, 2015

dôsledkami kompromitácie informácií, postup pri bezpečnostných incidentoch, spôsob ohlasovania trestnej činnosti spojenej s používaním počítačov a iné.

Cieľom by malo byť vytvorenie uceleného programu bezpečnostného vzdelávania a budovania bezpečnostného povedomia koncových užívateľov počítačov. Takýto vzdelávací program by mal využívať moderné, cielené a zrozumiteľné prístupy k výučbe, tréningu a systematickému vzdelávaniu, aby časovo nenáročným, nevtieravým, a pritom systematickým spôsobom postupne menil vnímanie bezpečnosti a budoval dlhodobo udržateľný postoj jednotlivca vo vzťahu k bezpečnosti v kybernetickom priestore.

Podľa nášho názoru práve v súčasnosti vzniká dostatočný priestor na zadefinovanie a inkorporovanie bezpečnostného vzdelávania do vzdelávacieho systému SR.

Bezpečnostné povedomie je však možné vnímať ucelenejšie a aj na kvalitatívne vyššej úrovni. Potom možno hovoriť o budovaní tzv. kultúry bezpečnosti na úrovní štátu. Kultúra bezpečnosti vo všeobecnosti vypovedá o miere a spôsobe naplnenia a osvojenia si cieľov a úloh v oblasti bezpečnosti, ich dosahovania, kontroly a rozvoja. Kultúra bezpečnosti komplexne určuje rozsah a vzory základných riešení, hodnôt, noriem, štandardov, symbolov a názorov vplývajúcich na spôsob prístupu k bezpečnostným hrozbám a k riadeniu bezpečnosti na všetkých hierarchických úrovniach bezpečnostného systému štátu. Zavádza stereotypy pre bezpečné správanie sa ľudí ako v každodennom živote doma, na verejnosti či na pracovisku, tak aj v krízových situáciách. Je súčasťou jednotného vzťahu: ”Kultúra bezpečnosti - bezpečnostné povedomie - bezpečné správanie”[11].

Pri dostatočne etablovanej kultúre bezpečnosti a primeranom bezpečnostnom povedomí jednotlivcov je možné vytvoriť efektívny systém predchádzania a eliminovania moderných bezpečnostných hrozieb a kybernetickej kriminality, vrátane bezpečnosti kybernetického priestoru.

V širšom kontexte vnímania bezpečnostného povedomia a možností predchádzania kybernetickej kriminalite je preto potrebné brať v úvahu aj zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti[12]. Je však nutné obozretne vnímať ciele a zámer tohto zákona, nakoľko jeho primárnym cieľom je vytvorenie funkčného legislatívneho rámca nevyhnutného pre efektívnu realizáciu kľúčových opatrení pre bezpečnosť národného kybernetického priestoru, ktorý transponuje priority a požiadavky, ktoré boli vytvorené na európskej úrovni a prijaté všeobecným konsenzom prostredníctvom smernice NIS[13].

Medzi hlavné oblasti úpravy návrhu zákona v nadväznosti na smernicu NIS patria oblasti:

- organizácie a pôsobnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- národnej stratégie kybernetickej bezpečnosti,
- jednotného informačného systému kybernetickej bezpečnosti,
- postavenia a povinnosti,
- organizáciu a pôsobnosť jednotiek CSIRT a ich akreditáciu,
- systému zabezpečenia kybernetickej bezpečnosti a minimálnych požiadaviek na zabezpečenie kybernetickej bezpečnosti,
- kontroly a auditu.

Predmetný zákon o kybernetickej bezpečnosti v úvodných ustanovenia rozpracúva smernicu NIS na podmienky SR, no je zrejmé, že rieši najmä technické a organizačné aspekty

[11] Hofreiter, L. Kultúra bezpečnosti a riadenie bezpečnosti, In Zborník z 20. Vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí, Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2015, str.65.

[12] Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

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

bezpečnosti kybernetického priestoru. Vo vzťahu k bezpečnosti koncových užívateľov počítačov zákon priamo nestanovuje žiadne povinnosti, pravidlá alebo zásady.

Primárnym cieľom zákona o kybernetickej bezpečnosti nie je bezpečnosť koncového používateľa, ale vytvorenie systému, ktorý bezpečnosť koncového užívateľa umožní.

Zákon o kybernetickej bezpečnosti rieši vzdelávanie nepriamo, prostredníctvom §7, ktorým sa definuje Národná stratégia kybernetickej bezpečnosti a jej obsah. V §7 ods. 2, písm. f.) sa definuje obsah stratégie, a to: "určenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy"[14]. Tým sa vytvárajú všeobecné rámce pre vytvorenie potrebných vzdelávacích programov a uceleného systému vzdelávania pre oblasť kybernetickej bezpečnosti.

Činnosť policajných zložiek a kybernetická kriminalita

Prevencia, odhaľovanie a objasňovanie počítačovej kriminality vyžaduje osobitný prístup a nepretržité zavádzanie nových metód, neustále zvyšovanie odbornej kvalifikácie kriminalistov a v neposlednom rade užšiu spoluprácu s externými odborníkmi (súkromným sektorom). Dynamika kybernetického prostredia, technický a technologický pokrok naráža na zaužívané postupy a dlhodobo budované spôsobilosti. Je zrejmé, že je potrebné zmeniť spôsob prístupu policajných zložiek k oblasti počítačovej kriminality, nakoľko je čoraz ťažšie takmer až nemožné zvoliť jednoznačný a univerzálny postup pri riešení kriminalisticky relevantných udalostí v počítačovej kriminalite. Každá udalosť vyžaduje citlivý prístup a individuálne posúdenie všetkých aspektov potencionálneho trestného činu. Až po zvážení všetkých okolností je možné stanoviť postup pre konkrétny prípad. Dôležitým aspektom bude budovanie dôvery medzi občanom-používateľom počítačového systému a policajtom.

Určité obmedzenia pri budovaní potrebnej dôvery však predstavuje platná legislatíva, ktorá významným spôsobom prispieva k (ne)efektívnosti činností policajných zložiek, napr. zdĺhavému a komlikovanému procesu dokumentovania tejto trestnej činnosti. Ide najmä o činnosti odvíjajúce sa od oznámenie počítačovej kriminality - napr. zhodnotenie situácie (ide o bezpečnostný incident alebo o trestný čin), príprava na procesné úkony a ich začatie, identifikácia a zaistenie potencionálnych dôkazov, zabezpečenie a zaistenie počítačového zariadenia.

Na jednej strane primerané bezpečnostné povedomie a na druhej efektivita metodík a postupov bezpečnostných zložiek - ak existuje obeť a je si toho vedomá, mali by existovať postupy, ako takúto trestnú činnosť efektívne ohlásiť, zdokumentovať a objasniť.
Samotné ohlásenie je len začiatkom procesu, ktorý by mal zohľadňovať situáciu obete, a teda samotné objasňovanie a dokumentovanie by nemalo byť obťažujúce alebo stresujúce. Obeť by mala byť ochotne a dobrovoľne zapojená do spolupráce, primerane spolupracovať a motivovať aj iných.

Množstvo nových aspektov zohráva zásadnú rolu v boji proti kybernetickej kriminalite. S ohľadom na špecifickosť prostredia a nástrojov je potrebné systém a spôsobilosti budovať tak, aby bol občan - obeť ochotný spolupracovať, nakoľko inak nebudú mať bezpečnostné zložky prehľad o bezpečnostnej situácií v tomto prostredí. Prehľad a aktuálne tendencie vývoja sú potrebné ako základ na budovanie efektívnych procesov a postupov smerujúcich k bezpečnosti v kybernetickom prostredí.

Záver

Bezpečnosť a ochrana pred počítačovou kriminalitou predstavuje s nárastom využívania moderných informačných a komunikačných systémov a dynamicky rastúcou informatizáciou pre spoločnosť a štát čoraz väčšiu výzvu. Pozitívne je možné vnímať, že sa

[14] Pozri Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020, schválená uznesením vlády SR č. 328 zo 17.6.2015.

o tejto téme diskutuje na rozličných fórach, čo má priamy dopad na porozumenie tejto oblasti, či už medzi odborníkmi z praxe, akademickou obcou alebo politikmi. V konečnom dôsledku to má priamy dopad aj na prijímanie konkrétnych, praktických krokov a opatrení.

Pre rozvoj oblasti prevencie kybernetickej kriminality je dôležité porozumieť jej špecifikám a aplikačným výzvam. **Za zásadné považujeme zmeniť zvyky ako sa na kybernetický priestor nazerá, pretože je to vo svojej podstate obyčajný svet, ktorý len má svoje špecifiká".** V tomto kontexte je potrebné zabezpečiť zmenu chápania úloh bezpečnostných orgánov, najmä polície v kontexte prispôsobenia zavedených nástrojov a postupov dynamike a špecifikám kybernetického prostredia. Práve identifikácia špecifík počítačovej kriminality by mohla byť dobrým začiatkom umožňujúcim prijatie a realizáciu správnych rozhodnutí v oblasti prevencie.

Dôležitým faktorom počítačovej kriminality jej latentnosť, čo predstavuje výrazný faktor ovplyvňujúci celkový stav tejto problematiky v spoločnosti, priamo súvisiaci s úrovňou bezpečnostného povedomia koncových užívateľov. Spôsob reakcie orgánov činných v trestnom konaní priamo ovplyvňuje správanie sa potencionálnych obetí a ich ochotu oznamovať počítačovú kriminalitu.

Používateľská dilema:

Je potrebné zaoberať sa postupným odstránením triviálnej dilemy používateľa, ktorá v prípade bezpečnostného incidentu spočíva vo voľbe medzi ohlásením podozrenia z trestného činu a neohlásením. Používateľ, hoc si je vedomý, že pravdepodobne ide o trestný čin, tento neohlási, nakoľko neočakáva pomoc zo strany policajného zboru. Skôr vníma negatívne komplikácie súvisiace s procesom vyšetrovania a dokumentovania trestného činu.

Používateľ má spravidla záujem na vyriešení problému a pomoci, zníženie prípadnej škody, odstránenie dôsledkov a pokračovaní v používaní počítačového systému.

S ohľadom na uvedené je možné predpokladať, že používateľ sa skôr obráti na súkromné spoločnosti so žiadosťou o pomoc, bez ohľadu na možnú trestno-právnu zodpovednosť súvisiacu s neohlásením možného trestného činu.

Ochrana a zvyšovanie bezpečnosti samotných informačných systémov a poskytovaných on-line služieb sú priamo závislé od koncových užívateľov. Ľudský faktor, ako bezpečnostné riziko, predstavuje čoraz dôležitejší aspekt bezpečnosti počítačového prostredia. Je zrejmé, uvedomelý užívateľ počítačových systémov je základným prvkom predchádzania páchania počítačovej kriminality, ktorý svojim konaním alebo nekonaním zásadným spôsobom ovplyvňuje celkový stav a možnosti páchania počítačovej kriminality, vrátane rozsahu vzniknutých škôd. Vzdelávanie možno považovať za základný a najefektívnejší spôsob predchádzania páchania počítačovej trestnej činnosti.

Je pravdepodobné, že práve preventívne aktivity budú zohrávať podstatnú rolu v boji proti rôznym formám kybernetickej kriminality. K takémuto konštatovaniu nás vedú nasledujúce tézy:

- samotný vzťah medzi technologickým a technickým pokrokom a novými formami kybernetickej kriminality podmieňuje možnosti prevencie, zásadným obmedzením bude schopnosť analyzovania vývojových trendov techniky a technológií a následného predvídania nových foriem kybernetickej kriminality,
- rýchlosť transformácie poznania v oblasti páchania kybernetickej kriminality do efektívneho odhaľovania a objasňovania - činnosti orgánov činných v trestnom konaní,
- vytváranie vhodných legislatívnych podmienok v súlade s trendmi a vývojom kybernetickej kriminality,

- schopnosť a rýchlosť reakcie bezpečnostného systému na jednotlivé formy kybernetickej kriminality je v príkrom rozpore s dynamikou kybernetického prostredia[15],
- latentnosť kybernetickej kriminality podmienené neznalosťou základných pravidiel bezpečnosti kybernetického prostredia koncovými užívateľmi,
- nedostatok spolupráce a dôvery medzi bezpečnostnými zložkami (orgánmi aplikujúcimi právo) a koncovými užívateľmi,
- nutnosť identifikovať nové formy kybernetickej kriminality je obtiažné, ak nie nemožné, bez spolupráce s koncovými užívateľmi počítačov.

Zväčšujúca sa priepasť medzi zavedenými spôsobmi práce bezpečnostných zložiek a ich budovanie a novým, dynamicky sa meniacim bezpečnostným prostredím poukazuje na nutnosť zaoberania sa problematikou kybernetickej kriminality komplexne, na primeranej vedeckej a odbornej úrovni. Rola, úlohy a miesto policajného zboru v oblasti kybernetickej bezpečnosti a kriminality sa bude musieť prispôsobiť novej situácii.

Bez zásadných zmien v činnosti policajných zložiek nebude možné efektívne predchádzať, odhaľovať a objasňovať nové moderné formy kriminality, medzi ktoré nesporne možno zaradiť kybernetickú kriminalitu.

Zoznam použitej literatúry:

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

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

BRVNIŠŤAN, M. Bezpečnostné povedomie v kontexte boja proti novodobým bezpečnostným hrozbám. In*: Zborník príspevkov z IX. medzinárodnej vedeckej konferencie v Banskej Bystrici 11. – 12. februára 2016.* Banská Bystrica: Fakulta politických vied a medzinárodných vzťahov UMB, 2016, ISBN 978-80-557-1093-8, str. 520-530.

BRVNIŠŤAN, M. Kybernetická bezpečnosť a jej možné implikácie na systém vzdelávania SR. In*: Zborník z medzinárodnej vedeckej konferencie, ktorá je súčasťou plnenia integrovanej vedeckovýskumnej úlohy A PZ v Bratislave - Krízové scenáre v systéme prípravy krízových manažérov na vysokých školách bezpečnostného zamerania.* Bratislava: A PZ, 2015, ISBN 978-80-8054-662-5, str. 76-83.

HOFREITER, L. Kultúra bezpečnosti a riadenie bezpečnosti. In: *Zborník z 20. vedeckej konferencie s medzinárodnou účasťou Riešenie krízových situácií v špecifickom prostredí.* Žilina: Fakulta špeciálneho inžinierstva Žilinskej univerzity v Žiline, 2015, ISBN 978-80-554-1024-1, str. 36-43.

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

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

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

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

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

Posilnená politika kybernetickej obrany NATO. Enhanced NATO Policy on Cyber Defence. 2014.

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

[15] Ako príklad dlhotrvajúcej reakcie bezpečnostného systému môže poslúžiť prijímanie zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti - proces trval viac ako 7 rokov - pozn. autora.

STRÉMY, T. Počítačová kriminalita. In: DIANIŠKA, G. a kol. *Kriminológia.* Plzeň: Aleš Čeněk s.r.o., 2011, s. 245.
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
Zákon Národnej rady SR č. 300/2005 Z. z. o Trestnom zákone (Trestný zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c
www.efocus.sk/images/archiv/file_1183_0.pdf
http://recent-ecl.blogspot.fr/2012/07/cybercrime-new-eu-statistics.html:
https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

Kontaktné údaje:
JUDr. Miroslav Brvnišťan, PhD.
Akadémia Policajného zboru v Bratislave
brvnistan@bmsec.sk

Využitie metód pri definovaní bezpečnostných hrozieb v oblasti informačných systémov

Jaroslava Demčáková

Abstrakt:
Metódy identifikácie a posúdenie miery rizika vedú k procesu prevencie a prognózy zníženia rizika na prijateľnú úroveň. Využívame hodnotenie rizík ako prvý krok v metodike riadenia rizika na prognózovanie či definovanie potencionálnych hrozieb, zraniteľnosti a rizika spojeného s informačnými systémami. Metódy vedú k stanoveniu priorít, hodnotení a implementáciu vhodných kontrol znižujúcich riziko. Konečným cieľom využitia týchto metód je pomôcť lepšie riadiť riziká súvisiace s informačnými technológiami.
Kľúčové slová:
metódy, bezpečnostné hrozby, informačné systémy

Abstract:
Process of prevention and risk reduction forecast have been led to an acceptable level by the methods of risk identification and assessment. In order to forecast or to define potential threats, vulnerabilities, risk associated with the information system, we use risk assessment as the first step in the particular management methodology. The methods lead to prioritisation, evaluation and implementation of appropriate risk-control measures. The final objective is to use these methods in order to reach better risk management associated with information technologies.
Key words:
methods, security threats, information systems

Úvod

Každá spoločnosť, či už súkromná alebo štátna má úlohu v oblasti IT. V tejto digitalizovanej sfére, kde spoločnosti používajú automatizované informácie a využívajú systémy informačných technológií musia byť obzvlášť dôsledné z hľadiska bezpečnostnej politiky. Organizácie spracovávajú informácie na efektívnu podporu svojich procesov, kde riziko manažmentu IT bezpečnosti zohráva dôležitú úlohu pri ochrane informačnej bezpečnosti, preto jeho poslanie súvisí s rizikom informačných technológií. Hlavnou úlohou procesu riadenia rizík by mala byť ochrana spoločnosti. Riziko je považované za negatívny dopad so zraniteľnosťou a negatívnym dopadom. Riadenie rizík je proces identifikácie rizika, posúdenia rizika a navrhnutia efektívnych opatrení na zníženie rizika na akceptovateľnú hranicu.

Analýza súčasného stavu EÚ a SR

Nový systém bezpečnosti, ktorý je založený na medzinárodných vzťahoch, sa formuje už od skončenia studenej vojny a je ovplyvnený dominantným postavením USA ako jedinej svetovej superveľmoci a rastúcim vplyvom niektorých medzinárodných organizácií, ktorými sú NATO, Európska únia, Medzinárodný menový fond a Svetová banka.

Analýza hrozieb pre bezpečnosť je predpokladom efektívnej stratégie manažmentu rizík bezpečnostných hrozieb, pretože vznik mimoriadnej udalosti môže postihnúť obyvateľstvo určitej krajiny na celom území. Slovenská republika sa snaží cieľ bezpečnosti krajiny uplatňovať na báze ustanovení ústavného zákona č.227/2002 Z.z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov, ďalej prostredníctvom zákona č.319/2002 Z.z. o obrana Slovenskej republiky v znení neskorších predpisov.

V súčasnosti patrí medzi najväčšie bezpečnostné hrozby existencia umelej inteligencie a dronov najmä v rámci členských štátov Severoatlantickej aliancie. Taktiež môžeme medzi ne zaradiť hybridné hrozby, kybernetické útoky či terorizmus. Nová podoba stratégie bezpečnosti prináša definovanie bezpečnostných záujmov Slovenskej republiky, charakteristiku

bezpečnostného prostredia v ktorom sa nachádzame a odpočet rizík na ktoré je Slovenská republika pripravená reagovať.

Povinnosti v oblasti zabezpečenia bezpečnosti krajiny vyplývajú zo strategických dokumentov ktorými sú Lisabonská zmluva, Stratégia EÚ v oblasti ochrany zdravia, Stratégia vnútornej bezpečnosti EÚ k budovaniu a odolnosti voči prírodným a iným katastrofám a taktiež Európsky bezpečnostný program na roku 2015-2020 Usmernenie Európskej komisie pre vyhodnocovanie a mapovanie rizík v kontexte manažmentu katastrof.

V rámci Európskej únie je prognózovania a modelovanie bezpečnostných hrozieb definované v rámci dokumentu EUDefence: Smerom k európskej obrannej únii Smerom k jednotnejšej, silnejšej a demokratickejšej únii. V oblasti obrany nejde iba o to, aby Európska únia vytvorila alternatívu k NATO ale členské štáty Európskej únie musia predovšetkým postupovať spoločne vo vzájomnej súčinnosti. Na základe Európskej komisie bol odsúhlasený plán k prehĺbeniu spolupráce Európskej únie v oblasti bezpečnosti a obrany, v rámci ktorého mali byť stanovené nasledujúce priority:

1. chrániť Európsku úniu a jej občanov
2. reagovať na vonkajšie konflikty a krízy
3. posilniť kapacitu partnerov

Európska únia zriadila spoločný Európsky obranný fond, z ktorého bude financovať spoločný výskum a vývoj najmä v záujme prehĺbenia vzájomnej spolupráce v oblasti obrany a bezpečnosti členských štátov, aby tak nadviazala stálu štruktúrovanú spoluprácu. Európska únia zintenzívnila spoluprácu s NATO na veľmi vysokú úroveň.

V SR bol zriadený tím Ministerstvom financií SR s cieľom zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry – NIKI. Tím zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňujúcich ich následkov a následnou obnovou činností informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi integrovaných služieb a inými štátnymi orgánmi.

Riziko v IT

Existujú rôzne formy na chápanie rizika a jeho vyjadrenie v odborných literatúrach. Definovanie rizika je rozdielne aj z hľadiska odborov, inak ho definuje bankový sektor, inak poisťovníctvo a inak sa chápe v informačných systémoch.

„V technických (technologických) procesoch je riziko kvalitatívne a kvantitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia. Je to pravdepodobnosť vzniku negatívneho javu a jeho dôsledku “ [1].

„Z poistného hľadiska predstavuje riziko pravdepodobnosť vzniku nebezpečenstva, o ktorom sa nevie či a kedy vznikne. Je to teda neistota, možnosť vzniku neželanej a nechcenej straty. Finančné riziko je definované ako potencionálna, neočakávaná finančná strata (unexpected loss) subjektu, strata v budúcnosti.“ [2].

[1] ŠIMÁK, L. *Krízový manažment vo verejnej správe.* Žilina: ŽU, 2001, s. 39
[2] HOFREITER, L. *Bezpečnosť, bezpečnostné riziká a ohrozenia*. Žilina: ŽU, 2004, s. 54

Riziko v informačných systémoch charakterizujeme ako kombináciu bezpečnostných jednotiek. Bezpečnostné jednotky sú aktíva, hrozba a zraniteľnosť. Vzťahy medzi nimi môžeme vyjadriť rovnicou. Každá zmena aktív alebo hrozby výrazne ovplyvní riziko a to buď zníženiu rizika alebo zvýšeniu rizika. Riziko (R) v informačnom prostredí môžeme definovať ako funkciu aktív (Assets). Každé aktíva má svoju hodnotu (A), definovanú hrozbu (Threats) (T) a zraniteľnosť dopadu (vulnerability) (V). Zraniteľnosť je funkciou vykonaných preventívnych oaptrení (safeguards) (SG). Matematicky definujeme rovnicu v tvare:

$$\mathbf{R= f (A,T,V,), V=f (SG)}$$

Hlavnou úlohou krízového manažéra v oblasti IT je znížiť úroveň rizika na hodnotu akceptovateľného rizika. Každá spoločnosť si na základe analýzy definuje svoje akceptovateľné riziko, ktoré je potrebné neustále znižovať. Po prijatí výsledkov z analýzy sa definujú ochranné opatrenia a určí sa hodnota zbytkového rizika,

Analýza rizík v IT

Analýza rizika je spravidla v spoločnosti vykonávaná identifikáciou hrozieb manažmentom rizík, ktorý definuje nežiadúce dopady na chod spoločnosti. Nežiadúce stavy môžu mať vplyv na celý chod firmy či spoločnosti a nežiadúcim dopadom je daná škála hodnotenia výsledkov z analýzy možných škôd. Pravdepodobnosť vzniku závisí na vstupných parametroch a to je útočník, výskyt pravdepodobnosti a miesto zraniteľnosti. Závery z analýzy rizík vedú k identifikácii a výbere ochranných opatrení, ktoré znížia možnosť vzniku útoku v oblasti IT. Analýza v IT sektore vedie k vytvoreniu bezpečnej ochrany informačných systémov.

Metódy analýzy v IT

Na vykonanie analýzy rizík existuje množstvo metód. V dnešnej novodobej spoločnosti a rozvojom IT systémov je k dispozícii množstvo softwerových produktov, ich výsledkov je hodnotenie rizík. Softwarové produkty sú založené na fyzikálnych modeloch jednoduchších či zložitejších, čo predurčuje v kvalitnú alebo nekvalitnú spoľahlivosť produktu. Konečné rozhodnutie k výberu metódy analýzy má krízový manažment IT. Jednými z možností sú tieto metódy:

CHECK LIST - Kontrolný zoznam

Táto metóda check listu je založená na systematickej kontrole plnenia stanovených opatrení v spoločnosti. Zoznam kontrolných otázok je generovaný na základe zoznamu charakteristík sledovaných systémov alebo činnosti, ktoré súvisia so systémom a potencionálnymi dopadmi zo zlyhania systému alebo časti prvku. Štruktúra check listu je formulár od jednoduchého zoznamu po zložitý, ktorý zahrňuje dôležité parametre v rámci súboru pre stanovenie váhy.

SAFETY AUDIT - Bezpečnostná kontrola

Audit, ktorý prehľadá rizikové situácie v spoločnosti či organizácii a navrhne opatrenia na zvýšenie bezpečnosti. Metóda predstavuje postup hľadania potencionálne možnej nehody alebo problému, ktorý sa môže objaviť v informačnom systéme. Metóda predstavuje postup hľadania potencionálnej možnej hrozby, ktorá ovplyvní proces v podniku. Formálne je používaná pripravením zoznamom otázok a matice ohodnotenia rizík.

WHAT- IT ANALYSIS - Analýza toho, čo sa stane ak

Analýza toho, čo sa stane ak je postup na hľadanie nebezpečných dopadov vybraných prevádzkových situácií. V podstate, ide je spontánne diskusie a hľadaní opatrení, nápadov

v odbornej skupinke ľudí oboznámených sa s procesom, ktorá si kladie otázky a vyslovuje úvahy o možných nehodách. Nie je vnútorne štruktúrovaná technikou ako iné metódy.

PREMINARY HAZARD ANALYSIS – PHA Predbežná analýza ohrozenia
Predbežná analýza ohrozenia – tiež kvantifikuje zdroj rizika a jeho postup na vyhľadávanie nebezpečných stavov či núdzových situácií, ich príčiny a dopady. Rozdeľuje dopady do kategórií podľa predom stanovených kritérií. Koncept PHA vo svojej podstate predstavuje súbor techník, vhodných pre posúdenie rizika.

HAZARD OPERATION PROCESS – HAZOP Analýza ohrozenia a prevádzkovania
Kvalitatívne posudzovanie rizika je systematický prístup pre predikciu odhadu početnosti a dopadov nehôd pre zariadenie alebo prevádzku systému. Analýza kvantitatívnych rizík procesu je koncept, ktorý rozširuje kvalitatívne metódy hodnotenia rizík o numerické hodnoty. Algoritmus využíva kombináciu s inými konceptmi a smeruje k zavedeniu kritérií pre rozhodovací proces, potrebnú stratégiu a programami k efektívnemu zvládnutiu rizika s využitím simulácií.

PROCES QUANTITATIVE RISK ANALYSIS – QRA Analýza kvalitatívnych rizík procesu
Kvantitatívne posudzovania rizika je systematický a komplexný prístup pre predikciu odhadu početnosti a dopadu nehôd. Analýza kvantitatívnych rizík procesu je koncept, ktorý rozširuje kvalitatívne metódy hodnotenia rizík o numerické hodnoty. Algoritmus využíva kombináciu s konceptmi a smeruje k zavedeniu kritérií pre rozhodovací proces, potrebnú stratégiu a programami k efektívnemu zvládnutiu rizika. Vyžaduje náročnú databázu a počítačovú podporu.

EVENT TREE ANALYSIS – ETA Analýza stromu udalostí
Analýza stromu udalostí je postup, ktorý sleduje priebeh procesu od iniciačnej udalosti cez konštruovanie udalosti vždy na základe dvoch možností. Tieto možnosti sú priaznivé alebo nepriaznivé. Metóda ETA je graficko-statická metóda. Názorné zobrazenie systémového stromu udalostí predstavuje rozvetvený graf s dohodnutou symbolikou a popisom. Znázorňuje všetky udalosti, ktoré sa v posudzovanom systéme môžu vyskytnúť. Výsledný graf sa rozvetvuje ako konáre stromu.

FAULTS TREE ANALYSIS – FTA Analýza stromu porúch
Analýza strumu porúch je založená na systematickom spätnom rozbore udalostí za využitím reťazca príčin a následkov, ktoré môžu viesť k vybranej vrchovej udalosti. Metóda FTA je graficko-analytická. Názorné zobrazenie stromu porúch predstavuje rozvetvený graf s vopred dohodnutou symbolikou a popisom. Hlavným cieľom analýzy je posúdenie pravdepodobnosti vrcholovej udalosti s využitím analytických metód.

HUMAN RELIABILITY ANALYSIS – HRA Analýza ľudskej spoľahlivosti
Analýza ľudskej spoľahlivosti je postup na posúdenie vplyvu ľudskej činnosti na výskyt živelných katastrof, nehôd, havárií. Koncept analýzy HRA smeruje k systematickému posúdeniu ľudského faktoru a ľudskej chyby. Zahrňuje prístupy mikroergonomické a makroergonimické. Analýza HRA má väzbu na aktuálne platné pracovné predpisy z hľadiska bezpečnosti pri práci.

CAUSES AND CONSEQUENSES ANALYSIS – CCA Analýza príčin a dopadov

Analýza príčin a dopadov je zmes analýzy stromov a porúch a analýzy stromu udalostí. Najväčšou prednosťou je použitie komunikačného prostriedku. Ako už vyplýva z názvu, účelom tejto analýzy je odhaliť základné príčiny a dopady možných nehôd.

Záver

V dnešnej dobe už nikto nespochybňuje potrebu adekvátneho zabezpečenia informačného systému v spoločnosti, organizácii, ktoré sú v ňom spracované na základe vybraných analýz. Takýto prístup k bezpečnosti sa premieta k účinnému vytvoreniu preventívnych opatrení pre zaistenie spoľahlivej a bezpečnej prevádzky informačnej politiky. Medzi príčiny nedostatočnej analýzy rizík chápeme nedostatočné chápanie zložitosti systému a problémov týkajúce sa IT politiky v spoločnosti. Súvislosti medzi odbornou stránkou a hĺbkou poznania nášho IT systému prinášajú výsledky z vybraných metód analýz informačných systémov v organizácii. Z analýzy rizík je možné vykonať analýzu rizík informačného systému a následne realizáciu bezpečnosti v praxi spôsobom, ktorý vyberá oblasť IT manažmentu. Výsledky z analýz sú využité pre navrhnutie preventívnych opatrení proti útokom, hrozbám IT systému pre danú organizáciu. Väčšina informačných systémov v spoločnosti je veľmi slabo zabezpečená, pretože firmy, organizácie vynakladajú malé finančné prostriedky na zabezpečenie svojej IT bezpečnostnej politiky.

Zoznam použitej literatúry:

HOCR, K. *Logika, metodológia a metódy vedeckého poznania.* Bratislava: Akadémia PZ, 1996, s. 55. ISBN 80-88751-91-8.
HOFREITER, L. *Bezpečnosť, bezpečnostné riziká a ohrozenia*, ŽU, Žilina, 2004, 146 s. ISBN 80-8070-181-4.
HORÁK, R. a kol. *Průvodce krizovým řízením pro veřejnou správu*. 2. vyd. Praha: Linde, a.s., 2011. ISBN 978-80-7201-827-7.
MATOUŠEK, O. *Sociální služby: legislativa, ekonomika, plánování, hodnocení*. Vyd 1. Praha: Portál, 183 s. ISBN 9788073673109.
PROCHÁZKOVÁ, D. *Řízení bezpečnosti, krizové řízení a plánování, ochrana kritické infrastruktury*. Praha : Regionservis, 2005. s. 11
REKTOŘÍK, J. *Krizový management ve veřejné správě: teorie a praxe.* 1. vyd. Praha: Ekopress, 2004. s. 81
ŠIMÁK, L. *Krízový manažment vo verejnej správe*. Žilina: ŽU, 2001, s. 39

Internetové zdroje:

Baldwin, M. E., and S. Lakshmivarahan, 2003: Development of an events-oriented verification system using data mining and im-age processing algorithms. Preprints, Third Conf. on Artifi-cial Intelligence Applications to Environmental Science, LongBeach, CA, Amer. Meteor. Soc., CD-ROM, 4.6. Black, T. L., 1994: The new NMC mesoscale Eta model: Description and forecast examples. Wea. Forecasting,9,265.
NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. August 2001.

Kontaktné údaje:

Ing. Jaroslava Demčáková
externý doktorand Akadémia PZ v Bratislave
jaroslava.demcakova@gmail.com

Implementácia IDS systému netxms.org v organizácii

Michal Greguš, Peter Veselý

Abstrakt:
Praktická implementácia systému typu IDS (intrusion detection system) alternatívneho open source riešenia netxms.org k pasívnej detekcii narušenia kybernetickej bezpečnosti so zameraním na inštaláciu servera netxms a jednotlivých klientov s nastavením generovania pravidelných výstupov a upozornení.
Kľúčové slová:
Osobné údaje, kybernetická bezpečnosť, GDPR, IDS

Abstract:
Analysis of cyber security breach models for the purpose of misuse of personal data, analysis of selected security incidents and proposal of appropriate measures to reduce the risk of these types of incidents, especially with the use of open source resources. Analysis of potential impacts on the organization in relation to the GDPR Regulation and the ePrivacy Directive.
Key words:
Personal data, cyber security, GDPR, ePrivacy

Úvod

V niekoľkých posledných desaťročiach sa požiadavky na informačnú bezpečnosť značne výrazne zmenili. Pri celosvetovom budovaní siete internet a rýchlom rozvoji informačných technológií sa zmenil celkový pohľad na bezpečnosť, ktorá bola predtým založená najmä na fyzickej a administratívnej ochrane dokumentov. Pribúdajúci počet počítačov pre spracovanie a ukladanie dát a taktiež pribúdajúci počet inteligentných zariadení typu smartphone, ktoré sa pripájajú prostredníctvom siete internet k ukladaným dátam, spôsobil potrebu chrániť tieto systémy proti strate dát a najmä proti neoprávnenému použitiu. V tomto kontexte vývoja sa vyvíjal aj termín počítačová bezpečnosť. Počas tohto vývoja s rastúcim počtom sietí a rastúcou dostupnosťou množstva online systémov vznikali nové druhy hrozieb a taktiež sa vyvíjala i terminológia, napríklad sieťová alebo internetová bezpečnosť, ktorá dnes už tvorí samostatný odbor[1] v rámci informačných technológií.

Útoky na počítačové siete je možné chápať z dvoch pohľadov – pohľadu zraniteľnosti a pohľadu napadnutia. Z pohľadu zraniteľnosti ide o chybu, vzniknutú u rôznych dôvodov v programe alebo jeho nastavení, ktorá umožňuje porušenie nastavených bezpečnostných pravidiel a umožňuje tiež neoprávnenú manipuláciu. Z pohľadu napadnutia ide o úmyselný čin, ktorý využíva zraniteľnosť za účelom obídenia bezpečnostného mechanizmu. Napadnutia, teda útoky, je možné klasifikovať do dvoch základných kategórií, a to pasívny útok a aktívny útok. Pasívne napadnutie informačného systému spočíva v získavaní dát zo siete, ktoré sa realizuje odposluchom alebo monitorovaním dátového toku. Detekcia pasívnych napadnutí je pomerne zložitá, pretože neovplyvňuje samotný dátový tok a príjemca a ani odosielateľ nevedia, že sú monitorovaní. Veľmi účinnou obranou voči pasívnemu napadnutiu je šifrovanie medzi účastníkmi komunikácie. Dôraz v obrane pred pasívnym napadnutím je teda skôr na prevencii (šifrovanie) ako na detekcii monitorovania. Naopak, aktívne napadnutie je definované ako pozmeňovanie dát alebo vytvorenie nových dát. Jedným z typov aktívneho napadnutia je tzv. predstieranie identity (masquerade), kde sa útočník snaží vydávať za inú identitu s cieľom zneužitia oprávnenia tejto identity. Ďalším typom aktívneho napadnutia je opakované prehranie (replay), kde útočník opakovane odošle dopredu odposlúchnuté dáta s cieľom vyvolať určitú akciu. Modifikácia správy (modification od message) upravuje alebo blokuje dáta taktiež za účelom neoprávnenej akcie. Odmietnutie služby (DoS – denial of service) alebo jeho

[1] STALLINGS, W. *Network security essentials: applications and standards*. Boston: Prentice Hall, 2011

ditribuovaná forma (DDoS[2]) ma za cieľ obmedzenie alebo úplnú stratu funkčnosti jednej alebo viacerých služieb siete alebo zariadenia. Aktívna prevencia v prípade aktívneho napadnutia je veľmi zložitá. Obranou voči aktívnemu napadnutiu je detekcia alebo blokácia napadnutia a následné zotavenie sa z útoku.

Nariadenie GDPR a kybernetická bezpečnosť

Nariadenie GDPR v pôvodnom znení (priama aplikovateľnosť nariadenia GDPR) zavádza používanie nových pojmov „privacy by design" a „privacy by default" v článku 25:

Článok 25

Špecificky navrhnutá a štandardná ochrana údajov

1. So zreteľom na najnovšie poznatky. náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.

2. Prevádzkovateľ vykoná primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne sa spracúvajú len osobné údaje, ktoré sú nevyhnutné pre každý konkrétny účel spracúvania. Uvedená povinnosť sa vzťahuje na množstvo získaných osobných údajov, rozsah ich spracúvania, dobu ich uchovávania a ich dostupnosť. Konkrétne sa takýmito opatreniami zabezpečí, aby osobné údaje neboli bez zásahu fyzickej osoby štandardne prístupné neobmedzenému počtu fyzických osôb.

3. Schválený certifikačný mechanizmus podľa článku 42 sa môže použiť ako prvok na preukázanie súladu s požiadavkami uvedenými v odsekoch 1 a 2 tohto článku.

Definícia podľa vyššie citovaného článku 25 nariadenia GDPR je však natoľko všeobecná a filozofická, že nie je fakticky možné, bez poskytnutia širšieho kontextu výkladu tohto práva, pokračovať v ďalšej diskusii o danom výklade pre prax. Technické ako aj organizačné opatrenia upravené týmto článkom 25 nariadenia GDPR však je možné vyjadriť siedmimi princípmi ochrany súkromia, ktoré sú vytvárané so zreteľom na predmetnú legislatívu už niekoľko desiatok rokov:[3]

- Pro- aktívny nie reštriktívny prístup; Preventívne nie nápravné opatrenia
- Ochrana súkromia ako predvolené nastavenie
- Ochrana súkromia ako súčasť dizajnovania procesov
- Plná funkcionalita
- End-to-end bezpečnosť informačných systémov
- Transparentnosť
- Rešpektovanie súkromia užívateľov - orientovať sa na dátový subjekt.

Pojmy Privacy by design a by default je nutné ponímať ako komplexnú zmenu kultúry v každej organizácii, ktorá sa odzrkadľuje nie iba v implementovaní požiadaviek nariadenia GDPR, ale aj v reálnom uplatňovaní týchto pravidiel v praxi. Aspekty Privacy by design and by default musia byť viditeľné vo všetkých procesoch a na všetkých úrovniach riadenia.

[2] KAN, B. M., MARCH 6, 2018 2:21PM EST, MARCH 6, 2018. Powerful DDoS Attack Sets New Record at 1.7 Tbps. In: *PCMAG* [online] [cit. 17.03.2018]. Dostupné na internete: https://www.pcmag.com/news/359693/powerful-ddos-attack-sets-new-record-at-1-7-tbps

[3] TREND.SK. Privacy by design by default kde končí filozofia a začína prax? In: *blog.etrend.sk* [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

Určitým predpokladom pre správne implementovanie Privacy by design by default je funkčná "Data governance"[4]. Bezpečnostné projekty spracované v súlade s normou ISO 27001 sa v praxi ukázali z pohľadu ochrany osobných údajov ako bezvýznamné, samotná prax ukázala, že tieto dokumenty sú striktne formálne a neodzrkadľujú reálne aspekty spracúvania osobných údajov a slúžili iba pre potreby výkonu dohľadu zo strany ÚOOÚ (Úrad na ochranu osobných údajov).[5] Vo svojej podstate to znamená, že *každá organizácia a každý programátor pri vypracovaní, navrhovaní, výbere a používaní aplikácií, služieb a produktov, ktoré sú založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje, musia zohľadniť tie najnovšie poznatky modernej technologickej doby tak, že budú zodpovedať presne podmienkam organizácie (by design) a že sa o ochrane osobných údajov bude uvažovať od počiatku uvažovania o službe alebo produkte (by default).*[6]

Je však nutné upozorniť na jeden veľmi dôležitý problém bezpečnosti - samotná bezpečnosť IS/IT. Pre ilustratívny príklad je možné uviesť vznik problému s elektronickým podpisom eID[7], kde bola nájdená zraniteľnosť v samotnej podstate šifrovacieho algoritmu a štát musel zmeniť všetky elektronické podpisy vo vydaných občianskych preukazoch. To isté však platí pre všetky organizácie - pri známom bezpečnostnom probléme musia zmeniť používanú technológiu a bezpečnostné postupy. V súčasnosti rezonuje aj problém s procesormi počítačov pod názvami Meltdown a Spectre[8], ktoré predstavujú veľmi vážne ohrozenie bezpečnosti osobných údajov, v prípade operačných systémov spoločnosti Microsoft [9] je zatiaľ záplata, ktorá však nerieši podstatu zraniteľnosti, ale iba jej výrazné spomalenie využitia, iba na Windows 10 (RTM, 1511,1607,1703, 1709), Windows 8.1 a Windows 7 SP1. Všetky ostatné verzie desktopových verzií sú bez ochrany pred danou hrozbou. Opravené sú aj verzie OS Windows Server, version 1709 (Server Core Installation), Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, ostatné verzie sú bez bezpečnostnej záplaty.[10]

Systém IDS a IPS

Systém IDS (intrusion detection system) a systém IPS (intrusion prevention system) sú systémy na detekciu sieťových útokov, ktoré sa navzájom líšia predovšetkým svojou konfiguráciou, pričom systém IPS detekované útoky taktiež proaktívne blokuje. Pre oba systémy sú charakteristickým prvkom sady kritérií na detekciu štandardnej a nežiadúcej sieťovej prevádzky. Podľa miesta nasadenia v sieti môžeme systémy rozdeľovať na network-based a host based,[11] pričom network-based je umiestnenie samostatne na sieti na sieťových

[4] TREND.SK, Privacy by design by default kde končí filozofia a začína prax? [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

[5] TREND.SK, Privacy by design by default kde končí filozofia a začína prax? [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

[6] TREND.SK, Privacy by design by default kde končí filozofia a začína prax? [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

[7] ŽIVÉ.SK. Šéf výskumníkov, ktorí našli chybu aj v našich e-občianskych: Štát to nezvládol. Potrebuje rázny tím. In: *Živé.sk* [online] [cit. 13.12.2017]. Dostupné na internete: https://www.zive.sk/clanok/129275/sef-vyskumnikov-ktori-nasli-chybu-aj-v-nasich-e-obcianskych-stat-to-nezvladol-potrebuje-razny-tim/

[8] Meltdown and Spectre. In: [cit. 21.01.2018]. Dostupné na internete: https://meltdownattack.com/

[9] Protect against speculative execution side-channel vulnerabilities in Windows client. In: [cit. 21.01.2018]. Dostupné na internete: https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

[10] Windows Server guidance to protect against the speculative execution side-channel vulnerabilities. In: [cit. 21.01.2018]. Dostupné na internete: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

[11] AKANE. IPS/IDS ochrana. In: *Jak na webové stránky* [online] [cit. 04.12.2017]. Dostupné na internete: http://timehosting.cz/ipsids-ochrana/

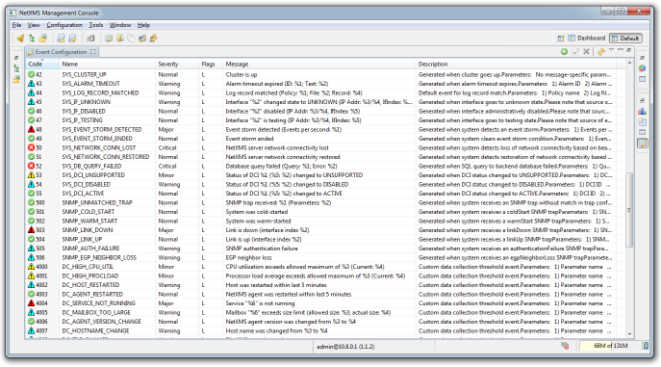
uzloch. Tento druh umiestnenia môže pokrývať väčšie množstvo cieľových systémov. Umiestnenie na cieľovom počítači, teda host-based, výrazne zlepšuje výkonnosť celého IDS/IPS riešenia. Výkon je tak distribuovaný do viacerých prvkov. Takéto nasadenie umožňuje aj meniť rozsah chránených služieb podľa konfigurácie na rozdiel od network-based, ktoré môže chrániť viacero odlišných systémov.

Systémy IDS a IPS je ďalej možné rozdeliť na dve kategórie spôsobov detekcie útokov a to signature-based a anomaly-based. Detekcia útokov signature-based je založená na detekcii podľa stanovených odtlačkov dát, pričom týmito odtlačkami dát rozumieme konkrétne vzory, kódy, ktoré obsahujú pakety dát signalizujúce využitie zraniteľností. Toto riešenie je výhodné pre svoje presné cielenie a nízke percento falošných hlásení, naopak, týmto spôsobom nie je možné detekovať dosiaľ nedokumentované zraniteľnosti a vznikajúce anomálie v dátovej prevádzke. Nesprávne konfigurované pravidlá môžu mať za následok aj zníženie výkonu dátovej prevádzky a vysoké percento falošných hlásení, alebo naopak, efektivita detekcie môže byť rovná nule. Druhý spôsob detekcie útokov - anomaly-based sa snaží problém detekcie riešiť vyhľadávaním abnormalít dátovej prevádzky. Vo svojej prvej fáze sa systém nachádza v tzv. učiacej sa (learning) fáze, kedy sa monitoruje štandardná dátová prevádzka a na základe týchto získaných dát sa potom deteguje prípadná odchýlka. Výhodou tohto riešenia spočíva v tom, že na základe tejto analýzy je možné detegovať aj nelegitímnu dátovú prevádzku alebo zdroj. Nevýhodou je vyššie percento falošných pozitív vzhľadom na nutnosť rozdelenia na štandardnú a neštandardnú dátovú prevádzku.[12]

IDS systém netxms.org

IDS systém NETXMS je výkonný multiplatformový (podpora viac druhov operačných systémov) systém správy a monitorovania otvorených zdrojov dátovej prevádzky siete v organizácii. Systém poskytuje komplexnú správu udalostí a monitorovanie výkonu, kde výstupom sú upozornenia, hlásenia a grafy pre všetky vrstvy IKT infraštruktúry. Systém je založený na trojvrstvovej architektúre: všetky informácie sú zhromažďované monitorovacími agentmi (vlastnými vysoko výkonnými agentmi alebo agentmi SNMP) a tieto sú posielané na monitorovací server na spracovanie a ukladanie. Správca siete má potom prístup k zhromaždeným údajom pomocou bohatej klientskej aplikácie alebo webového rozhrania.

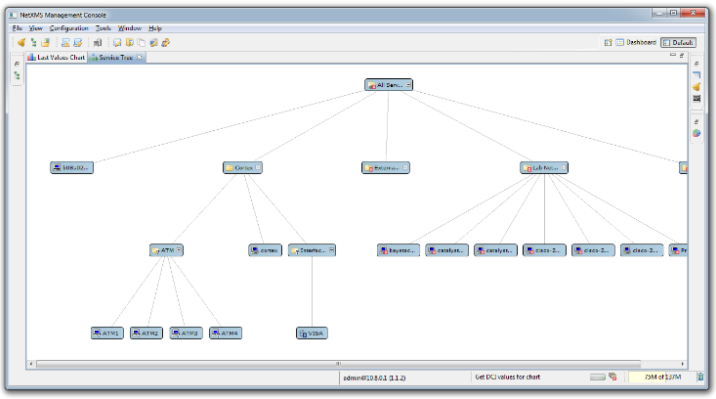
Samotná správa a nastavenie pravidiel je prevádzané v samostatnej aplikácii alebo cez webové rozhranie, podľa toho, ako sa to inštaluje v danej organizácii. Správca siete zmapuje všetky aktívne ako aj pasívne prvky sieťovej infraštruktúry, nainštaluje agentov vlastných alebo agentov SNMP a bude nastavovať pravidlá.



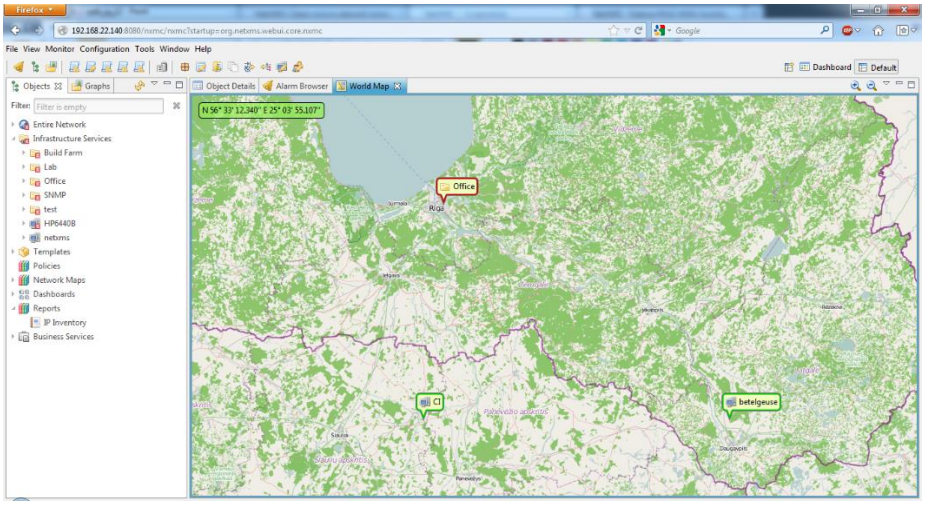
Obrázok 1 Nastavenie pravidiel v konzole NETXMS.
Zdroj: https://netxms.org/screenshots/

[12] IDS. In: [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni

Systém monitoruje aj prostriedky jednotlivých počítačov v sieťovej infraštruktúre ako aj priebežne monitoruje dátový tok v sieti. Tieto základné výstupy sú potrebné pre ďalšiu analýzu chovania sa sieťovej infraštruktúry. Je vhodné aj graficky mapovať umiestnenie jednotlivých prvkov sieťovej infraštruktúry:

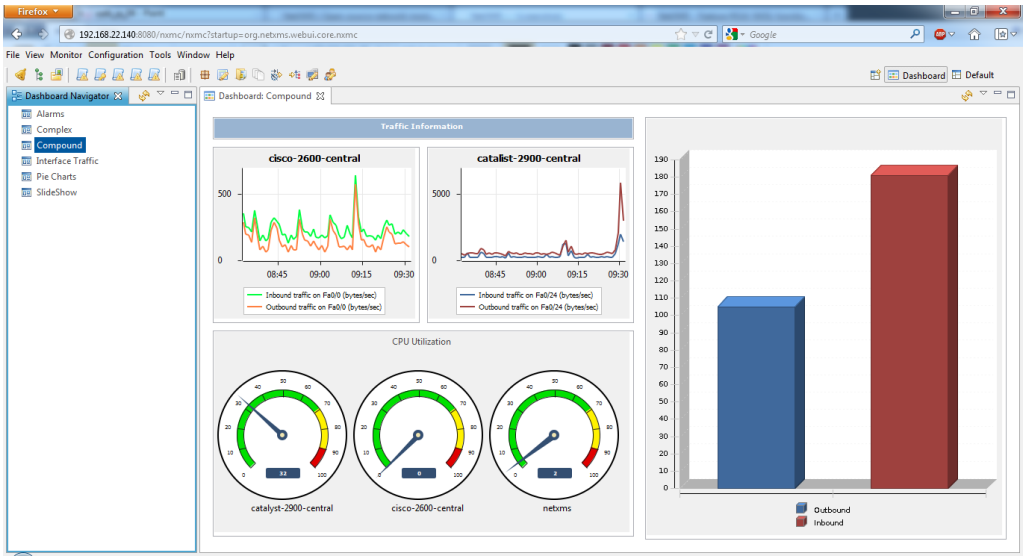


Obrázok 2 Stromová sieťová štruktúra
Zdroj: https://netxms.org/screenshots/



Obrázok 3 Geografická mapa rozloženia infraštruktúry.
Zdroj: https://netxms.org/screenshots/

Výsledkom spávneho nastavenia celého IDS systému NETXMS je mapovanie celej sieťovej infraštruktúry, detekcia štandardnej dátovej prevádzky a generovanie upozornení na anomálie. Tu je nutné zdôrazniť, že výsledkom je aj celkové monitorovanie výkonnosti sieťovej infraštruktúry a jej jednotlivých častí, čo spôsobí, že je možné detegovať zníženie výkonnosti a zachytiť tak neželaný stav, ktorý za bežnej štandardnej prevádzky môže byť spôsobený technickým výpadkom alebo prebiehajúcim útokom.



Obrázok 4 Monitorovanie dátovej komunikácie
Zdroj: https://netxms.org/screenshots/

Inštalácia servera netxms a klientov

Server NETXMS môže byť prevádzkovaný na viacerých druhoch operačných systémov, z ktorých vyberáme nasledujúce[13] :

- Windows 7 a vyšší, Windows Server 2003 a vyšší
- Red Hat Enterprise Linux, SUSE Linux, CentOS, Debian Linux, Ubuntu Linux
- FreeBSD, NetBSD, OpenBSD
- Solaris 10, 11
- HP-UX 11.23, 11.31
- AIX 5.3+

NETXMS agent sa môže prevádzkovať na rovnakých operačných systémoch. Dané operačné systémy musia mať inštalovaný databázový systém, ktorý je podporovaný serverovou časťou a to sú napríklad nasledujúce databázové systémy, pričom ich predpokladaná veľkosť môže byť značne rozdielna podľa druhu nasadenia systému NETXMS:

- Microsoft SQL 2005 a vyšší
- MySQL 5.1 a vyšší alebo MARIADB 10.0 a vyšší
- Oracle 11g, 12
- PostgreSQL 9.1 a vyšší
- DB/2 v10
- SQLite (iba pre testovacie účely)

Z hľadiska prevádzky alternatívneho open source riešenia sa odporúča operačný systém typu open source. Ako vhodnú alternatívu je možné použiť Debian Linux alebo Ubuntu Linux založený na Debian Linuxe. V našom prípade budeme využívať operačný systém Ubuntu 16.04 LTS, teda verziu s viacročnou technickou podporou.

Inštalácia sa začína stiahnutím balíka netxms-release_1.1_all.deb, ktorý obsahuje popis na NETXMS repozitár[14] (tento balík podporuje všetky systémy založené na Debian Linux alebo Ubuntu Linux):

[13] Installation - NetXMS 2.2.5 Administrator Guide. In: [cit. 01.07.2018]. Dostupné na internete: https://www.netxms.org/documentation/adminguide/installation.html

[14] Add software repositories. In: [cit. 01.07.2018]. Dostupné na internete: https://help.ubuntu.com/stable/ubuntu-help/addremove-sources.html.en

$ wget http://packages.netxms.org/netxms-release_1.1_all.deb
$ sudo dpkg -i netxms-release_1.1_all.deb

Obnoviť APT cache:

$ sudo apt-get update

Pre samotnú inštaláciu servera je potrebné použiť nasledovný príkaz:

apt-get install netxms-server

Aplikácia servera NETXMS však neobsahuje v štandarde ovládač na príslušnú databázovú platformu, tento ovládač je nutné nainštalovať samostatným príkazom:

apt-get install DRIVER_NAME

Parameter DRIVER_NAME je nutné nahradiť jedným z nasledujúcich výrazov, ktoré definujú databázovú platformu:

netxms-dbdrv-pgsql - PostgreSQL driver
netxms-dbdrv-mysql - MySQL driver
netxms-dbdrv-odbc - unixODBC driver (môže byť použitý s DB/2 a Microsoft SQL)
netxms-dbdrv-oracle - Oracle driver
Štandardné prihlasovacie údaje pre správcu sú po inštalácii servera a jeho ovládača databázy nasledovné :

Login: admin
Heslo: netxms

Pre inštaláciu NETXMS agenta sa používa nasledovný príkaz:

apt-get install netxms-agent

Inštalácia Web Management Console je v prípade Ubuntu Linux závislá na existencii JAVA prostredie servlet kontainerov. Môžu to byť Tomcat7 alebo Jetty7, na stránke netxms.org v sekcii Downloads sa stiahne príslušný súbor a po rozbalení sa nahrá do adresára pre webovú aplikáciu http://SERVER_IP:SERVER_PORT/nxmc/

Na záver sa inštaluje na server ešte aplikácia Desktop Management Console alebo Web Management Console, ako už je spomenuté vyššie. V našom prípade sa inštalujem Web Management Console. V praxi samotná inštalácia vrátane inštalácie Ubuntu Linux 16.04 na virtuálnom počítači systému Openstack trvala zhruba 1,5 hodiny vrátane aktualizácie systémových knižníc. Konfigurácia a nastavenie pravidiel systému NETXMS však trvalo zhruba 4 pracovné dni vzhľadom na nutnosť analýzy dátových tokov v sieti organizácie.

Záver

V zmysle legislatívnych predpisov na úrovni EÚ smerníc a EÚ nariadení sú povinné všetky dotknuté organizácie zabezpečovať aj detekciu narušení kybernetickej bezpečnosti. Existuje viacero spôsobov, ako to zabezpečiť, vzhľadom na povahu útokov však nie je možné

použiť univerzálne riešenie pre všetky organizácie. Jedným z použiteľných riešení v praxi je aj alternatívne open source riešenie netxms.org určené najmä k pasívnej detekcii narušenia kybernetickej bezpečnosti. Na jednoduchom príklade sa poukázalo na jednoduchosť inštalácie servera NETXMS a pomerne jednoduché nastavenie reportovania, ktoré však je časovo zdĺhavé z dôvodu časovej náročnosti analýzy dátovej prevádzky v organizácii, táto časová náročnosť je však aj pri podobných produktoch ako je napríklad SNORT.

Prínosom použitia navrhovaného riešenia je zníženie nákladov na prevádzku bezpečnostného riešenia sieťovej prevádzky v organizácii použitím alternatívneho open source riešenia a taktiež podľa nastavenia konfigurácie výrazné zvýšenie bezpečnosti celého IKT v organizácii.

Zoznam použitej literatúry:

AKANE. IPS/IDS ochrana. In: *Jak na webové stránky* [online] [cit. 04.12.2017]. Dostupné na internete: http://timehosting.cz/ipsids-ochrana/

FUKSOVÁ, N. Zvyšovanie konkurenčnej spôsobilosti malých a stredných podnikov v SR v rámci medzinárodnej spolupráce. In: *Forum Statisticum Slovacum Forum Statisticum Slovacum*. 2013, č. 9, s. 52-60. ISSN ISSN 1336-7420.

HOLCR, K. et al. *Policajné vedy : úvod do teórie a metodológie*. Praha: Aleš Čeněk, 2011. ISBN ISBN 9788073803292.

KAN, By Michael, MARCH 6, 2018 2:21PM EST, MARCH 6, 2018. Powerful DDoS Attack Sets New Record at 1.7 Tbps. In: *PCMAG* [online] [cit. 17.03.2018]. Dostupné na internete: https://www.pcmag.com/news/359693/powerful-ddos-attack-sets-new-record-at-1-7-tbps

KRČMÁŘ, P. DDoS útoky: jak se účinně bránit? In: *Root.cz* [online] [cit. 18.02.2018]. Dostupné na internete: https://www.root.cz/clanky/ddos-utoky-jak-se-ucinne-branit/

KRYVINSKA, N. An analytical approach for the modeling of real-time services over IP network. In: *Mathematics and Computers in Simulation* [online]. 2008, roč. 79, č. 4, s. 980-990. ISSN 03784754. DOI: 10.1016/j.matcom.2008.02.016

PAWERA, R. *Manažment európskej bezpečnosti*. Bratislava: Eurounion, 2004. ISBN 80-88984-71-8.

PORÁZIKOVÁ, E., VOJTECHOVSKÝ, J. Trends in e-business and their application in development of SMEs in Slovakia. In: *Management in theory and practice [elektronický zdroj]*. Praha: Newton College, 2016, s. S. 106-112. ISBN ISBN 978-80-87325-08-7.

STALLINGS, W. *Network security essentials: applications and standards*. Boston: Prentice Hall, 2011. ISBN 978-0-13-610805-4.

TREND.SK. Privacy by design by default kde končí filozofia a začína prax? In: *blog.etrend.sk* [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

ŽIVÉ.SK. Šéf výskumníkov, ktorí našli chybu aj v našich e-občianskych: Štát to nezvládol. Potrebuje rázny tím. In: *Živé.sk* [online] [cit. 13.12.2017]. Dostupné na internete: https://www.zive.sk/clanok/129275/sef-vyskumnikov-ktori-nasli-chybu-aj-v-nasich-e-obcianskych-stat-to-nezvladol-potrebuje-razny-tim/

Add software repositories. In: [cit. 01.07.2018]. Dostupné na internete: https://help.ubuntu.com/stable/ubuntu-help/addremove-sources.html.en

IDS. In: [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni

Installation — NetXMS 2.2.5 Administrator Guide. In: [cit. 01.07.2018]. Dostupné na internete: https://www.netxms.org/documentation/adminguide/installation.html

Meltdown and Spectre. In: [cit. 21.01.2018]. Dostupné na internete: https://meltdownattack.com/

Protect against speculative execution side-channel vulnerabilities in Windows client. In: [cit. 21.01.2018].
Dostupné na internete: https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in
Windows Server guidance to protect against the speculative execution side-channel vulnerabilities. In: [cit. 21.01.2018]. Dostupné na internete: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

Kontaktné údaje:

doc. RNDr. Michal Greguš, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
820 05 Bratislava
michal.gregus.ml@fm.uniba.sk

PhDr. Peter Veselý, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
820 05 Bratislava
Thomson Reuters Researcher ID: H-5695-2017
ORCID ID: 0000-0002-7857-6355
Scopus Author ID: 57195951243
peter.vesely@fm.uniba.sk

Znalosti informačního managementu – jeden z nástrojů prevence počítačové kriminality

Petr Jedinák

Abstrakt:
V příspěvku je upozorněno na skutečnost, že počítačová kriminalita je v současné době velký fenomén, se kterým musí orgány činné v trestním řízení počítat. Jedním z nástrojů potlačení počítačové kriminality je zvýšení znalosti uživatelů. Jedná se např. o znalosti základních principů informačních systémů a jejich ochranu a zabezpečení. To by mělo být vedeno s cílem ochrany dat, který každý uživatel zálohuje ve svém počítači.
Klíčová slová:
informační management, principy, správa informací, ochrana dat

Abstract:
The paper draws attention to the fact that cybercrime is currently a major phenomenon with which law enforcement bodies have to count. One of the tools to suppress computer crime is to increase user knowledge. These include knowledge of the basic principles of information systems and their protection and security. This should be done to protect the data that every user backs up on their computer..
Key words:
Information management, principles, information management, data protection

Úvod

V dnešní době, která je charakteristická svou globalizací a využíváním nejmodernějších technologických zařízení, je i z pohledu každého občana prioritní získávání informací. Informace patří ke strategickým zdrojům, podobně jako lidi, peníze a hmotná aktiva. Proto by měly být všechny informace spravovány tak, aby maximalizovaly jejich hodnotu a zabezpečit, aby:

1. V oblasti uživatelů a zákazníků:
- všichni mohli snadno najít, získat přístup a sdílet informace, na které mají nárok, když je potřebují,
- služby správy informací byly vytvářeny a udržovány ve spolupráci s odpovědnými pracovníky i uživateli a zákazníky,
- inovace a tvořivost v oblasti řízení informací a technologií umožňovaly jejich podporu.
- uživatelé i zákazníci měli důvěru v informační zdroje jim poskytované,
- pro usnadnění přístupu k informacím a souvisejícím službám byly používány vhodné normy.

2. V oblasti kvality informací:
- údaje a informace obsažené v informačních systémech a generované těmito systémy, byli přesné, spolehlivé a dostupné,
- každý prvek strategických dat a související atribut v informační architektuře měl jasně definované postupy správce, použité standardy a údržbu,
- (pokud je to možné) údaje pocházeli z jediného důvěryhodného zdroje, měly by být provedeny změny v jediném zdroji a změny automaticky promítnuté do odvozených dat.

3. V oblasti archivace a likvidace dat/informací:
- základní informace byly uchovávány v době, která je požadovaná, a poté byly řádně zlikvidovány v souladu s příslušnými interními normami a externími závazky.

Využívání informačního managementu v organizacích

V následujícím textu se zaměříme na možnosti počítačové kriminality ve vztahu k organizacím. Každá organizace se snaží, aby byla vnímána kladně svým okolím a excelentně

naplňovala vytyčené strategické cíle. Mezi své hlavní zdroje řadí právě informační zdroje a zdroje lidské, protože zaměstnanci tyto informační zdroje obsluhují a každodenně jich využívají při výkonu svých činností. Z pohledu všech činností organizace, jako např. tvorba strategie, osobní údaje zaměstnanců a mnoho dalších potřebných informací musí být zabezpečeno, aby data, která jsou součástí těchto informací, nebyla zneužita. Údaje a informace jsou rozhodující pro správné provedení rozhodnutí založená na faktech a důkazech. Existuje značný a téměř matoucí výběr souborů programového vybavení pro aplikační programy poskytování informací a generování různých souborů. Softwarové firmy neustále inovují a vytvářejí své produkty, které slouží následně organizacím[1].

Organizace generují, používají a archivují obrovské množství dat, z nichž některá byla pořízena za dlouhou dobu a za značné náklady. Jasné zásady a postupy pomůžou se o data a informace starat a hodnotit, vytěžovat a správně využívat. Jako možné řešení, které je některými organizacemi využíváno (např. instituce veřejné správy), je dokument „Informační principy pro veřejný sektor UK (Information Principles for the UK Public Sector) principy dobrého řízení dat a informací“. Tento dokument zveřejnil v roce 2012 kabinet pro britský veřejný sektor. Obsahoval sedm určených principů, které se staví do přirozené hierarchie. Uspořádání principů je zřejmé z této hierarchie, například je nepravděpodobné, aby byla informace opětovně použita (zásada 5), pokud není oceněna, řízena, podřízena účelu zpracování a standardizovaná (principy 1-4).

Principy dobrého řízení dat

Dle výše uvedeného dokumentu jsou principy dobrého řízení dat a informací následující[2]:

Princip 1 – *(hodnota informací)*. Informace jsou cenná aktiva, měly by být chápány a hodnoceny stejně, jako jiné pracovní a výrobní prostředky, jakými jsou budovy, stroje, lidé nebo peníze. Tento princip zdůrazňuje, že plná hodnota informací nespočívá pouze v jejich původním účelu, resp. ceně za pořízení, ale v možnosti jejich opětovného využití pro jiné účely.

Princip 2 *(řízení informací)* - Informace jsou spravovány/řízeny uchovávány, chráněny a využívány podle jejich hodnoty. Správci údajů a informací musí zvážit celý životní cyklus informací, a to od identifikace potřeb, tvorby, zajištění kvality, údržby, znovu použití a nakonec k archivaci nebo zničení, jakmile informace přestaly být užitečné. V kontextu správy informací je zapotřebí vytvořit řadu osvědčených postupů, například k zajištění vhodnosti dostupnosti a bezúhonnosti, vyhýbání se ztrátám a zajištění kontinuity mezi technologiemi a upgrady. Je zvláště důležité, aby byly osobní údaje přiměřeně chráněny. Informace se také musí řídit po celou dobu svého životního cyklu, aby bylo vždy jasné, kdo je za ně odpovědný *(tj. identifikovatelný majitel)*, a musí splňovat příslušné právní předpisy. Dalším důležitým faktorem správy dat a informací je důsledné hodnocení informačních rizik. Organizační kultura musí podporovat osvědčené postupy v oblasti údajů a managementu informací a ujistit se, že všichni odpovědní za zpracování informací jsou odborně vzdělaní a náležitě kvalifikovaní. Tento princip proto také zahrnuje procesy, role, odpovědnosti, vzdělávání/školení, organizační strukturu a organizační kulturu, které jsou zapotřebí k zajištění účinného a efektivního využívání informací.

Princip 3 *(účelnost informací)* Informace jsou vhodné pro daný účel - Informace musí být kvalitní a vhodné jak pro svůj účel, pro který jsou primárně určeny, taktéž musí poskytovat potenciál pro jejich sekundární použití. Nelze ale vždycky zabezpečit, že uživatel bude schopen předvídat sekundární využití informací, takže je důležité, aby byla sdělována kvalita informací

[1] ARMSTRONG, M. *Řízení lidských zdrojů*, Praha 2002, s. 783.

[2] ŠULC, V. – ČANDÍK, M. Základní principy informačního managementu. *Právo – Bezpečnost – Informace* [online]. 2017, roč. 4, č. 3 [cit. 25.02.2018]. Dostupné z: http://teorieib.cz/pbi/. ISSN 2336-3657.

konzistentně tak zaručit, že budoucí uživatelé mohou rozhodnout, zda informace jsou pro ně vhodné. Kvalita zahrnuje faktory, jako je přesnost, platnost, spolehlivost, včasnost, relevance a úplnost. Kvalita údajů a informací by měla být také pravidelná, aby se zajistilo, že alespoň odpovídají hodnotám, které byly posouzeny jako nezbytné pro účely, pro které byly informace získány. Dalším aspektem této zásady je také možnost zvážení, jak sladit platformu podpůrných technik a datových formátů s tím, jak budou informace využívány. Například pokud je pravděpodobné, že informace budou zapotřebí k online statistické analýze, nebude vhodné je ukládat v systému nebo ve formátu, který je přístupný pouze autorovi *(např. nestrukturovaný formát PDF).* Tento princip nevyžaduje, aby informace byly dokonalé, pouze aby disponovali správnou kvalitou pro jeho zamýšlené použití a že jejich kvalitativní charakter je pro budoucí uživatele jasný.

Princip 4 *(standardizace a propojitelnost informací)* - Informace jsou standardizované a propojitelné. Existuje totiž mnohem více příležitostí k využívání informací, pokud informace jsou k dispozici ve standardizovaném tvaru a ve spojitelných/propojitelných formách. Standardizace je důležitá pro strukturované informace, jako jsou definice datových sad *(skupin informací),* a také pro nestrukturované informace, jako jsou tagy meta dat aplikovaných na dokumenty. Normalizace v rámci organizace je důležitá pro to, aby zaměstnanci plně využívali informace; pokud organizace používá široce přijímané otevřené standardy, poskytuje tím dokonce větší hodnotu informací pro ostatní uživatele. Standardizace je důležitá jak pro oblast zaznamenávání informací, tak pro vnitřní strukturu, např.: *formát,* např. datum je vždy zadán jako yyyy-mm-dd, *obsah,* např. jméno, příjmení, adresa, atd., *pojmy,* např. definování rolí jako pacient, pachatel, žák, žadatel, řidič. Standardizace je otevřená i pro další atributy, ke kterým lze propojit informace. Dobrým příkladem jsou odkazy na dokumenty a citace, které umožňují čtenáři čerpat související informace. Podobný koncept může být aplikován na strukturované údaje založené na pochopení vztahů mezi položkami a použitím konzistentních identifikátorů pro odkazování na autoritativní zdroje *(základ "sémantického webu").*

Princip 5 *(znovupoužití)* Informace musí nabízet možnost opakovaného použití. Cena informací roste, pokud mohou být použity více než jednou, nebo více než pro jeden účel. Správný správce dat by měl proaktivně hledat příležitosti k opětovnému použití. Tento princip zahrnuje: Interní opětovné využití - co nejvíce informací určených pro primární účel použití a identifikaci sekundárního použití. Například provozní údaje mohou být někdy znovu použity ke stanovení nebo podpoře zlepšení výkonu nebo pro oblast výzkumu. Externí opětovné použití - sdílení informací s jinými organizacemi, a to buď v rámci veřejného sektoru, nebo soukromých podniků a občanů. Uchovávání hlavních dat - zajištění toho, aby data organizace představovala jediný autoritativní zdroj informací – např. o svém podnikání *(např. autoritativní seznam organizačních kódů),* který je vytvořený, spravovaný a udržovaný jako takový. Opětovné použití znamená zvážit, jaké informace může organizace zpřístupnit jinými a podívat se na to, jak může organizace opětovně využívat informace, které mají ostatní. Zatímco tato zásada silně podporuje opakované použití, je důležité si uvědomit, že opakované použití vyžaduje pečlivé posouzení založené na rizicích, pokud jde o využívání, v kontextu ochrany informací, jakož i zohlednění nákladů, přínosů, a veškerých práv nebo jiných obchodních podmínek. Informace, které se zpočátku jeví jako nevhodné, mohou být opakovaně použitelné, jestliže se změní jejich formát, nebo vnitřní struktura. Například některé provozní informace mohou být "anonymní" nebo agregované a pak mít širší hodnotu.

Princip 6 *(veřejné informace)* Veřejné informace jsou prezentované veřejně – jsou veřejně přístupné. Veřejné informace zahrnují objektivní a věcné informace o veřejných službách, generované v průběhu poskytování veřejných služeb a měly by být zveřejněné tam, kde je to možné, pokud neexistují naléhavé důvody pro jejich nezveřejnění. Tento princip přesahuje dodržování minimálních právních požadavků k proaktivnímu přístupu ke zveřejňování informací, k jejich prezentaci, formátování a propagaci užitečných informací pro

širší použití, aniž by bylo nutné výslovně dodržovat ustanovení dané v právních předpisech. K tomuto účelu můžou být použité různé kanály, které jsou k dispozici k prezentování informací veřejnosti, jako např. interní publikační procesy (úřední deska), použití firemních publikačních uzlů (firemní web), vztahy s "informačními zprostředkovateli" třetích stran, jako jsou např. komerční vydavatelé. Výhody zveřejňování informací by měly být vyváženy s ohledem na možná rizika a citlivost informací, jako jsou informace, které by mohly ohrozit soukromí jednotlivců, obchodní a právně privilegované informace a informace, které jsou nezbytné pro bezpečnost chodu organizací.

Princip 7 *(Přístupnost k osobním/interním informacím)* - Občané a podniky mají mít přístup k informacím o sobě, a to s vysvětlením, jak tyto informace používají ostatní. Rozsah tohoto požadavku může být variabilní – zveřejnění může být omezeno, rozšířeno, nebo např. přednostně zpřístupněno. Ve skutečnosti takové informace by měla být považovány za součást péče o občany, ačkoli je péče o informace přenesena na veřejnoprávní subjekt. Tento princip přesahuje minimální právní požadavky. Prosazuje proaktivní přístup, který občanům usnadňuje přístup k informacím o sobě, aniž by museli podávat žádosti, a to i v případě, kdy není přístup právně zdůvodněn. Toho lze dosáhnout například tím, že jsou přístupy k informacím bezpečné a jsou k dispozici online. Ke zvážení je možnost provádění některých transakcí/operací, například oprava nepřesností. Je zřejmé, že touha zveřejňovat informace musí být vyvážena určitými omezeními (výjimky by byly například zákonně privilegované informace a informace, které jsou potřebné k udržení bezpečnosti).

K naplnění uvedených principů bylo dále vymezeno deset klíčových zásad:

- **Určení odpovědnosti** *(identify responsibilities),* cílem kterého je rozhodnout, kdo je vlastníkem a kdo je odpovědný za správu a sdílení informačních prostředků. Důležitým je také to, kdo má efektivně koordinovat správu informací.
- **Provedení informačního auditu** *(conduct an information audit*), cílem kterého je identifikovat stávající informační entity, jejich uživatele, použití a důležitost. Součástí auditu by mělo být určení zdrojů, nákladů a hodnoty informací.
- **Propojení s procesy řízení** *(link to management processes*), cílem kterého je ověření/ujištění, že pro oblast rozhodování a klíčových obchodních procesů mají informace vysokou informační hodnotu a každý proces je posuzovaný podle svých informačních potřeb.
- **Systematické skenování** (*Systematic scanning*), které je zaměřeno na systémovou kontrolu podnikového prostředí a poskytování selektivních a přizpůsobených informací ve smyslu rozšíření relevantních funkcí hlavním manažerům. To přesahuje denní abstrakce.
- **Směs tvrdých/měkkých, vnitřních/vnějších informací** *(Mix hard/soft, internal/external),* cílem které je nabídnout/poskytnout možnost doplnění vzorů a postřehů, které se objevují zpracování dat/informací – např. v případě, když jsou data vyhodnocována kvalitativní, resp. kvantitativní analýzou, je k dispozici nabídka interních a externích dat vedle sebe.
- **Optimalizace nákupu informací** *(Optimise information purchases),* zaměřená na oblast zpracování poradenství, průzkum trhu, dostupných publikací, on-line služeb atd. Např. pro mnoho uživatelů je matoucí obsah médií – jejich název/pojmenování neodpovídá obsahu.
- **Zavedení informačních procesů** *(Introduce information processes*), cílem kterého je správné řízení informací zahrnující vytěžování dat, jejich klasifikaci, syntézu, předzpracování, vstupní a výstupní zpracování, atd.
- **Konvergence využitelných technologií** *(Exploit technology convergence),* jakými jsou telekomunikace, kancelářské systémy, typografie, atd.
- **Vypracování informační strategie** *(Develop an Information Strategy*), cílem které je stanovit rámec pro dlouhodobý horizont práce s informacemi. Informační strategie se nesmí zaměňovat se strategií informačních systémů *(jako systémů pro zpracování dat).*

- **Vytvoření kultury sdílení** *(Develop a sharing culture)* s cílem pochopení zavedené informační politiku, s důrazem na pozornost na kulturní dimenzi práce s informacemi, jejich rozsahem pro využití, a jejich hodnot.

Abychom mohli uplatnit tyto zásady, byl vytvořen tzv. model informačních zdrojů (The Information Resource Model)[3], obsahující pět základních atributů pro posouzení informačních zdrojů:

- **Identifikace** *(Identification*) - Jaké informace existují? Jak jsou identifikovatelné, jak jsou kódované/zaznamenané?
- **Vlastnictví** *(Ownership)* - Kdo je zodpovědný za různé informační subjekty (informační entity) a jejich koordinaci?
- **Náklady a hodnota** *(Cost and Value)* - základ pro rozhodnutí o pořízení, nákupu a užívání.
- **Rozvoj** *(Development)* Zvyšování jeho hodnoty nebo povzbuzení poptávky.
- **Využití** *(Exploitation)* - Proaktivní maximalizace jejich hodnoty *(peněžní benefity).*

Největším úskalím při posuzování informací je stanovení, jak přidat hodnotu k informacím. K řešení tohoto problému se musí zohlednit:

- **Aktuálnost** *(Timeliness)*: Informace z hlediska času velmi rychle podléhají prudkému snížení ceny. K tomuto účelu jsou k dispozici různé parametry, např. tzv. poločasy (half lives), stanovující jejich kritickou tržní hodnotu v závislosti na čase.
- **Dostupnost** *(Accessibility):* Snadné vyhledávání a pořízení/získání informací.
- **Použitelnost** *(Usability*): Snadné použití; možnost snadné manipulace, přizpůsobení, aby vyhovovaly používané aplikaci.
- **Užitečnost/použitelnost** *(Utility)*: vhodnost a použitelnost informace pro více aplikací.
- **Kvalita** *(Quality*): posouzení přesnosti, spolehlivosti, důvěryhodnosti, validity
- **Přizpůsobitelnost** *(Customising):* posouzení možností filtrace, třídění, vhodného stylu a formátu; posouzení zda vyžaduje minimální zpracování pro konkrétní aplikaci, atd.
- **Přenositelnost a archivace** *(Medium*): posouzení datových nosičů pro přenositelnost a průběžné používání.
- **Postprocessing (Repackaging):** posouzení možností přeformátování/migrace dat (změny typu dat) tak, aby odpovídalo dalšímu použití
- **Flexibilita** *(Flexibility*): posouzení pracnosti zpracování; možností přistupovat k nim použitím různých způsobů.
- **Opakovatelnost** *(Reusability)*: posouzení možnosti opětovného použití *(v ideálním případě se zlepšením jejich kvality, či zvýšením ceny*) kvalitu; posouzení množství uživatelů, kteří k nim mají přístup, atd. Existují i různé jiné kompromisy, např. přizpůsobení ve smyslu snížení objemu, ale s vyšší hodnotou, atd.

Ze všech takto definovaných bodů lze jednoznačně souhlasit s výrokem, že jsou to opatření vedoucí primárně k tomu, jak udělat organizaci výkonnější, efektivnější a kreativnější. Sekundárně by tyto nastavené procesy měly zabezpečit možnosti zcizování dat organizaci.

Závěr

Článek prezentuje základní principy informačního managementu, uvádí principy dobrého řízení dat a informací a deklaruje klíčové zásady pro naplnění těchto principů. Informační systémy a informační technologie se stávají strategickým faktorem úspěšnosti a konkurenceschopnosti[4]. To se týká nejenom organizací jako celku, ale i konkrétních zaměstnanců. Půjdeme-li ještě obecněji, tak tyto principy a zásady po určitých modifikacích lze uplatňovat u všech u všech uživatelů informačních technologií.

[3] POWELL, M. *Information Management: for Development Organisations*. Oxford: Oxfam GB, 2003.
[4] MLÁDKOVÁ, L., JEDINÁK, P. a kol. Management, 2009, s. 170.

Zoznam použitej literatúry:

ARMSTRONG, M. *Řízení lidských zdrojů,* Praha: Grada Publishing a.s., 2002, ISBN 80-247-0469-2.
MLÁDKOVÁ, L., JEDINÁK, P. a kol. *Management*. Plzeň: Aleš Čeněk, 2009, ISBN 978-80-7380-230-1.
POWELL, M. *Information Management: for Development Organisations*. 2. vyd. Oxford: Oxfam GB, 2003. ISBN 0-85598-483-X.
ŠULC, V. – ČANDÍK, M. *Základní principy informačního managementu*. *Právo – Bezpečnost – Informace* [online]. 2017, roč. 4, č. 3 [cit. 25.02.2018]. Dostupné z: http://teorieib.cz/pbi/. ISSN 2336-3657.

Kontaktní údaje:

PhDr. Petr Jedinák, Ph.D.
Fakulta bezpečnostního managementu
Policejní akademie České republiky v Praze
katedra managementu a informatiky

Znalostná aliancia kybernetickej bezpečnosti – konzorcium pre odbornú a právnu podporu Národného kompetenčného centra kybernetickej bezpečnosti SR

Miroslav Kelemen, Jaroslav Klátik

Abstrakt:
Príspevok prezentuje zámer projektu v oblasti odbornej a právnej implementácie budovania silnej kybernetickej bezpečnosti Európskej únie na národnej úrovni členského štátu v kontexte realizácie novej právnej normy o kybernetickej bezpečnosti štátu.
Kľúčové slová:
hybridné hrozby, kybernetická bezpečnosť, chránené záujmy, právo, kybernetická kriminológia.

Abstract:
The paper presents the project's intention to the professional and legal aspects of implementation the building of the European Union's strong cyber security at the national level of the Member State in the context of the new cyber security norm.
Key words:
hybrid threats, cyber security, protected interests, law, cyber criminology.

Úvod

Fenoménom dnešnej doby sú o.i. hybridné hrozby pre spoločnosť, vo verejnej a privátnej sfére, v národnej a medzinárodnej dimenzii. Nebezpečný potenciál majú nielen informačné aktivity, ale aj kybernetické hrozby a útoky na vybrané subjekty/ infraštruktúru/ štát. Prioritou medzinárodného spoločenstva sa preto stala kybernetická bezpečnosť.

Európska únia v uvedenej oblasti plánuje realizovať zámery vyjadrené v spoločnom oznámení Európskemu parlamentu a Rade „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ“. V dokumente sa zdôrazňuje kľúčová myšlienka, že „Kybernetická bezpečnosť je nevyhnutná pre našu prosperitu a bezpečnosť“.[1] „Naša budúca bezpečnosť závisí od transformácie našej schopnosti chrániť EÚ pred kybernetickými hrozbami: civilné infraštruktúry, ako aj vojenské kapacity závisia od bezpečných digitálnych systémov. Bolo to uznané na zasadnutí Európskej rady v júni 2017“[2] ako aj v Globálnej stratégii pre zahraničnú a bezpečnostnú politiku Európskej únie.[3]

Na národnej úrovni nachádzame v súčasnosti reakciu v podobe novej právnej normy zákona o kybernetickej bezpečnosti, s účinnosťou od 1. apríla 2018. Odborné a právne aspekty zákonom chránených záujmov sú preto predmetom systematického a dlhodobého skúmania.[4]

Identifikácia problému

Európska komisia vo svojom spoločnom oznámení z roku 2017 oznámila zámer podporiť vytvorenie siete stredísk kompetencií v oblasti kybernetickej bezpečnosti s cieľom podnietiť vývoj a zavádzanie technológií v oblasti kybernetickej bezpečnosti. Ako prvý krok v tomto smere Európska komisia vykonala mapovanie existujúcich centier odborných znalostí v oblasti kybernetickej bezpečnosti (napr. univerzitné oddelenie, výskumné centrum, atď.).

[1] Spoločné oznámenie Európskemu parlamentu a Rade „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti EÚ“, Brusel 13.9.2017, JOIN (2017) 450 final
[2] http://www.consilium.europa.eu/sk/press/press-releases/2017/06/23-euco-conclusions/
[3] http://europa.eu/globalstrategy/.
[4] KELEMEN, M. *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests*. 2nd. suppl. ed. Banská Bystrica: Belianum. Matej Bel University Press, 2017. p. 11.

Výsledky tohto mapovania budú preložené do tzv. "Cybersecurity Atlas" (index existujúcich centier EÚ pre kybernetickú bezpečnosť), ktorý bude verejne dostupný. Cieľom tohto Atlasu je stať sa cenným nástrojom a referenciou pre komunitu v oblasti kybernetickej bezpečnosti, ktorá hľadá potenciálnych partnerov a združuje európske zdroje.

Podľa informácií poskytnutých Slovenským styčným úradom pre výskum a rozvoj v Bruseli[5] Okrem toho prichádza Európska komisia v roku 2018 s pilotným projektom v rámci programu Horizont 2020 s cieľom prepojiť národné centrá do siete a vytvoriť nový impulz v oblasti kompetencií v oblasti kybernetickej bezpečnosti a rozvoja technológií.

Riešením problému na národnej úrovni je podľa nášho návrhu identifikácia Národného kompetenčného centra pre kybernetickú bezpečnosť SR a vytvorenie konzorcia pre jeho odbornú a právnu podporu realizácie uvedenej agendy.

Cieľ a spôsob riešenia projektu

Národným kompetenčným centrom pre kybernetickú bezpečnosť SR by mohlo byť pravdepodobne pracovisko Národného bezpečnostného úradu SR (rozhodnutie náleží štátu).

Cieľom plánovaného projektu je vytvorenie konzorcia pre odbornú a právnu podporu Národného kompetenčného centra pre kybernetickú bezpečnosť SR a realizácie uvedenej agendy.

Štruktúru partnerov konzorcia by mali tvoriť:
- Aktéri verejnej sféry;
- Aktéri privátnej sféry.

Charakter partnerov konzorcia by mal reprezentovať:
- Akademickú komunitu (primárne v oblasti edukácie IKT, práva);
- Verejné a privátne výskumné organizácie;
- Výrobcovia a systémoví integrátori v oblasti IKT, bezpečnostných technológií;
- Relevantné orgány verejnej správy;
- Predstavitelia sektorov kritickej infraštruktúry štátu (vrátane univerzít, ktoré pripravujú odborníkov pre jednotlivé sektory / podsektory KI štátu);
- Bezpečnostno-právna komunita;
- SME podniky v oblasti bezpečnostného vzdelávania, kybernetického priemyslu.

Záver

Na základe bezpečnostnej praxe môžeme súhlasiť s jedným z konštatovaní EUROPOLu v jeho hodnotení, že „Kybernetické hrozby prichádzajú zo strany neštátnych aj štátnych subjektov: často krát majú kriminálnu povahu, sú motivované ziskom, ale môžu mať aj politický alebo strategický charakter. Hrozbu trestnej činnosti zosilňujú nejasné hranice medzi počítačovou kriminalitou a „tradičnou“ trestnou činnosťou, keďže zločinci využívajú internet ako prostriedok na rozširovanie svojich činností a zároveň ako zdroj na nájdenie nových metód a nástrojov na páchanie trestnej činnosti“.[6]

Na národnej úrovni očakávame, že práca Národného kompetenčného centra kybernetickej bezpečnosti SR a Konzorcia pre odbornú a právnu podporu... zabezpečia realizáciu zámerov EÚ v oblasti posilnenia kyber-bezpečnosti, ako aj implementáciu ustanovení nového zákona o kybernetickej bezpečnosti SR:
- Koordináciou a metodickým usmernením aktivít z úrovne národnej autority;

[5] Slovak Liaison Office for Research and Development, Brussels, e-mail 24. januára 2018.
[6] EUROPOL: Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti, 2017.

- Podporou synergického efektu potenciálu relevantných aktérov na národnej úrovni (v rámci Znalostnej aliancie kybernetickej bezpečnosti, ale aj mimo nej);
- Podporou výskumu, inovácií technológií, výroby, ako aj edukácie v rámci kybernetickej bezpečnosti (na profesionálnej úrovni, vo vzdelávaní občianskej verejnosti, účasťou v národnom vzdelávacom programe na ZŠ, SŠ, realizáciou preventívnych programov a pod.);
- Rozvojom kapacít a spôsobilostí policajného a právneho vzdelávania pre forenzné vyšetrovanie trestných činov v kybernetickom priestore, a rozvojom kybernetickej kriminológie pre teóriu a prax.

Agentúra na podporu výskumu a vývoja (APVV) pripravuje vyhlásenie otvorenej verejnej výzvy na predkladanie žiadostí v rámci programu „Podpora prípravy projektov výskumu a vývoja rámcového programu EÚ pre výskum a inovácie do roku 2020 – Horizont 2020“ s označením PP H2020. Môže predstavovať reálny nástroj na medzinárodné „uchopenie“ problematiky.

Naša základná predstava pre realizáciu projektu „Znalostná aliancia kybernetickej bezpečnosti – Konzorcium pre odbornú a právnu podporu Národného kompetenčného centra kybernetickej bezpečnosti SR“ sa opiera podanie projektu na opakovanú výzvu Ministerstva školstva, vedy, výskumu a športu SR v oblasti Dlhodobý strategický výskum, v nasledujúcom období. Projektoví partneri – aktéri z verejnej aj privátnej sféry, sú vítaní.

Zoznam použitej literatúry:

EUROPOL. *Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti,* 2017.
KELEMEN, M. *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests*. 2nd. suppl. ed. Banská Bystrica: Belianum. Matej Bel University Press, 2017. 112 p. ISBN 978-80-557-1261-1
Slovak Liaison Office for Research and Development, Brussels, 24. januára 2018
Spoločné oznámenie Európskemu parlamentu a Rade „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti EÚ“, Brusel 13.9.2017, JOIN (2017) 450 final
http://www.consilium.europa.eu/sk/press/press-releases/2017/06/23-euco-conclusions/
http://europa.eu/globalstrategy/.

Kontaktné údaje:

Dr.h.c. prof. Ing. Miroslav Kelemen, DrSc., MBA, LL.M.
Katedra trestného práva, kriminológie, kriminalistiky a forenzných disciplín
Právnická fakulta UMB v Banskej Bystrici
miroslav.kelemen@umb.sk

doc. JUDr. Jaroslav Klátik, PhD.
Katedra trestného práva, kriminológie, kriminalistiky a forenzných disciplín
Právnická fakulta UMB v Banskej Bystrici
jaroslav.klatik@umb.sk

Online podnecovanie k terorizmu

Simona Kočišová

Abstrakt:
Príspevok sa zaoberá vybranými otázkami, špecifickej oblasti kriminality páchanej prostredníctvom internetu, ktorou je tzv. kyberterorizmus. Kyberterorizmus možno považovať za relatívne široký pojem, pod ktorý možno okrem iného subsumovať používanie internetu na účely spáchania násilných trestných činov spojených s terorizmom a majúcich za následok straty na životoch alebo vážne ublíženie na zdraví, pričom páchateľ má za cieľ nadobudnutie najmä politickej výhody. S ohľadom na rozsah danej problematiky sa príspevok zaoberá najmä podnecovaním k spáchaniu terorizmu, ktoré je realizované prostredníctvom internetu. [1]
Kľúčové slová:
terorizmus, kyberterorizmus, podnecovanie, internet, počítačová kriminalita

Abstract:
The contribution deals with selected issues, of the specific area of Internet Crime, which is so-called "cyber-terrorism". Cyber-terrorism can be considered as a relatively broad content under which we could subsumed inter alia the use of the Internet for the purpose of committing violent offenses linked to terrorism which result in death or serious bodily harm and by which the perpetrator seeks in particular a political advantage. In view of the extent of the issue, the contribution is particularly concerned with the incitement of terrorism, which is committed via the Internet.
Key words:
terrorism, cyber-terrorism, incitement, Internet, cyber-crime

Úvod

Technológia je jedným zo strategických faktorov vedúcich k rastúcemu využívaniu internetu teroristickými organizáciami a ich podporovateľmi na široké spektrum účelov vrátane náboru, financovania, propagandy, odbornej prípravy resp. tréningu, podnecovania k spáchaniu teroristických činov a zhromažďovania a šírenia informácií relevantných pre teroristické účely. Zatiaľ čo mnohé výhody využitia internetu sú samozrejmé, treba pripomenúť, že jeho využitie sa môže aj zneužiť na uľahčenie komunikácie v rámci teroristických organizácií a na prenos informácií, ako aj na materiálnu podporu plánovaných teroristických činov, ktoré vyžadujú osobitné technické znalosti a to aj vo vzťahu k účinnému vyšetrovaniu takýchto trestných činov. S ohľadom na vyššie uvedené sa tak príspevok zaoberá vybranými otázkami, vyššie uvedenej špecifickej oblasti kriminality páchanej prostredníctvom internetu, ktorá býva označovaná ako tzv. kyberterorizmus. Nakoľko kyberterorizmus možno chápať ako relatívne široký pojem, pod ktorý možno subsumovať vyššie špecifikované používanie internetu na teroristické účely, príspevok sa bude sústreďovať najmä na priblíženie podnecovania k terorizmu prostredníctvom internetu, ktoré možno nazvať ako tzv. online podnecovanie k terorizmu. Je teda zrejmé, že hoci aj v príspevku budem pracovať s všeobecným pojmom „používanie internetu na teroristické účely“, je potrebné nevyhnutne si toto slovné spojenie dať do súvislosti s konkrétnym druhom takéhoto používania, ktorým je práve podnecovanie k terorizmu.

Pre začiatok považujem za žiaduce určitým spôsobom sa venovať aspoň vo všeobecných kontúrach vymedzeniu jednotlivých pojmov, ako napr. počítačová kriminalita, kyberterorizmus a podnecovanie, nakoľko ich správne pochopenie prispieva ku komplexnosti príspevku. Nakoľko online podnecovanie k terorizmu je konaním, s ktorým sa spája cezhraničný charakter takéhoto typu kriminality, je tak relevantné ozrejmiť právne nástroje na medzinárodnej úrovni, ktoré majú za cieľ elimináciu takéhoto nežiaduceho protiprávneho konania.

[1] Táto práca bola podporovaná Agentúrou na podporu výskumu a vývoja na základe zmluvy č. APVV-14-0893

V tejto súvislosti tak príspevok stručne približuje opatrenia prijímané na úrovni Európskej únie (ďalej len „EÚ“), ktorých účelom je ako predchádzanie tak aj odstraňovanie a kriminalizácia kyberterorizmu a teda aj online podnecovania k terorizmu. V nadväznosti na uvedené tak príspevok približuje existenciu ako aj výstupy z projektu Clean IT, ktorý je špecifickým projektom z dielne EÚ a jeho vytvorenie ako aj fungovanie sa sústreďuje výlučne na otázky spojené s elimináciou používania internetu na teroristické účely. V prípade projektu Clean IT možno hovoriť o opatrení takpovediac nelegislatívneho charakteru, nakoľko výstupom projektu, neboli konkrétne legislatívne akty, avšak skôr zásady a praktické pokyny, ktoré určitým spôsobom ovplyvnili alebo môžu ovplyvniť následné prijatie budúcich aktov legislatívnej povahy.

Popri nelegislatívnom opatrení ako uvádzam vyššie sa však javí ako žiaduce poukázať aj na záväzné legislatívne opatrenia, pričom pre limitáciu rozsahu príspevku som vybrala aktuálnu, novú smernicu Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017), ktorej transpozičná lehota uplynie ku dňu 8. septembra 2018 a v súčasnosti je v Slovenskej republike, v pokročilom štádiu legislatívneho procesu vnútroštátna právna úprava, ktorou sa má transpozícia tejto smernice zabezpečiť. Uvedená smernica je všeobecným nástrojom v boji proti terorizmu, pričom sa však vo svojom čl. 5 zaoberá aj konkrétne otázkou online podnecovania k terorizmu. V tejto nadväznosti sa domnievam, že taktiež priblíženie uvedenej vnútroštátnej právnej úpravy je možno považovať za relevantné a preto v príspevku priblížim aj transpozíciu vyššie uvedenej smernice do právneho poriadku Slovenskej republiky.

Cieľom príspevku je najmä ozrejmiť obsah pojmu podnecovanie k terorizmu prostredníctvom internetu resp. online podnecovanie k terorizmu a v tejto nadväznosti je relevantné taktiež priblížiť opatrenia EÚ spočívajúce v realizácii projektu Clean IT a prijatí smernice Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017), ktorá sa v čl. 5 venuje online podnecovaniu k terorizmu.

Všeobecne k počítačovej kriminalite a k významu pojmov

Úvodom možno konštatovať, že v súčasných podmienkach je používanie počítačov takmer každodennou súčasťou našich životov. S ohľadom na nespočetné množstvo funkcií, ktoré plní využívanie počítačov je jeho úloha v súčasnej dobe nenahraditeľná. Vzhľadom na extrémne široký rozsah využitia možno len exemplifikatívnym výpočtom uviesť, že okrem zábavy spočívajúcej napr. v pozeraní videí, filmov či počúvaní hudby je v súčasnosti prostredníctvom počítačov možné zabezpečiť napr. priamu komunikáciu prekonávajúc mimoriadnu geografickú diaľku, pričom využitie počítačov taktiež predstavuje elementárny prostriedok pre výkon určitej práce, či prostriedok, ktorým je možné dosiahnuť uľahčenie každodenných povinností spojených s úhradami rôznych platieb a pod.. V neposlednom rade sú počítače využívané taktiež pre zabezpečenie určitej formy ochrany, napríklad prostredníctvom vytvorenia šifrovacích, či kódovacích programov, „zaheslovania“ súborov a vytvorenia iných bezpečnostných prvkov.

Napriek širokej škále pozitív, ktoré so sebou prináša využívanie počítačov sa však v novodobej ére, ktorú by bolo možné označiť aj ako tzv. digitálnu éru objavuje negatívny jav, ktorý sa stáva takpovediac fenoménom, pričom tento je označovaný ako počítačová kriminalita. Samotný pojem kriminalita všeobecne možno definovať ako určitý výskyt chovania, ktoré sa v spoločnosti považuje za trestné. Ide tak o súhrn trestných činov, ktoré sa v konkrétnej spoločnosti vyskytli a vyskytujú. Tieto činy resp. takéto chovanie je sankcionovateľné

v medziach trestného zákona príslušnej krajiny, pričom môže ísť tak aj o zjavné ako aj latentné chovanie resp. činy. Počítačová kriminalita je špecifickou kategóriou kriminality ako takej, pričom je potrebné zdôrazniť najmä skutočnosť, že táto sa stáva mimoriadne nebezpečnou najmä pre jej škodlivé následky, ktoré môžu dosahovať cezhraničný rozmer. Jedná sa tak o kriminalitu, ktorá v praxi „stiera" určité geografické hranice jednotlivých štátov, čo značne prispieva k sťaženiu jej odhaľovania. Vo vzťahu k definícii počítačovej kriminality právna teória zdôrazňuje, že pri jej definovaní možno uvedené realizovať najmä na základe jej vymedzenia prostredníctvom zadefinovania určitých skupín počítačových trestných činov. Bude sa tak jednať o kategóriu trestných činov, ktorých cieľom je počítač, ďalej skupinu trestných činov, pri ktorých má byť počítač používaný ako nástroj na ich spáchanie a treťou kategóriou sú také trestné činy, pri ktorých má počítač len vedľajšiu úlohu pri ich spáchaní.

Pri prvej kategórii trestných činov, ktoré tvoria počítačovú kriminalitu je možné počítač chápať ako cieľ, voči ktorému útok smeruje. Za týmto účelom páchateľ uskutočňuje útoky smerujúce najmä k prieniku do počítača s cieľom neoprávneného nadobudnutia určitých dát, či informácií, ktoré takýto počítač obsahuje. Jedná sa teda o „štandardné" prípady tzv. hackerstva. V rámci druhej kategórie trestných činov, ktoré tvoria počítačovú kriminalitu ide o také prípady, kedy je počítač chápaný len ako nástroj, ktorý je využívaný resp. zneužívaný na páchanie určitej trestnej činnosti. V praxi tak pôjde najmä o prípady falšovania peňazí, či ilegálneho sťahovania napr. audio-vizuálnych záznamov, ktoré vedie k porušeniu autorských práv, ktoré sú viazané k takýmto audio-vizuálnym záznamom. Pri tretej kategórii trestných činov má počítač len vedľajšiu úlohu pri páchaní trestných činov, pričom teda nie je nevyhnutným prostriedkom pre spáchanie trestného činu, avšak pri jeho spáchaní sa objavuje.[2] Do tejto kategórie by sme jednoznačne mohli zaradiť aj podnecovanie k terorizmu prostredníctvom internetu.

V súvislosti s vyššie uvedeným treba ozrejmiť, že nám vznikol pojem kyberterorizmus, pričom tento možno charakterizovať ako nezákonný útok alebo nebezpečenstvo útoku proti počítačom, počítačovým sieťam a informáciám, ktoré sú v nich skladované v prípade, ak je takýto útok vykonávaný za účelom zastrašenia alebo donútenia vlády, alebo obyvateľstva k podpore určitých sociálnych alebo politických cieľov.[3] V zmysle uvedenej definície by sme tak mohli tvrdiť, že kyberterorizmus bude zahŕňať trestné činy prvej a druhej kategórie, tak ako uvádzame vyššie, čiže trestné činy, kde je počítač cieľom útoku a trestné činy pri ktorých je počítač prostriedkom pre páchanie trestnej činnosti. Otázne sa tak javí, či pod kyberterorizmom možno chápať aj také protiprávne konanie páchateľa, pri ktorom počítač zohráva len vedľajšiu úlohu a teda či je možné pod kyberterorizmus subsumovať aj trestné činy tretej kategórie, tak ako uvádzame vyššie. Odpoveď na túto otázku a s tým súvisiace rozšírenie vyššie uvedenej definície môžeme jasne vydedukovať z obsahu Správy Úradu OSN pre drogy a kriminalitu (UNODC)[4] (ďalej len „Správa UNODC"), v zmysle ktorej je kyberterorizmus rozdelený do šiestich rôznych kategórií, ktorými sú: i) propaganda, ii) financovanie, iii) tréning, iv) plánovanie, v) vykonávanie a vi) kybernetické útoky. V tomto smere je tak potrebné upriamiť pozornosť na prvú kategóriu, ktorú tvorí tzv. propaganda. Pod propagandu UNODC zaradil nábor na terorizmus, radikalizáciu a podnecovanie k terorizmu.[5] Je tak nepochybné, že aj v prípade trestných činov, pri ktorých má počítač len vedľajšiu úlohu, ako je tomu v prípade

[2] Klimek, L. Základy trestného práva Európskej únie, Bratislava:Wolters Kluwer, 2017, s. 101 a 102
[3] Jirovský, V. Kybernetická kriminalita, Praha:Grada Publishing, a.s., 2007, s. 271
[4] Správa Úradu OSN pre drogy a kriminalitu (UNODC): Používanie internetu na teroristické účely 3, New York:2012, dostupná na: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
[5] Správa UNODC, s. 3

podnecovania k terorizmu prostredníctvom internetu, tieto je tiež možné subsumovať pod kyberterorizmus.

Po ozrejmení vyššie uvedeného zaradenia „internetového“ podnecovania k terorizmu pod kyberterorizmus považujem za relevantné taktiež poukázať aj na určité definičné znaky, prípadne zmeny vo vzťahu k definícii podnecovania na terorizmus v zmysle právneho rámca, ktorý bol vytvorený na úrovni EÚ. Prvotný právny akt sekundárneho práva EÚ upravujúci boj proti terorizmu, ktorým bolo rámcové rozhodnutie Rady 2002/475/SVV z 13. júna 2002 o boji proti terorizmu (Ú. v. ES L 164/3, 22. 6. 2002) neobsahoval formuláciu, ktorá by určitým spôsobom prispievala k definícii podnecovania k terorizmu, ktoré má byť postihnuteľné v zmysle textu predmetného rámcového rozhodnutia. Uvedený právny akt bol však zmenený a doplnený rámcovým rozhodnutím Rady 2008/919/SVV z 28. novembra 2008, ktorým sa mení a dopĺňa rámcové rozhodnutie 2002/475/SVV o boji proti terorizmu (Ú. v. E Ú L 330, 9.12.2008), v zmysle ktorého obsah čl. 3 ods. 1 písm. a) uvádza, že má ísť o verejné podnecovanie k páchaniu teroristického trestného činu, pričom uvedené sa vymedzuje ako *„…rozširovanie správy určenej verejnosti alebo jej sprístupnenie iným spôsobom s úmyslom podnietiť spáchanie jedného z trestných činov uvedených v článku 1 ods. 1 písm. a) až h), keď z takejto činnosti, či už priamo obhajujúcej teroristické trestné činy, alebo nie, plynie nebezpečenstvo spáchania jedného alebo viacerých takýchto trestných činov;…“*. Z uvedeného je tak zrejmé, že podnecovanie musí byť „verejné“, s čím súvisí obsah definície, z ktorého je zrejmé, že o verejné podnecovanie pôjde v prípade rozširovania správy, ktorá má byť adresovaná širšiemu okruhu subjektov a teda verejnosti, pričom relevantným aspektom je taktiež úmysel aby takéto rozširovanie predmetnej správy malo za cieľ podnietenie adresátov k spáchaniu niektorého z trestných činov terorizmu. Z uvedeného však len implicitne vyplýva, že okrem rozširovania napr. prostredníctvom tlače môže ísť aj o rozširovanie informácií prostredníctvom internetu.

V nadväznosti na uvedené však výraznú zmenu priniesla nová smernica Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV (Ú. v. EÚ L 88, 31.3.2017) (ďalej len „smernica 2017/541“), ktorá v čl. 5 uvádza, že pri verejnom podnecovaní sa jedná o šírenie alebo akékoľvek iné sprístupnenie akýmkoľvek spôsobom, či online alebo offline, informácií verejnosti s úmyslom podnietiť spáchanie niektorého z trestných činov terorizmu, tak ako sú uvedené v čl. 3 ods. 1 písm. a) až i) smernice 2017/541, pokiaľ takéto konanie priamo alebo nepriamo obhajuje páchanie trestných činov terorizmu, napríklad ich glorifikáciou, a spôsobuje tým riziko, že môže byť spáchaný jeden alebo viacero takých trestných činov, za predpokladu, že takéto konanie je úmyselné. V zmysle uvedeného tak možno uviesť, že podnecovanie k terorizmu prostredníctvom internetu je v považované za verejné podnecovanie v zmysle smernice 2017/541, za predpokladu, že spĺňa definičné znaky, medzi ktoré možno zaradiť konanie spočívajúce v rozširovaní určitej informácie vo vzťahu k špecifickému adresátovi, ktorým je verejnosť, ďalej spôsob takéhoto rozširovania, pričom je explicitne uvedené, že môže ísť aj o „online“ rozširovanie, z čoho je zrejmé, že pod uvedené možno zaradiť rozširovanie prostredníctvom internetu a taktiež musí byť splnený znak spočívajúci v úmysle páchateľa, ktorý smeruje k podnieteniu adresátov na spáchanie niektorého z trestných činov terorizmu.

Opatrenia EÚ

V uplynulých rokoch bol internet používaný zo strany islamských fundamentalistov ako hlavný nástroj slúžiaci na radikalizáciu nespokojných občanov v celej Európe, pričom uvedené malo za následok, že niektorí z týchto radikalizovaných občanov sa aj reálne dopustili

teroristických útokov. Aj vzhľadom na cezhraničný rozmer kriminality spočívajúcej v konaní, ktoré predstavuje využitie internetu na podnecovanie k terorizmu bolo tak účelnejšie prijať opatrenia nielen na vnútroštátnej úrovni, ale naopak na úrovni takpovediac regionálnej, pričom mimoriadne významným subjektom, schopným zabezpečiť vytvorenie opatrení na takejto úrovni je práve EÚ.[6]

Projekt Clean IT

Snaha EÚ smerujúca k prijatiu opatrení na účely zabezpečenia eliminácie teroristických prejavov na internete, vrátane internetového podnecovania k terorizmu sa výraznejšie začala prejavovať už v roku 2010, kedy Európska komisia vyzvala členské štáty EÚ, aby predložili návrhy projektov na riešenie problému internetového podnecovania k terorizmu a s tým bezprostredne súvisiacej internetovej radikalizácie. Európska komisia taktiež vyzvala členské štáty EÚ aby do pracovných metód, prostredníctvom ktorých by bolo možné realizovať predmetné projekty, zahrnuli spoluprácu verejného a súkromného sektora. Uvedené podnietilo holandské Ministerstvo bezpečnosti a spravodlivosti, aby predložilo návrh projektu s názvom "Clean IT". Cieľom projektu Clean IT bolo otvorenie konštruktívneho dialógu medzi jednotlivými vládami členských štátov, podnikmi a občianskou spoločnosťou s cieľom preskúmať, ako možno znížiť teroristické využívanie internetu. Tento dialóg následne vyústil do súboru všeobecných zásad a prehľadu možných osvedčených postupov, ktoré predstavujú riešenie pre boj proti internetovému podnecovaniu k terorizmu a s tým spojenej radikalizácie. Predmetné všeobecné zásady ako aj súbor jednotlivých osvedčených postupov sú sumarizované v rámci obsahu správy Clean IT s názvom Zníženie využívania internetu na účely terorizmu (ďalej len „Správa Clean IT“)[7].

Všeobecné zásady sú v Správe Clean IT formulované nasledovne:

I. Všetky organizácie tak ako sú definované v prvej časti správy majú záujem na zamedzení použitia internetu na teroristické účely. To si vyžaduje, aby boli organizácie dostatočne financované, zodpovedné, inovatívne, spoľahlivé a profesionálne v súvislosti s ich aktivitami zameranými na zníženie využívania internetu teroristami, zohľadňujúc ich kapacity a ciele.
II. Akékoľvek kroky podniknuté na zníženie teroristického použitia internetu, či už zo strany vlád alebo súkromných subjektov, musia byť v súlade s vnútroštátnymi ustanoveniami, právnymi nástrojmi EÚ a inými medzinárodnými právnymi nástrojmi a musia rešpektovať základné práva a občianske slobody vrátane prístupu k internetu, slobody prejavu a zhromažďovania sa, právo na súkromie a ochranu údajov.
III. Tento dokument nenavrhuje kroky, ktoré nemôžu byť zavedené právnymi predpismi z dôvodu ústavných alebo ľudských práv.
IV. Opatrenia na obmedzenie využívania internetu teroristami musia byť účinné, primerané a legitímne. Zníženie používania internetu na teroristické účely si vyžaduje transorganizačnú spoluprácu a malo by sa čo najviac začleniť do existujúcich programov, systémov a postupov.
V. V prípadoch jednoznačného nezákonného teroristického použitia internetu by sa mali podniknúť okamžité a primerané kroky s cieľom zastaviť takýto nezákonný stav.
VI. V prípadoch podozrenia z teroristického použitia internetu, ak sa činnosť nepovažuje za jednoznačne nezákonnú, ale môže sa považovať za škodlivú, organizácie (t. j. príslušné

[6] REDIKER, E. *e Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union,* 36 Mich. J. Int'l L. 321 (2015), s. 328, dostupné na: http://repository.law.umich.edu/mjil/vol36/iss2/3

[7] *Správa Clean IT: Zníženie využívania internetu na účely terorizmu*, Haag 2013, dostupná na: http://www.cleanitproject.eu/files/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf

orgány a poskytovatelia internetových služieb) sa najskôr pokúsia čo najrýchlejšie vyriešiť situáciu medzi sebou v rámci svojich príslušných právnych záväzkov a kompetencií. Organizácie majú vždy právo obrátiť sa na príslušný súd alebo požiadať o iný opravný prostriedok, ktorý príslušné zákony poskytujú.

VII. Dokonca aj v prípadoch, keď poskytovatelia prístupu na internet, dodávatelia obsahu, hostingové a vydavateľské spoločnosti nie sú právne zodpovedné za teroristický obsah alebo teroristickú činnosť v rámci svojej siete, budú stále konať v súlade s cieľmi tohto dokumentu a pomáhať znížiť teroristické využívanie internetu v rámci prostriedkov, ktoré poskytujú.

VIII. Používatelia internetu by mali disponovať prostriedkami na to, aby sa vyhli teroristickému používaniu internetu. Mali by existovať používateľsky prívetivé mechanizmy, ktoré by uľahčili nahlasovanie používania internetu na teroristické účely.

IX. Je potrebný ďalší dialóg a spolupráca medzi verejným a súkromným sektorom, založený na vzájomnej dôvere a porozumení, aby sa zabezpečilo pokračovanie a budúce rozšírenie možností zníženia využívania neustále sa vyvíjajúceho internetu na účely terorizmu.[8]

Z uvedeného je zrejmé, že EÚ sa prostredníctvom realizácie projektu Clean IT, ktorý bol vykonaný s finančnou podporou programu Európskej komisie na prevenciu a boj proti kriminalite, pod záštitou generálneho riaditeľstva Európskej komisie pre spravodlivosť, slobodu a bezpečnosť, snaží o elimináciu *inter alia* podnecovania k terorizmu prostredníctvom internetu. Uvedené sa snaží EÚ realizovať zapojením nielen vlád členských štátov, ale taktiež súkromného sektora, čo možno hodnotiť pozitívne, nakoľko zapojením tejto časti spoločnosti do diskusií sa môže predísť neprimeraným zásahom do činnosti subjektov spadajúcich pod tento súkromný sektor a ďalej možno týmto spôsobom zabezpečiť efektivitu eliminácie teroristických prejavov na internete, nakoľko práve subjekty súkromného sektora sú spravidla poskytovateľmi prístupu k internetu a služieb s tým spojených.

V Správe Clean IT sú taktiež špecifikované tzv. osvedčené postupy, ktoré determinujú realizáciu boja proti využívaniu internetu na teroristické účely v praxi. Tieto sú v Správe Clean IT kategorizované do štyroch typov osvedčených postupov nasledovne:

I. Proaktívne osvedčené postupy
II. Ohlasovacie osvedčených postupov
III. Reaktívne osvedčené postupy
IV. Vzdelávanie v oblasti osvedčených postupov.

Každý typ osvedčených postupov sa skladá z čiastkových oblastí, pričom prvá kategória tzv. proaktívnych osvedčených postupov v sebe zahŕňa praktické pokyny vo vzťahu k subkategóriám, ktorými sú právny rámec, politika vlád, pravidlá a podmienky a povedomie. Kategória tzv. ohlasovacích osvedčených postupov v sebe zahŕňa praktické pokyny pre subkategórie, ktorými sú mechanizmy označovania, mechanizmy prehliadača koncového používateľa a subkategória viažuca sa k referenčným jednotkám (t. j. subjektom, ktorým je možné nahlásiť potenciálny teroristický obsah) a tzv. pohotovostným linkám označovaným ako „hotlines“. Kategória reaktívnych osvedčených postupov v sebe zahŕňa praktické pokyny vo vzťahu k subkategóriám, ktorými sú oboznámenie sa s postupmi konania, ďalej subkategória venujúca sa kontaktným miestam, spolupráci pri vyšetrovaní, zdieľaniu informácií o zneužívaní a subkategória venujúca sa dobrovoľným kontrolným službám zo strany koncového užívateľa. Posledná kategória upravujúca vzdelávanie v oblasti osvedčených postupov zahŕňa praktické pokyny vo vzťahu k subkategórii, ktorá sa zaoberá výskumnou a poradenskou organizáciou.

[8] Správa Clean IT, s. 14

Pre obmedzujúci rozsah nie je možné prostredníctvom príspevku poskytnúť vyčerpávajúce ozrejmenie vo vzťahu k obsahu všetkých vyššie uvedených osvedčených postupov, preto sa ďalej zameriam na stručné ozrejmenie vybraných subkategórii, ktorými sú právny rámec a spolupráca pri vyšetrovaní. Každý z osvedčených postupov obsahuje časť venovanú výzve, resp. teda problému, ktorý sa v danej oblasti vyskytuje, ďalej časť venovanú popisu praktických pokynov, ktoré možno považovať za osvedčený postup pre naplnenie výzvy, resp. zamedzenia problému, ktorému spoločnosť v danej oblasti čelí a časť venovanú vysvetlivkám, ktoré ozrejmujú detaily navrhovaného osvedčeného postupu.

Osvedčený postup v oblasti právneho rámca vymedzuje ako výzvu to, že teroristické využívanie internetu nie je vždy jasne vysvetlené, čo môže byť sťažujúce vo vzťahu k uplatňovaniu existujúcej legislatívy upravujúcej protiprávne teroristické činnosti aj vo vzťahu k technickej realite kybernetického priestoru. Každý členský štát EÚ používa svoje vlastné právomoci na implementáciu právnych predpisov, ale nie vždy sú prispôsobené zvýšenému a cezhraničnému používaniu internetu teroristami. Rozdiely medzi vnútroštátnymi právnymi predpismi komplikujú činnosť kompetentných orgánov a internetových spoločností vo vzťahu k ich možnosti zaoberať sa teroristickým používaním internetu. Osvedčeným postupom je v nadväznosti na uvedené to, že právny rámec smerujúci k eliminácii využívania internetu na účely terorizmu by mal byť používateľom, mimovládnym organizáciám, príslušným orgánom a internetovým spoločnostiam jasne vysvetlený, aby ich činnosť bola účinnejšia. Zvýšená spolupráca a medzinárodná spolupráca pomôžu znížiť využívanie internetu teroristami. Podrobnosti sú ozrejmené v rámci časti tzv. vysvetlivky, v zmysle ktorej všetky opatrenia prijaté na zníženie teroristického použitia internetu musia byť v súlade s ľudskými právami, základnými právami a slobodami. Všetky opatrenia členských štátov sú založené na vykonávaní rámcového rozhodnutia EÚ z 13. júna 2002 o boji proti terorizmu a rámcového rozhodnutia EÚ 2008/919 / SVV z 28. novembra 2008. Viac analýz a vysvetlení rozdielov v právnych predpisoch členských štátov pomôže praktikom pri znižovaní medzinárodných aspektov teroristického použitia internetu. Členské štáty by mali mať zavedené jasné postupy na ukončenie používania internetu teroristom. Právny rámec na zníženie využívania internetu na účely terorizmu musí byť jasne vysvetlený používateľom, mimovládnym organizáciám, internetovým spoločnostiam a príslušným orgánom, aby ich práca bola efektívnejšia. Legislatíva na ochranu mládeže v niektorých krajinách poskytuje ochranu aj proti teroristickému používaniu internetu. Vlády by nemali klásť príliš veľký tlak na organizácie pri vysvetľovaní legislatívy, napr. tým, že by pohrozili (hoci legitímne, ale) veľmi invazívnymi opatreniami. Neprimeraným zásahom, hoci smerujúcim k zamedzeniu teroristického využívania internetu by mohlo dôjsť k neprimeranému zásahu do slobodu prejavu. Vysvetlenie právnych predpisov by malo byť vyvážené a malo by vychádzať z primeranej analýzy príslušných (vnútroštátnych) právnych predpisov.[9]

V prípade subkategórie zameranej na spoluprácu pri vyšetrovaní je výzva špecifikovaná tým spôsobom, že v prípadoch keď kompetentné orgány majú podozrenie na nezákonné používanie internetu na teroristické účely a kontaktujú internetové spoločnosti za účelom poskytnutia súčinnosti pri vyšetrovaní zo strany tretích subjektov, spolupráca medzi nimi nie je vždy efektívna a účinná. Osvedčeným postupom v takýchto prípadoch má byť to, aby sa niektoré internetové spoločnosti a kompetentné orgány dohodli na tom, ako efektívne a legálne spolupracovať pri vyšetrovaní pravdepodobnej nezákonnej teroristickej činnosti na internete. V rámci vysvetlivky je špecifikované, že právny základ a účel vyšetrovania príslušných orgánov by mali byť vždy jasné. V tomto smere by malo byť jasné najmä, aký je právny štatút

[9] Správa Clean IT, s. 17

žiadosti o spoluprácu, teda či je súčinnosť povinná na základe právnych predpisov alebo dobrovoľná podľa uváženia internetovej spoločnosti, ktorej sa žiadosť týka. Spolupráca by mala byť štandardizovaná, ale ľudský kontakt zostáva dôležitý. Internetové spoločnosti majú veľmi odlišné zázemie a aktivity, ale majú spoločné to, že chcú znížiť teroristické využívanie internetu. Výmena vedomostí môže zlepšiť vzájomné porozumenie a viesť k ďalšej spolupráci pri vyšetrovaní. Príslušné orgány by mali rešpektovať technickú integritu spoločnosti zapojenej do vyšetrovania ("neodpájajte servery, ktoré by mohli byť inými entitami, ako sú tie, na ktoré sa zameriavajú operácie"). Ak sú pre vyšetrovanie potrebné dodatočné informácie od internetových spoločností, ktoré už prijali rozumné opatrenia na zníženie teroristického použitia internetu, je pochopiteľné, že žiadajú štandardizovanú primeranú kompenzáciu zo strany vlády.[10]

V nadväznosti na vyššie uvedené je zrejmé, že výsledkom projektu Clean IT nie sú konkrétne štandardné legislatívne opatrenia, avšak prostredníctvom sumarizácie určitých praktických odporúčaní, ktoré sú uvedené v Správe Clean IT je možné zo strany dotknutých subjektov osvojiť si určité postupy a pravidlá, na ktorých možno realizovať ich činnosť, pričom za predpokladu, že tieto budú dodržiavané je možné účinným a efektívnym spôsobom eliminovať využívanie internetu na teroristické účely s čím bezprostredne súvisí aj eliminácia používaniu internetu na účely podnecovania k terorizmu. Okrem uvedeného tieto praktické pokyny vzhľadom na skutočnosť, že vyplývajú zo situácii, ktoré sa objavujú v praxi, môžu podnietiť vlády jednotlivých členských štátov aj k prijatiu relevantných opatrení priamo legislatívneho charakteru, pričom tieto budú náležite reagovať na požiadavky praxe, čo v konečnom dôsledku môže prispievať k efektívnosti právne záväznej eliminácie využívania internetu na teroristické účely, pod ktoré možno zahrnúť internetové podnecovanie k terorizmu.

Transpozícia čl. 5 smernice 2017/541 do právneho poriadku Slovenskej republiky

Smernica 2017/541 predstavuje právne záväzný legislatívny akt sekundárneho práva[11], pričom z hľadiska jej obsahu kriminalizuje verejné podnecovanie k terorizmu, pričom explicitne vyjadruje, že uvedené zahŕňa aj online podnecovanie k terorizmu, pod ktorým možno rozumieť podnecovanie k terorizmu realizované prostredníctvom internetu. Normatívne vymedzenie verejného podnecovania je vyjadrené v čl. 5 smernice 2017/541 nasledovne: *„Členské štáty prijmú potrebné opatrenia na zabezpečenie toho, aby šírenie alebo akékoľvek iné sprístupnenie akýmkoľvek spôsobom, či online alebo offline, informácií verejnosti s úmyslom podnietiť spáchanie niektorého z trestných činov uvedených v článku 3 ods. 1 písm. a) až i), pokiaľ takéto konanie priamo alebo nepriamo obhajuje páchanie trestných činov terorizmu, napríklad ich glorifikáciou, a spôsobuje tým riziko, že môže byť spáchaný jeden alebo viac takých trestných činov, bolo trestné, ak je takéto konanie úmyselné.“*. Vo viacerých bodoch recitálu k smernici 2017/541 „únijný zákonodarca“ ozrejmuje, akým spôsobom má byť chápané online podnecovanie ako aj čo je cieľom kriminalizácie takéhoto online podnecovania.

V zmysle bodu 10 recitálu k smernici 2017/541: *„Za trestný čin verejného podnecovania k spáchaniu trestného činu terorizmu sa považuje okrem iného glorifikácia a ospravedlňovanie terorizmu alebo šírenie správ či snímok, či už online alebo offline, aj v súvislosti s obeťami terorizmu ako spôsob získavania podpory pre ciele teroristov alebo vážneho zastrašovania obyvateľstva. Takéto správanie by malo byť trestné, ak vytvára riziko spáchania teroristických činov. V každom konkrétnom prípade by sa pri určovaní, či takéto riziko vzniklo, mali zvažovať osobitné okolnosti prípadu, napríklad autor a adresát*

[10] Správa Clean IT, s. 24

[11] Podrobne k účinkom smerníc pozri tiež SIMAN, M. - SLAŠŤAN, M. *Právo Európskej únie (inštitucionálny systém a právny poriadok Únie s judikatúrou)*. Bratislava: EUROIURIS - Európske právne centrum, o. z., 2012, s. 334 a nasl.

komunikácie, ako aj kontext, v ktorom bol daný skutok spáchaný. Pri uplatňovaní ustanovenia o verejnom podnecovaní v súlade s vnútroštátnym právom by sa tiež mala zvážiť závažnosť a vierohodnosť takéhoto rizika.“. Predmetný recitál špecifikuje aké konanie sa má všeobecne považovať za podnecovanie, pričom v rámci tohto bodu sa nerozlišuje medzi spôsobom akým je podnecovanie realizované, čiže nerozlišuje sa, či má ísť o podnecovanie prostredníctvom internetu, alebo iným spôsobom.

Obsah recitálu 22 k smernici 2017/541 už však pracuje s online resp. internetovým podnecovaním k terorizmu, pričom poskytuje členským štátom návod, na základe ktorého je možné prijať náležité opatrenia na jeho elimináciu: *„Účinným prostriedkom boja proti terorizmu na internete je odstrániť online obsah, ktorý predstavuje verejné podnecovanie k páchaniu trestných činov terorizmu, pri jeho zdroji. Členské štáty by sa mali čo najviac usilovať o spoluprácu s tretími krajinami v snahe zabezpečiť odstránenie online obsahu, ktorý predstavuje verejné podnecovanie k páchaniu trestných činov terorizmu, zo serverov na ich území. Ak však odstránenie takéhoto obsahu pri jeho zdroji nie je možné, môžu sa zaviesť mechanizmy, ktoré zablokujú prístup k takémuto obsahu z územia Únie. Opatrenia, ktoré členské štáty prijmú v súlade s touto smernicou s cieľom odstrániť online obsah, ktorý predstavuje verejné podnecovanie k páchaniu trestných činov terorizmu, alebo, ak to nie je uskutočniteľné, s cieľom zablokovať prístup k takémuto obsahu, by mohli vychádzať z rôznych druhov verejných aktov, či už legislatívnych alebo nelegislatívnych aktov alebo súdnych rozhodnutí. V tejto súvislosti touto smernicou nie sú dotknuté dobrovoľné opatrenia, ktoré prijme internetový priemysel s cieľom zabrániť zneužívaniu služieb, ktoré poskytuje, ani akákoľvek podpora členských štátov takýmto opatreniam, ako sú napríklad odhaľovanie a nahlasovanie teroristického obsahu. Bez ohľadu na to, aký základ sa zvolí pre opatrenia alebo metódy, členské štáty by mali zaručiť, že tento základ poskytne dostatočnú mieru právnej istoty a predvídateľnosti pre používateľov a poskytovateľov služieb, ako aj možnosť súdnej nápravy v súlade s vnútroštátnym právom. Všetky takéto opatrenia musia zohľadňovať práva koncových používateľov a byť v súlade s existujúcimi právnymi a súdnymi postupmi, ako aj s Chartou základných práv Európskej únie (Charta).“*.

Na uvedené nadväzuje znenie recitálu 23 k smernici 2017/541, v zmysle ktorého: *„Odstránením online obsahu, ktorý predstavuje verejné podnecovanie k páchaniu trestných činov terorizmu, alebo ak to nie je uskutočniteľné, zablokovaním prístupu k takémuto obsahu v súlade s touto smernicou by nemali byť dotknuté pravidlá stanovené v smernici Európskeho parlamentu a Rady 2000/31/ES (11). Konkrétne by sa poskytovateľom služieb nemala ukladať všeobecná povinnosť monitorovať informácie, ktoré prenášajú alebo ktoré uložili, ani aktívne zisťovať skutočnosti alebo okolnosti, ktoré by naznačovali, že ide o nezákonnú činnosť. Okrem toho by poskytovatelia hostingových služieb nemali byť uznaní za zodpovedných, ak nevedia o nezákonnej činnosti alebo informáciách a nie sú si vedomí skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo informácie.“*. Z uvedeného je zreteľné, že vo vzťahu k eliminácii online podnecovania k terorizmu je potrebné aby členské štáty prijali najmä opatrenia smerujúce k možnosti odstránenia takéhoto obsahu. Je tak možné konštatovať, že členské štáty majú klásť dôraz nielen na samotnú kriminalizáciu konania spočívajúceho v online podnecovaní k terorizmu, ale aj na určitú prevenciu spočívajúcu v odstránení takéhoto obsahu, za účelom zabezpečenia aby sa k takémuto obsahu nemohli dostať potenciálni adresáti, ktorí by takýmto spôsobom mohli byť radikalizovaní a „inšpirovaní“ k obdobnej alebo súvisiacej trestnej činnosti.

V podmienkach Slovenskej republiky sa transpozícia smernice 2017/541 realizuje prostredníctvom návrhu zákona, ktorým sa mení a dopĺňa zákon č. 300/2005 Z. z. Trestný zákon

v znení neskorších predpisov a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“). Predmetný návrh zákona bol predložený zo strany Ministerstva spravodlivosti Slovenskej republiky, ako gestora zákona č. 300/2005 Z. z. Trestný zákon, do medzirezortného pripomienkového konania pod číslom legislatívneho procesu LP/2017/936, pričom v súčasnosti je predmetný návrh zákona už takpovediac vo finálnej fáze legislatívneho procesu, nakoľko bol predložený Národnej rade Slovenskej republiky.

Ešte vo fáze medzirezortného pripomienkového konania predkladateľ vo vlastnom materiáli transponoval čl. 5 smernice 2017/541 nasledovne: *„Kto verejne podnecuje na spáchanie niektorého z trestných činov terorizmu spôsobom obhajujúcim alebo ospravedlňujúcim spáchanie takého činu a spôsobí tak nebezpečenstvo jeho spáchania, potrestá sa odňatím slobody na tri roky až desať rokov.“*. V dôvodovej správe k navrhovanému zneniu predkladateľ uvádzal, že *„Ide o situáciu kedy páchateľ verejne podnecuje k spáchaniu niektorého trestného činu terorizmu a to takým spôsobom, že prípadné spáchanie obhajuje alebo ospravedlňuje, čím spôsobí riziko reálneho spáchania niektorého z trestných činov terorizmu. Pod verejným podnecovaním treba pojem „verejne“ chápať v zmysle § 122 ods. 2 Trestného zákona, čiže ak je predmetné podnecovanie realizované obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom, alebo pred viac ako dvoma súčasne prítomnými osobami. Vychádzajúc z uvedeného je zrejmé, že aj „online“ podnecovanie, teda napr. prostredníctvom sociálnych sietí a internetu bude možné subsumovať pod trestný čin niektorých foriem účasti na terorizmu v zmysle navrhovaného § 419b ods. 1.“*, čím zdôrazňoval, že pod verejné podnecovanie, hoci to nie je explicitne vyjadrené v dikcii navrhovaného ustanovenia spadá aj online podnecovanie k terorizmu.

Uvedené odôvodnenie sa zdalo nedostatočné pripomienkujúcemu subjektu, ktorým bola Generálna prokuratúra Slovenskej republiky, ktorá vzniesla k tejto časti dôvodovej správy zásadnú pripomienku, v zmysle ktorej požadovala za účelom dôkladnejšieho vysvetlenia konceptu „verejného podnecovania k páchaniu trestných činov terorizmu“ v kontexte transpozície čl. 5 smernice (EÚ) 2017/541 aby sa ešte dôslednejšie precizovalo používanie pojmu „verejne“, a to najmä s ohľadom na skutočnosť, že podľa bodu 10 preambuly i čl. 5 smernice (EÚ) 2017/541 sa má za trestný čin podnecovania k páchaniu trestných činov terorizmu považovať aj šírenie správ či snímok „offline“ (nie iba „online“). Generálna prokuratúra Slovenskej republiky vo vznesenej pripomienke uviedla, že z praxe jej boli signalizované odlišnosti v chápaní pojmu „verejne“, ak sa spája s použitím počítačovej siete, pričom uvedené podporila komentárom Trestný zákon (Všeobecná časť) od autorov Eduard Burda, Jozef Čentéš, Juraj Kolesár, Jozef Záhora a kol., vydavateľstvo C.H.Beck, I. vydanie 2010, kde sa na str. 700 uvádza: *„Informácia je šírená verejne hromadne účinným spôsobom použitím počítačovej siete, aj keď je šírená mailom, ak je určená veľkému počtu osôb, najmä pokiaľ ide o nevyžiadanú poštu (tzv. spam). Ak je však mail použitý čisto na osobné účely, napríklad na priamo komunikáciu s inou konkrétnou osobou, nejde o verejné šírenie informácie hromadne účinným spôsobom.“*. Predkladateľ akceptoval túto pripomienku a na základe uvedeného upravil text dôvodovej správy nasledovne: *„Ide o situáciu kedy páchateľ verejne podnecuje k spáchaniu niektorého trestného činu terorizmu a to takým spôsobom, že prípadné spáchanie obhajuje alebo ospravedlňuje, čím v zásade môže spôsobiť riziko reálneho spáchania niektorého z trestných činov terorizmu. Pod verejným podnecovaním treba pojem „verejne“ chápať v zmysle § 122 ods. 2 Trestného zákona, čiže ak je predmetné podnecovanie realizované obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom, alebo pred viac ako dvoma súčasne prítomnými osobami. Vychádzajúc z uvedeného je zrejmé, že okrem „offline“ podnecovania aj „online“ podnecovanie, teda napr. prostredníctvom sociálnych sietí*

a internetu bude možné subsumovať pod trestný čin niektorých foriem účasti na terorizmu v zmysle navrhovaného § 419b ods. 1. Pre potreby praxe je potrebné zdôrazniť, že pojem verejne v súvislosti s využitím počítačovej siete je pri tomto trestnom čine potrebné chápať tým spôsobom, že zahŕňa situácie, kedy je určitá informácia šírená verejne hromadne účinným spôsobom a aj keď je šírená e-mailom, ktorý nemusí byť nevyhnutne určený veľkému počtu osôb (tzv. spam), postačujúce je ak je šírená e-mailom, ktorý bol použitý na čisto súkromné účely, napríklad na priamu komunikáciu s jednou konkrétnou osobou.“.

Z uvedeného je tak zrejmé, že predkladateľ sa doplnením odôvodnenia snaží aby internetové podnecovanie sa považovalo za verejné a tak bolo postihnuteľné prostredníctvom navrhovanej skutkovej podstaty trestného činu verejného podnecovania k terorizmu a to vo všetkých prípadoch, kedy dochádza k použitiu počítačovej siete a teda internetu na účely podnecovania k terorizmu, hoci by aj došlo k takému konaniu, kedy by bol internet využitý len na „súkromnú“ komunikáciu medzi dvoma osobami napr. prostredníctvom e-mailu. Je potrebné taktiež zdôrazniť, že v priebehu rozporových konaní, ktoré sa uskutočnili na základe vznesenia zásadných pripomienok aj iných subjektov (napr. Ministerstvo vnútra Slovenskej republiky, či Najvyšší súd Slovenskej republiky) sa aj mierne upravila dikcia navrhovaného ustanovenia nasledovne: *„Kto verejne podnecuje na spáchanie niektorého z trestných činov terorizmu alebo verejne schvaľuje niektorý z trestných činov terorizmu, potrestá sa odňatím slobody na tri roky až desať rokov.”*.

Vo vzťahu k odstraňovaniu online obsahu, ktorý je možné spájať s podnecovaním k terorizmu a ktoré upravuje čl. 21 smernice 2017/541 predkladateľ preukázal transpozíciu odkazom na už existujúcu právnu úpravu, najmä s poukazom na § 16a zákona Národnej rady Slovenskej republiky č. 46/1993 Zb. o Slovenskej informačnej službe v zmysle ktorého: *„Právnická osoba alebo fyzická osoba, ktorá prevádzkuje webové sídlo alebo poskytuje doménové meno, je povinná na základe príkazu súdu vydaného na základe žiadosti informačnej služby podľa odseku 3 zamedziť prevádzku webového sídla alebo prístup na doménové meno, ak prevádzkou takéhoto webového sídla alebo doménového mena dochádza k šíreniu myšlienok podporujúcich alebo propagujúcich terorizmus, politický alebo náboženský extrémizmus, extrémizmus prejavujúci sa násilným spôsobom alebo škodlivé sektárske zoskupenia.“*.

V nadväznosti na uvedené sa domnievam, že je možné konštatovať, že predmetná formulácia normatívneho textu ako aj dôvodovej správy je dostatočná na účely preukázania úplnej transpozície čl. 5 smernice 2017/541 a teda, že predkladateľ náležite legislatívne upravil kriminalizáciu podnecovania k terorizmu vrátane online podnecovania k terorizmu.

Záver

V nadväznosti na cieľ príspevku, ktorým bolo najmä ozrejmenie obsahu pojmu podnecovanie k terorizmu prostredníctvom internetu resp. online podnecovanie k terorizmu a v tejto nadväznosti priblíženie opatrení EÚ spočívajúcich v realizácii projektu Clean IT a prijatí smernice 2017/541 sa domnievam, že je potrebné zosumarizovať, že online podnecovanie k terorizmu možno vo všeobecnosti subsumovať pod tzv. verejné podnecovanie k terorizmu. V tejto nadväznosti tak v prípade internetového resp. online podnecovania k terorizmu pôjde o konanie spočívajúce v online šírení informácií verejnosti, či už v podobe správ alebo snímok, v rámci ktorých pôjde najmä, ale nie len, napríklad o glorifikáciu, ospravedlňovanie terorizmu, či schvaľovanie terorizmu s cieľom podnietiť spáchanie niektorého z trestných činov terorizmu, alebo na účely získania podpory terorizmu alebo vážneho zastrašenia obyvateľstva. Pod pojmom „online“ šírenie treba chápať podnecovanie k terorizmu prostredníctvom použitia počítačovej siete. Nakoľko v podmienkach Slovenskej

republiky sa má v zmysle dôvodovej správy online podnecovanie k terorizmu postihovať v rámci verejného podnecovania k terorizmu, predkladateľ vhodne precizoval odôvodnenie k navrhovanému normatívnemu textu, tak aby bolo možné zreteľne určiť, že ide o prípady kedy je využitá počítačová sieť, pričom sa má jednať aj o také prípady, kedy je počítačová sieť využitá na „neverejnú komunikáciu" napr. e-mail len medzi dvoma osobami. V prípade, že by uvedené odôvodnenie absentovalo, javilo by sa ako diskutabilné, či by mohlo byť takéto online podnecovanie subsumované pod pojem verejné podnecovanie, nakoľko ide o súkromnú komunikáciu, hoci aj s použitím počítačovej siete, a teda problematickým by sa javilo splnenie podmienky „verejnosti".

Vo vzťahu k priblíženiu opatrení EÚ spočívajúcich v realizácii projektu Clean IT treba poukázať najmä na skutočnosť, že závery vyplývajúce zo Správy Clean IT sa pretavili do naformulovania všeobecných zásad a súboru praktických pokynov, ktoré sú označované ako osvedčené postupy. Vytvorenie takéhoto súboru zásad a s tým spojených praktických pokynov má za cieľ zníženie využívania internetu na účely terorizmu. Pretože projekt Clean IT mal takpovediac nelegislatívny prístup, výsledky nemôžu byť akýmkoľvek spôsobom právne záväzné s čím súvisí aj skutočnosť, že využitie osvedčených postupov a dodržiavanie všeobecných zásad nemožno legálne presadzovať. Nakoľko teda v zmysle uvedeného závery vyplývajúce zo Správy Clean IT nemožno považovať za záväzné legislatívne akty je potrebné zamyslieť sa nad ich významom. Hoci predstavujú nelegislatívne opatrenie a nemožno s nimi priamo spájať právnu záväznosť je zrejmé, že môžu predstavovať prínos a to aj s ohľadom na to, že ide o výsledky dialógu nielen medzi vládami členských štátov, ale aj dialógu so súkromným sektorom. Ďalej možno na základe formulácie jednotlivých osvedčených postupov konštatovať, že vzhľadom na to, že tieto obsahujú ako vymedzenie problémov, vyplývajúcich z praxe, tak aj návrhy riešení, je zo strany členských štátov možné inšpirovať sa nimi pri vytváraní legislatívnych opatrení, čo len podčiarkuje význam týchto záverov vyplývajúcich zo Správy Clean IT, aj napriek tomu, že nie sú spájané s právnou záväznosťou.

Vo vzťahu k priblíženiu opatrenia EÚ, ktorým je smernica 2017/541 som sa snažila poukázať najmä na relevantné časti tejto smernice vo vzťahu k online podnecovaniu k terorizmu. Oproti predchádzajúcim právnym aktom EÚ, ktoré upravovali podnecovanie k terorizmu, smernica 2017/541 predstavuje určité nóvum už len z toho titulu, že explicitne pracuje s pojmom „online" podnecovanie k terorizmu. Hoci je smernica 2017/541 zameraná na boj proti terorizmu všeobecne, nemalú pozornosť venuje aj online podnecovaniu k terorizmu, čo možno konštatovať už len z toho titulu, že sú mu venované taktiež rozsiahlejšie časti recitálu k smernici 2017/541, pričom uvedené len poukazuje na skutočnosť, že online podnecovanie k terorizmu predstavuje aktuálny problém, pričom vzhľadom na rozvoj technologického prostredia môže aj do budúcna predstavovať boj proti tomuto online podnecovaniu k terorizmu nemalú výzvu pre prax.

Zoznam použitej literatúry:

FISHER, S., ŠKODA, J. *Sociální patologie: Závažné sociálně patologické jevy, příčiny, prevence, možnosti řešení,* 2., rozšířené a aktualizované vydání, Praha: Grada Publishing, a.s., 2014, s. 169 a 170, ISBN-978-80-247-5046-0

JIROVSKÝ, V. *Kybernetická kriminalita*, Praha: Grada Publishing, a.s., 2007, ISBN-978-80-247-1561-2

KLIMEK, L. *Základy trestného práva Európskej únie*, Bratislava: Wolters Kluwer, 2017, ISBN-978-80-8168-601-6

REDIKER, E. e Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union, 36 Mich. J. Int'l L. 321 (2015), s. 328, dostupné na: http://repository.law.umich.edu/mjil/vol36/iss2/3
SIMAN, M., SLAŠŤAN, M. *Právo Európskej únie* (inštitucionálny systém a právny poriadok Únie s judikatúrou), Bratislava: EUROIURIS - Európske právne centrum, o. z., 2012, ISBN 978-80-89406-12-8
Správa Clean IT: Zníženie využívania internetu na účely terorizmu, 2013, dostupná na: http://www.cleanitproject.eu/files/wp-content/uploads/2013/01/Reducing-terrorist-use-of-the-internet.pdf
Správa Úradu OSN pre drogy a kriminalitu (UNODC): *Používanie internetu na teroristické účely 3*, New York:2012, dostupná na: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Zoznam internetových zdrojov:

http://www.cleanitproject.eu (navštívené 24. 3. 2018)
https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-936 (navštívené 26. 3. 2018)
https://www.nrsr.sk/web/Default.aspx?sid=zakony/zakon&MasterID=6708 (navštívené 28. 3. 2018)

Kontaktné údaje:

Mgr. Simona Kočišová
Paneurópska vysoká škola, Fakulta práva
Ústav medzinárodného a európskeho práva
Tomášikova 20, 821 02 Bratislava
simona.kocisova@paneurouni.com

Východiská legislatívnej prevencie počítačovej kriminality

Eva Kresl

Abstrakt:
Autorka príspevku predkladá základné pojmy, definície, princípy, dokumenty, založené inštitúcie a aktivity predstavujúce východiská legislatívnej prevencie počítačovej kriminality v EÚ a na Slovensku. Uvedené pojmy, definície a princípy približujú vlastný predmet počítačovej kriminality. Prehľad dokumentov, inštitúcií a rozvinutých aktivít charakterizuje súčasné štádium budovania legislatívnej prevencie počítačovej kriminality v EÚ a na Slovensku.
Kľúčové slová:
Počítačová kriminalita, počítačové pirátstvo, informačná bezpečnosť, kybernetická bezpečnosť, digitálny priestor, internet, informačné technológie, informačná spoločnosť, hacker, Občiansky zákonník, Trestné právo, Zákon o priestupkoch, bezpečnostné povedomie, Koncepcia kybernetickej bezpečnosti Slovenskej republiky

Abstract:
Theauthor of thepaperpresentsbasicconcepts, definitions, principles, documents, institutions and activitiesthat are thebasis of thelegislativeprevention of cybercrime in the EU and Slovakia. Theseterms, definitions and principlesapproximatethesubject of computercrime. Anoverview of documents, institutions and advancedactivitiescharacterizesthecurrentstage of thedevelopment of thelegislativeprevention of cybercrime in the EU and Slovakia.
Key words:
ComputerCrime, ComputerPiracy, InformationSecurity, CyberSecurity, DigitalSpace, Internet, InformationTechnology, Information Society, Hacker, Civil Code, CriminalLaw, InfringementAct, SecurityAwareness, CyberSecurityConcept of the Slovak Republic

Úvod

Počítačové pirátstvo a počítačová kriminalita patria dnes k populárnym a frekventovaným témam u nás. Počul o nich asi každý z nás a niektorí s nimi už majú aj osobnú skúsenosť. Mladí ľudia bežne profitujú z počítačového pirátstva ilegálnym sťahovaním hudby a filmov. Pre zaujímavosť, ale najmä pre názornosť spomenieme, že počítačová kriminalita začala, keď John Drapper po prvý krát zneužil telefónnu sieť AT&T. Zistil, že sieť sa dá odblokovať triviálnym spôsobom a to písknutím do telefónneho slúchadla píšťalkou vydávajúcou tón o frekvencii 2600 Hz. Po tomto úkone sa telefónna ústredňa prepla do servisného režimu a prestala rátať impulzy. Tým sa telefonovanie stalo bezplatným.

Čím sa odlišuje počítačové pirátstvo od počítačovej kriminality? Na prvý pohľad sa môže zdať, že ide o synonymá a obidva pojmy sa prakticky prekrývajú. Z hľadiska legislatívy to však nie je pravda, pretože počítačová kriminalita v slovenskom právnom poriadku je obligatórne viazaná na pojem trestný čin, definovaný v ustanoveniach § 8 Trestného zákona (ďalej len „TZ“): „Trestný čin je protiprávny čin, ktorého znaky sú uvedené v tomto zákone, ak tento zákon neustanovuje inak.“

Európsky dohovor počítačovú kriminalitu vymedzuje veľmi široko (počítačová kriminalita v širšom zmysle), keď sem zahŕňa aj priestupky ako protiprávne konania podľa ustanovení Zákona o priestupkoch.

Okrem toho medzi počítačovú kriminalitu v širšom zmysle zaraďujeme aj protispoločenské konania, ktoré v zmysle ustanovení § 39 Občianskeho zákonníka (ďalej len „OZ“) sú „konaním proti dobrým mravom“ (nemorálnym konaním), typické pre počítačové pirátstvo.

Napokon sem patria protiprávne konania podľa občianskeho práva, ktorými sú civilné delikty (spôsobenie škody napr. menej závažným porušením licenčnej zmluvy) podľa ustanovení § 420 OZ a nasl. o zodpovednosti za škodu a civilné kvázidelikty (prípady bezdôvodného obohatenia) podľa ustanovení § 451 OZ a nasl. o zodpovednosti za bezdôvodné obohatenie.

Slovenský právny poriadok neprebral vyššie citovanú definíciu počítačovej kriminality do trestného zákona, preto slovenské trestné právo postihuje len najzávažnejšie formy pirátstva (počítačové trestné činy). Slovenský trestný zákon nepozná termín počítačová kriminalita, ale veda trestného práva, kriminológia a kriminalistika ponúkajú definíciu počítačovej kriminality. Do počítačovej kriminality patrí akékoľvek protiprávne konanie spáchané prostredníctvom počítača, počítačových systémov alebo počítačových sietí (počítač ako prostriedok na spáchanie trestného činu) alebo protiprávne konanie smerujúce proti počítaču, počítačovým systémom alebo proti spracúvaným dátam (počítač ako hmotný predmet útoku).

Pojmy definície a princípy legislatívnej prevencie počítačovej kriminality

Pre spresnenie vlastného predmetu počítačovej kriminality a pre istejšie orientovanie sa v ňom uvedieme vybrané základné pojmy, definície a princípy, ktoré sa v tejto oblasti bežne používajú. Z technologickej stránky problematiky uvedieme len najnutnejšie minimum odborných pojmov a definícií.

Informačná spoločnosť (niektorí odborníci dávajú prednosť termínu informatická spoločnosť) je spoločnosť, kde práca s informáciami a údajmi je každodennou záležitosťou. Na prácu s informáciami sa používajú rôzne informačné a komunikačné technológie (IKT).

Počítačová kriminalita je relatívne novým druhom závažnej trestnej činnosti. Od klasickej kriminality sa odlišuje celým radom osobitných charakteristík a zvláštností. Trestný čin môže byť spáchaný v anonymite na diaľku, sprostredkovane a to všetko v priebehu niekoľkých sekúnd bez toho, aby poškodený zaregistroval spáchanie takéhoto trestného činu a niekedy sa o tom vôbec dozvedel. Internet, anonymita a nedostatočná legislatíva, robia z počítačovej kriminality mocný nástroj na páchanie domácich a medzinárodných trestných činov veľakrát závažného charakteru s priamym dopadom na ekonomiku krajiny a jej bezpečnosť.

Druhy počítačovej kriminality:

- útok na počítač, program, údaje, komunikačné zariadenie,
- neoprávnené užívanie počítača alebo komunikačného zariadenia,
- krádež počítača, programu, údajov, komunikačného zariadenia
- zmena v programoch a údajoch,
- podvody páchané v súvislosti s výpočtovou technikou.

Malware je škodlivý/zhubný program, všeobecné označenie škodlivého softvéru. Patria sem napríklad vírusy, trójske kone, spyware a adware.

Vírus je programový kód, ktorý sa bez vedomia užívateľa samovoľne replikuje (teda množí a rozširuje). Tento kód je pre užívateľa obvykle skrytý.

Antivírusový softvér je program, ktorého cieľom je identifikovať a eliminovať počítačové vírusy.

Prienik do počítačového systému je druh počítačovej kriminality a znamená útok na počítačový systém. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva hacker.

Hacker je počítačový expert, dobrý programátor, hľadajúci bezpečnostné diery v systémoch, za účelom zlepšenia ich bezpečnosti. O nájdených chybách a nedostatkoch informuje autorov programov, správcov systému aj verejnosť.

Cracker má technické schopnosti ako hacker, ktoré ale používa vo svoj prospech, väčšinou ilegálne. Patria sem aj takzvaní softvéroví, filmoví a hudobní piráti, lovci čísiel kreditných kariet a iní. Najčastejším motívom je pre nich uznanie v komunite a peniaze. Jedná sa o plánovanú a premyslenú činnosť.

Sociálne riziká informačných technológií sú negatívne vplyvy, ktoré nepriaznivo účinkujú na sociálny vývoj jednotlivca, na formovanie vzťahov jednotlivca k spoločnosti a vzťahy medzi jednotlivcami navzájom. Patria medzi najmä:

- strata súkromia na webe
- reklama na webových stránkach
- jednoduchý prístup k nevhodným informáciám
- dôveryhodnosť, pravdivosť informácií na webe, anonymita na webe
- kyberšikanovanie
- hry a gambling
- nevyžiadané e-maily – spamy, poplašné správy (hoax).

Digitálny priestor je súhrn:

- informačných a komunikačných technológií, vrátane ich programového vybavenia a informačných systémov a sietí
- informácií, vrátane údajov, ktoré sa prenášajú, spracovávajú alebo uchovávajú prostredníctvom informačných a komunikačných technológií alebo opisujú štruktúru, konfiguráciu a činnosť informačných a komunikačných technológií
- procesov, ktoré prebiehajú v rámci informačných a komunikačných technológií
- podpornej infraštruktúry zabezpečujúcej činnosť informačných a
- komunikačných technológií, vrátane elektronických komunikačných sietí
- vzťahov medzi údajmi a informáciami a pravidiel upravujúcich tieto vzťahy.

Digitálny priestor štátu alebo organizácie je časť digitálneho priestoru v ich pôsobnosti, pričom táto organizácia alebo štát majú právo určovať pravidlá a spôsob fungovania príslušnej časti digitálneho priestoru a majú prostriedky na presadzovanie týchto pravidiel.

Digitálny priestor Slovenskej republiky je časť digitálneho priestoru v pôsobnosti Slovenskej republiky, na ktorý sa vzťahujú všeobecné právne predpisy Slovenskej republiky.

Kybernetický priestor je časť digitálneho priestoru pozostávajúca zo všetkých informačných systémov prepojených na globálnej dátovej úrovni, pričom jej základom je Internet; informačný systém alebo prvok v izolovanom priestore nie je súčasťou kybernetického priestoru.

Bezpečnostné úrovne informácie na základe vážnosti dopadu alebo ujmy sú:

1. nepodstatná
2. nízka
3. stredná
4. vysoká.

Informačná bezpečnosť je podľa medzinárodného štandardu ISO/IEC 270011 (prijatého Národnou stratégiou pre informačnú bezpečnosť) ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je zaistenie kontinuity obchodných procesov, minimalizácia strát a maximalizácia návratnosti investícií. Základné bezpečnostné požiadavky na ochranu informácií sú ich dostupnosť, dôvernosť, autentickosť a integrita.

Kybernetická bezpečnosť (podľa Koncepcie kybernetickej bezpečnosti SR) je jedným z určujúcich prvkov bezpečnostného prostredia Slovenskej republiky a podsystémom národnej bezpečnosti. Na úrovni štátu, predstavuje systém nepretržitého a plánovitého zvyšovania politického, právneho, hospodárskeho, bezpečnostného, obranného a vzdelanostného povedomia, ktorý zahŕňa aj zvyšovanie účinnosti prijatých a aplikovaných technicko-organizačných opatrení riadenia rizík v kybernetickom priestore za účelom jeho transformácie do dôveryhodného prostredia, ktoré umožnia bezpečné fungovanie spoločenských ahospodárskych procesov pri zaistení akceptovateľnej úrovne rizík v kybernetickom priestore.Slovenská republika ešte nemá formálne ustálenú terminológiu v oblasti kybernetickej bezpečnosti. Slovo kybernetický, ako aj jeho ďalšie gramatické tvary sa nevyskytuje v žiadnom všeobecne záväznom právnom predpise, ani v terminologických slovníkoch.

Princípy informačnej bezpečnosti

Princípy informačnej bezpečnosti sú uvedené v smerniciach Guidelines for the Security of Information Systems, vydané OECD v júli 2002. Zdôrazňujú, že je potrebné podporovať vývoj bezpečnostnej kultúry, t.j. sústrediť sa na bezpečnosť pri vývoji informačných systémov a sietí a osvojiť si nové spôsoby myslenia a správania pri používaní informačných systémov a sietí. Postulujú 9 základných princípov, z ktorých je potrebné vychádzať pri riešení informačnej bezpečnosti systémov:

a) **Bezpečnostné povedomie** (awareness) Všetci zúčastnení by si mali uvedomovaťpotrebu informačnej bezpečnosti informačných systémov a sietí, ako aj toho čo môžuspraviť na rozšírenie bezpečnosti.
b) **Zodpovednosť** (responsibility) Všetci zúčastnení sú zodpovední (primerane úlohám,ktoré v systéme plnia) za bezpečnosť informačných systémov a sietí.
c) **Reakcia** (response) Zúčastnení by mali konať rýchlo a koordinovane aby zabránilivzniku bezpečnostného incidentu, včas ho odhalili a adekvátne naň odpovedali.
d) **Etika** (ethics) Zúčasnení by mali rešpektovať legitímne záujmy ostatných.
e) **Demokracia** (democracy) Bezpečnosť informačných systémov a sietí by mala byťkompatibilná s podstatnými hodnotami demokratickej spoločnosti, t.j. musí byťzachovaná sloboda myslenia, výmeny ideí, voľného toku informácií, dôvernosti informácie a ochrany osobných údajov.
f) **Odhad rizík** (risk assessment) Zúčastnení by mali robiť analýzu rizík, abyidentifikovali hrozby a ich možné dopady na systém a dokázali prijať riešeniaadekvátne zisteným rizikám.
g) **Návrh a implementácia bezpečnosti** (Security design and implementation)Zúčastnení by mali chápať bezpečnosť ako podstatný prvok informačných systémova sietí; t.j. bezpečnosť systému je potrebné zohľadniť už vo fáze jeho návrhu, vybrať a implementovať vhodné bezpečnostné opatrenia, zodpovedajúce hodnotám, ktorémajú chrániť.
h) **Riadenie informačnej bezpečnosti** (Security management) Zúčastnení by maliuplatňovať komplexný prístup k riadeniu informačnej bezpečnosti. Riadenieinformačnej bezpečnosti by sa malo zakladať na analýze rizík, malo by byť dynamickéa zahŕňať všetky úrovne aktivít ľudí pôsobiacich v systéme a všetky aspekty ichoperácií.
i) **Prehodnocovanie** (Reassessment) Zúčastnení by mali prehodnocovať bezpečnosťinformačných systémov a sietí a robiť nevyhnutné modifikácie bezpečnostnýchpolitík, praktík, opatrení a procedúr, aby zodpovedali vyvíjajúcim sa a vznikajúcimnovým bezpečnostným hrozbám.

Dokumenty, inštitúcie a aktivity legislatívnej prevencie počítačovej kriminality

Súčasný stav legislatívy a súvisiacich dokumentov v oblasti informačnej resp. kybernetickej bezpečnosti v SR prehľadne opísal a charakterizoval Ing. Ján Hochmann Data Centrum – Ministerstvo financií SR, vo svojej prezentácii Kybernetická bezpečnosť a štát, na konferencii Kybernetická bezpečnosť & ochrana osobných údajov (24. október 2017).

Z jeho chronológie rozvoja IB/KB v SR od roku 1992 tu uvediem nasledovné kľúčové míľniky:

- Vznik s.r.o. ESET (1992), ktorá je dnes svetovým lídrom v riešení návrhov proti počítačovým vírom, v r. 1999 bola založená spoločnosť ISACA Slovensko ako súčasť profesijnej organizácie ISACA, ktorá je lídrom v oblasti riadenia, bezpečnosti a kontroly informačných technológií a začínajú vznikať malé konzultačné spoločnosti, IKT firmy, pripojenie SR k EÚ
- Slovensko začína plniť odporúčania EÚ, metodiky, transpozícia smerníc
- Nová legislatíva (zákon o ochrane osobných údajov (2002), zákon o elektronickom podpise (2002), zákon o informačnom systéme verejnej správy ISVS (2006), začína elektronický obchod
- eGovernment - Cestovná mapa, Akčný plán (2004), Eurofondy (2005-2006),
- Tvorba PKI (PublicKeyInfrastructure) (NBÚ – národná autorita),
- Zák. č. 275/2006 Z.z. o ISVS (zabezpečenie kontinuity, zabezpečenie a ochrana ISVS, štandardy (ISO 27000), ...)
- EÚ fondy (OPIS (operačný program informatizácia spoločnosti) 2007 – 2013)
- Medzinárodná spolupráca - aktívne členstvo v ENISA (EuropeanNetwork and InformationSecurityAgency), OECD, ...
- Národná stratégia pre informačnú bezpečnosť v Slovenskej republike (NSIB), schválená uznesením vlády Slovenskej republiky č. 570/2008;
- Koncepcia šifrovej ochrany informácií, schválená uznes. vlády SR č. 771/2008;
- Návrh systému vzdelávania v oblasti IB/KB v Slovenskej republike (ďalej len „Stratégia vzdelávania v IB“), schválený uznes. vlády SR č. 391/2009;
- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – CSIRT.SK (ComputerSecurity Incident Response Team) schválený uznes. vlády SR č. 479/2009
- Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválený uznes. vlády SR č. 46/2010
- Legislatívny zámer zákona o IB, schválený uznes. vlády SR č. 136/2010
- Stratégia Európskej únie pre kybernetickú bezpečnosť: Otvorený, bezpečný a chránený kybernetický priestor, schválená EK 7. 2. 2013
- Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie rady 2005/222/SVV
- Správy o plnení úloh z Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a Akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády Slovenskej republiky
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, (uznes. vlády SR č. 328/2015)
- Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky (uznes. vlády SR č. 334/2015)
- Prijatie zákona č. 339/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších

predpisov, ktorým bol NBÚ ustanovený ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť

- Zriadenie Komisie pre kybernetickú bezpečnosť, ktorej štatút vzala na vedomie vláda Slovenskej republiky v roku 2015, (č. m. UV-33740/2015)
- Prijatie zákona č. 346/2015 Z. z., ktorým sa mení a dopĺňa zákon č.110/2004 Z. z o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z, ktorým boli zriadené Výbor pre energetickú bezpečnosť a Výbor pre kybernetickú bezpečnosť Bezpečnostnej rady Slovenskej republiky
- Akčný plán ku Koncepcii KB na roky 2015-2020 (uznes. Vlády č. 93/2016.)

Z kľúčových dokumentov EU uvedieme:

Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SW

Smernica plne rešpektuje ľudské práva a základné slobody a uznáva zásady Charty základných práv EÚ, ochranu osobných údajov, práva na súkromie, slobody prejavu a práva na informácie, práva na spravodlivý proces, prezumpciu neviny a práva na obhajobu a zásad primeranosti trestných činov.

Sleduje aproximáciu trestného práva členských štátov v oblasti útokov na informačné systémy, ustanovenie minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií a zlepšenie spolupráce medzi príslušnými orgánmi v členských štátoch a orgánoch EÚ (polícia, špeciálne zložky presadzovania práva, Eurojust, Europol, Európske centrum pre počítačovú kriminalitu, ENISA a pod.)

Smernica EP a Rady č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov

Stanovuje povinnosti členských štátov ako: prijať stratégiu BSI a určiť vnútroštátny orgán príslušný pre BSI disponujúci dostatočnými finančnými a ľudskými zdrojmi, na účely predchádzania rizikám a incidentom BSI, ich riešenia a reagovania na ne; vytvoriť mechanizmus spolupráce medzi členskými štátmi a Komisiou na účely vzájomného včasného varovania o rizikách a incidentoch prostredníctvom chránenej infraštruktúry, a na účely spolupráce a organizácie pravidelných partnerských hodnotení; prevádzkovatelia mimoriadne dôležitých infraštruktúr v niektorých odvetviach (energetika, finančné služby, doprava, zdravotníctvo), aktéri sprístupňovania služieb informačnej spoločnosti (osobitne: platformy elektronického obchodu založené na tzv. appstores, platby cez internet, cloudcomputing, internetové vyhľadávače, sociálne siete) a orgány verejnej správy musia prijať postupy riadenia rizík a podávať správy o významných bezpečnostných incidentoch na ich hlavných službách.

Európsky obranný akčný plán dokument (COM 2016) 950 vydaný Európskou komisiou dňa 30.11.2016 v Bruseli.

Inštitúty SR pre ochranu počítačovej bezpečnosti

Národný bezpečnostný úrad (NBÚ) - je ústredný orgán štátnej správy Slovenskej republiky pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby.

Komisia pre kybernetickú bezpečnosť je stály odborný poradný orgán riaditeľa Národného bezpečnostného úradu pre uplatňovanie štátnej politiky v oblasti kybernetickej bezpečnosti v Slovenskej republike.

Koordináciu a riadenie aktivít pre zaistenie počítačovej bezpečnosti vykonáva:

ÚPV SR pre investície a informatizáciu /Sekcia riadenia informatizácie zabezpečuje v oblasti informatizácie spoločnosti centrálne riadenie informatizácie spoločnosti

a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní finančných zdrojov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti. Jeho činnosť upravuje Zák. č. 275/2006 Z. z. o ISVS.

MV SRvykonáva v zmysle Zák. č. 45/2011 Z.z. o kritickej infraštruktúre štátnu správu na úseku kritickej infraštruktúry spolu s Vládou SR a MH SR.

Výkonnými zložkami v oblasti kritickej infraštruktúry sú odpovedajúce sektory MH SR, MDV SR, MF SR, MZ SR, MŽP SR.

Špecifické postavenie pri ochrane počítačovej bezpečnosti má MO SR upravené zák. č. 319/2002 Z.z. o obrane SR, zák. č. 321/2002 Z.z. o ozbrojených silách SR a unesením Vlády SR č.120/2007 - Koncepcia kritickej infraštruktúry v SR a spôsob jej ochrany a obrany.

Aktivity vytýčené na splnenie Akčného plánu plnenia úloh ku Koncepcii kybernetickej bezpečnosti na roky 2015-2020

Uznesením vlády SR č. 93/2016 boli aktivity na splnenie Akčného plánu plnenia úloh ku Koncepcii kybernetickej bezpečnosti na roky 2015-2020 rozčlenené do nasledovných oblastí:

1. Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
2. Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
3. Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.
4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti.
5. Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
6. Aktívna medzinárodná spolupráca.
7. Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Národný bezpečnostný úrad SR mal uznesením vlády Slovenskej republiky č. 328 zo dňa 17. júna 2015 uloženú úlohu do konca februára 2016 pripraviť a predložiť na rokovanie vlády Slovenskej republiky návrh zákona o kybernetickej bezpečnosti, v rámci ktorého budú kvantifikované relevantné vplyvy vrátane finančných dopadov.

Záver

Odborníci na ochranu počítačovej bezpečnosti charakterizujú súčasný stav legislatívneho zabezpečenia počítačovej bezpečnosti u nás nasledovnými nedostatkami:

- právna ochrana informácií je roztrieštená do viacerých právnych predpisov, rovnaké dáta môžu by chránené rôznymi predpismi
- neexistuje žiadna špecifická právna úprava
- aplikovanie právnych predpisov do praxe bez ich ďalších nepriamych úprav sa vykonáva komplikovane
- nevhodné a nekorektné postupy - cielená účelovosť právnych úprav
- neznalosť vecnej problematiky pri tvorbe právnych predpisov a materiálov
- nekompaktná a chybná terminológia
- nahrádzanie legislatívnych nedostatkov zmluvnou cestou (úskalia, účelovosť).

Za jeden z hlavných problémov považujú odborníci nejasnosti ohľadom vymedzenia pojmu „informačná bezpečnosť“, „počítačová bezpečnosť“ a „kybernetická bezpečnosť“, ktoré sa až do roku 2015 používali v oficiálnych dokumentoch (stratégie, zákony, či ďalšie nariadenia) bez jednoznačnej definície.

Pojem „kybernetická bezpečnosť“ sa začal frekventovanejšie objavovať v odbornej diskusii intenzívnejšie iba nedávno, najmä z dôvodu preberania a ďalšieho šírenia zahraničných odborných článkov a dokumentov medzi odbornou aj laickou verejnosťou. Ale tiež v súvislosti s dianím na európskej úrovni, ktoré rámcuje najmä zverejnenie Stratégie pre oblasť kybernetickej bezpečnosti EÚ: "otvorený, bezpečný a chránený kybernetický priestor" a návrhu Smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v celej Únii Európskou komisiou vo februári 2013.2 Istá diskrepancia vo vnímaní pojmov však naďalej pretrváva. Hoci existuje zhoda, že informačná bezpečnosť je vedecko-technický odbor a kybernetická bezpečnosť je len jednou z jeho riešených tém, zároveň tiež existuje istá tendencia zamieňania alebo prelínania týchto pojmov. Je preto pozitívne, že so snahou o terminologické rozlíšenie prišla aj nová Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schválenej Vládou SR v septembri 2015. Hoci je schválenie prvej koncepcie kybernetickej bezpečnosti úspechom, kritici jej vyčítajú prílišnú vágnosť, najmä v častiach, kde definuje strategické ciele a opatrenia.

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

Pravdou je, že Slovensko dodnes nemá ucelený a komplexný systém kybernetickej bezpečnosti na národnej/strategickej úrovni v podobe zastrešujúceho zákona, ktorý by upravoval všetky súvisiace oblasti. Napriek tomu, že v priebehu niekoľkých posledných rokov prebiehali práce na zákone o informačnej bezpečnosti - Návrh zákona o kybernetickej bezpečnosti

predložil NBÚ do vlády: 28.02.2016; 30.09.2016; 30.12.2016; 30.09.2017, ale dodnes nie je vypracovaný do finálnej podoby a schválený. V platnosti je tak jedine vládou schválený Legislatívny zámer zákona o informačnej bezpečnosti z roku 2010.

V poslednom desaťročí tiež možno badať postupné zbavovanie sa zodpovednosti štátnej sféry za kybernetickú bezpečnosť a realizovanie politiky len prostredníctvom prenájmu služieb od súkromného sektora. To zapríčinilo pokles snáh o budovanie vlastných kapacít a hľadanie komplexných riešení, ktoré by štátu umožnili schopnosť adekvátnej reakcie na dnešné aj budúce výzvy. Taktiež neexistuje zhoda na tom, ktoré úlohy by mali byť v zodpovednosti štátu, ktoré by mali byť predmetom spolupráce medzi verejným a súkromným sektorom a ktoré oblasti by mali zostať výlučne v súkromnom sektore.

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

Faktom, ktorý podporujeme zostáva, že v prípade snahy štátu o vytvorenie efektívneho systému kybernetickej či informačnej bezpečnosti, ale aj pri realizácii jednotlivých projektov, by to mal byť práve štát, ktorý by mal proaktívne oslovovať predstaviteľov súkromného sektora. Proaktívny prístup verejného sektora a vytvorenie podmienok pre rovnocenné

partnerstvo oboch strán by bol osobitne prínosný pri príprave strategických dokumentov, či legislatívnych opatrení. Táto spolupráca by mala byť nadväzovaná už v procese prípravy a nie až pri medzirezortnom (verejnom) pripomienkovom konaní.

Zoznam použitej literatúry:

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020,

HOCHMANN, J. *Kybernetická bezpečnosť a štát, referát na konferencii Kybernetická bezpečnosť & ochrana osobných údajov,* DataCentrum – Ministerstvo financií SR, október 2017

http://europa.eu/rapid/press-release_IP-14-129_sk.htm

http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf

http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf

http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Uznesenie-15430?prefixFile=u_

https://vyskoc.blog.sme.sk/c/144762/Rozoberme-si-navrh-Narodnej-strategie-pre-informacnu-bezpecnost.html

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020,

MAJER, M., NAĎ, J., MASARIKOVÁ, M. *Slovensko vo vzťahu k novej realite kybernetickej bezpečnosti,* Slovak SecurityPolicyInstitute, ISBN 978-80-972228-0-2 jan. 2016

Prvý rok Európskeho centra boja proti počítačovej kriminalite, tlačová správa, EURÓPSKA KOMISIA, Brusel 10. februára 2014,

Stratégia prevencie kriminality a inej protispoločenskej činnosti v Slovenskej republike na roky 2012 – 2015, Ministerstvo vnútra Slovenskej republiky, Číslo: KM-OPVA1-2011/005982 Materiál na rokovanie vlády Slovenskej republiky

STRÉMY, T. *Počítačová kriminalita.* In: DIANIŠKA, G. a kol. Kriminológia. Plzeň: Aleš Čeněk s.r.o., 2011

Úvod do počítačového pirátstva a počítačovej kriminality,

https://www.pravnenoviny.sk/analyzy/kto-je-kto-uvod-do-pocitacoveho-piratstva-pocitacovej-kriminality-na-slovensku

UZNESENIE VLÁDY SLOVENSKEJ REPUBLIKY č. 93 z 2. marca 2016 k návrhu Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020,

VYSKOČ, J. *Rozoberme si návrh Národnej stratégie pre informačnú bezpečnosť* 24.4.2008,

Kontaktné údaje:

JUDr. Eva Kresl
sudkyňa OS BA I
evakresl@gmail.com

Počítačové údaje v trestnom konaní

Remig Kubička, Oliver Kubička

Abstrakt*:*
Príspevok sa zaoberá vybranými a z pohľadu autorov a právnej praxe problematickými otázkami súvisiacimi s trestno-procesným postupom pri zisťovaní, zabezpečovaní a zaisťovaní počítačových údajov. Autori analyzujú názory na danú problematiku vyjadrené v rámci judikatúry a odbornej literatúry. Vysvetľujú technickú charakteristiku jednotlivých zariadení, v nadväznosti na ktorú zaujímajú stanovisko k obsahu pojmu počítačové údaje v zmysle § 90 Tr. por. prezentovanému v rámci judikatúry a odbornej literatúry.
Kľúčové slová*:*
Počítačové údaje, počítačový systém, mobilný telefón, emailová komunikácia.

Abstract*:*
This contribution deals with selected and from author's and law practice view problematic questions relative to criminally-trial procedure at finding-out, ensuring and locking computer informations. Authors analizes opinions on given issues in the case-law and professional literature. They explain the technical characteristics of the individual devices and gives their opinion on the concept of computer data in the sense of § 90 Tr. por. presented in the context of case law and professional literature.
Key words*:*
Computer data, computer system, mobile phone, email communication.

Úvod

Vzhľadom na technický rozvoj a využívanie jeho výsledkov v súvislosti s páchaním trestnej činnosti, počítačové údaje predstavujú pre orgány činné v trestnom konaní a súdy cenný zdroj dôkazov. Páchanie trestnej činnosti prostredníctvom počítačových systémov, prenášanie informácií o pripravovanej, páchanej alebo už spáchanej trestnej činnosti prostredníctvom nich a ukladanie informácií dôležitých pre trestné konanie prostredníctvom počítačových systémov, si vyžadujú, aby tieto orgány mali právom upravený dosah na počítačové údaje, či už s cieľom získania dôkazov alebo odstránenia počítačových údajov so závadným obsahom z počítačového systému. Na takúto potrebu a technický pokrok musela reagovať trestno-právna úprava tak na medzinárodnej, ako aj na vnútroštátnej úrovni. Výsledkom bolo doplnenie trestno-procesných ustanovení do nášho právneho poriadku, ktorých výklad v niektorých prípadoch nie je jednotný. Cieľom predkladaného príspevku je poukázať na niektoré prípady súvisiace so zisťovaním, zabezpečovaním a zaisťovaním počítačových údajov, ktoré možno hodnotiť ako problematické vzhľadom na názorové nezhody v právnej praxi, prezentovať názory na ich riešenie vyjadrené v rámci judikatúry a odbornej literatúry a zaujať odôvodnené stanovisko zo strany autorov na vybrané sporné otázky.

Údaje uložené v mobilných telefónoch a obdobných zariadeniach

V aplikačnej praxi orgánov činných v trestnom konaní existovali pochybnosti o tom, či postup v zmysle § 90 zákona č. 301/2005 Z. z. Trestný poriadok (ďalej tiež „Tr. por.“) je možné aplikovať aj vo vzťahu k údajom uloženým v mobilných telefónoch. Možno však konštatovať, že v rámci postupu orgánov činných v trestnom konaní prevládol názor, že počítačové údaje uložené v tzv. smartfónoch predstavujú počítačové údaje v zmysle § 90 Tr. por. Smartfón možno definovať ako „ mobilný telefón s operačným systémom. Najpoužívanejšími systémami sú Google Android, Apple iOS a Microsoft Windows, ktoré umožňujú, aby bol prístroj vybavený bohatou základnou výbavou aplikácií (funkcií) a neskôr rozšírený o ďalšie. Existujú aj operačné systémy, ktoré sa už takmer nepoužívajú – Symbian alebo PalmOS. Smartfón slúži predovšetkým na komunikáciu, GPS, prístup k internetu cez mobilné a WiFi siete a používanie

rôznych ďalších aplikácií, ktoré sa do smartfónu dajú inštalovať cez Internet priamo z mobilu, na hry, prácu, mobilnú kanceláriu a zábavu.“[1]

K uvedenej problematike zaujala stanovisko taktiež judikatúra. Toto stanovisko sa však odlišuje od dovtedy už ustálenej praxe orgánov činných v trestnom konaní.

Podľa R 47/2017 „napriek určitým spoločným technickým parametrom počítača a mobilného telefónu údaje uložené v mobilnom telefóne nie sú počítačovými údajmi v zmysle úpravy § 90 Trestného poriadku.“[2] Z obsahu odôvodnenia judikátu R 47/2017 (Uznesenie Najvyššieho súdu Slovenskej republiky z 23. marca 2017, sp. zn. 5 Tdo 7/2017) nie sú zrejmé úvahy, ktoré viedli k sformulovaniu citovanej právnej vety, podľa ktorej údaje uložené v mobilnom telefóne nie sú počítačovými údajmi v zmysle § 90 Tr. por.

V súvislosti s danou problematikou možno poukázať aj na časť odôvodnenia rozsudku Najvyššieho súdu SR z 26. novembra 2014, sp. zn. 2To 9/2014 podľa ktorej „námietka, že na znalecké preskúmanie mobilných telefónov bol vzhľadom k ich operačnému systému potrebný príkaz na uchovanie a vydanie počítačových údajov podľa § 90 Tr. por., a teda nepostačovalo vydanie, resp. odňatie veci podľa § 89, § 91 Tr. por., rovnako nie je dôvodná, ako na to poukázal aj ŠTS (Špecializovaný trestný súd - pozn. autorov). Možno dodať, že napriek niektorým podobným alebo zhodným technickým komponentom a spôsobu prevádzky, mobilný telefón nemožno stotožniť s počítačom a tento rozdiel sa prejavuje i pri ponuke a predaji príslušných zariadení ako rozdielnych druhov tovaru.“[3] Na základe odôvodnenia rozsudku z 26. novembra 2014, sp. zn. 2To 9/2014 možno taktiež odvodiť záver, že vo veci rozhodujúci senát Najvyššieho súdu SR údaje uložené prostredníctvom mobilného telefónu nepovažuje za údaje uložené prostredníctvom počítačového systému v zmysle § 90 Tr. por. Svoj názor senát odôvodňuje tým, že rozdiel medzi mobilným telefónom a počítačom vyplýva taktiež z ich označovania ako rozdielnych druhov tovaru. Iné konkrétne úvahy, na základe ktorých by bolo možné identifikovať rozdiel medzi údajmi uloženými v počítači a mobilnom telefóne, nie sú z odôvodnenia citovaného rozsudku Najvyššieho súdu SR identifikovateľné.

Podľa § 90 ods. 1 Tr. por., ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby a) také údaje uchovali a udržiavali v celistvosti, b) umožnili vyhotovenie a ponechanie si kópie takých údajov, c) znemožnili prístup k takým údajom, d) také údaje odstránili z počítačového systému, e) také údaje vydali na účely trestného konania.

Právna úprava inštitútu uchovania a vydania počítačových údajov obsiahnutá v § 90 Tr. por. „reaguje na dohovor Rady Európy o počítačovej kriminalite, ktorý bol prijatý členskými štátmi Rady Európy dňa 23.11.2001 v Budapešti.“[4] Vzhľadom na nadväznosť právnej úpravy inštitútu uchovania a vydania počítačových údajov na dohovor Rady Európy o počítačovej kriminalite, možno opodstatnene pri výklade § 90 Tr. por. použiť definície pojmov uvedené v tomto dohovore. Preto pri zodpovedaní otázky, či údaje uložené prostredníctvom mobilných telefónov predstavujú počítačové údaje, ktoré boli uložené prostredníctvom počítačového systému a teda, či vo vzťahu k nim môžeme aplikovať postup podľa § 90 Tr. por., je dôvodné vychádzať z výkladu pojmov uvedených v dohovore Rady Európy o počítačovej kriminalite a porovnať technickú charakteristiku mobilného telefónu a údajov uložených prostredníctvom mobilného telefónu s definíciou príslušných pojmov v dohovore.

[1] Dostupné na: https://sk.wikipedia.org/wiki/Smartf%C3%B3n
[2] R 47/2017
[3] rozsudok Najvyššieho súdu SR z 26. novembra 2014, sp. zn. 2To 9/2014
[4] Dôvodová správa k zákonu č. 301/2005 Z. z. Trestný poriadok

Podľa čl. 1 písm. a) dohovoru Rady Európy o počítačovej kriminalite „počítačový systém“ znamená zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu.

Podľa čl. 1 písm. b) dohovoru Rady Európy o počítačovej kriminalite „počítačové údaje“ znamenajú záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť.

Mobilný telefón predstavuje zariadenie obsahujúce okrem iného:

- základnú dosku
- procesor
- pamäť
- klávesnicu (hardvérovú alebo klávesnicu na displeji)
- displej
- vysielač/prijímač údajov.

Program v informatike možno definovať ako „úplný zoznam príkazov alebo inštrukcií na riešenie úlohy na počítači“.[5]

Mobilný telefón predstavuje zariadenie vykonávajúce automatizované spracovávanie údajov na základe programu, teda zoznamu príkazov alebo inštrukcií slúžiacich na riešenie úloh na tomto zariadení. Takýmto programom využívaným v mobilnom telefóne môže byť napríklad textový editor, program umožňujúci ukladanie a triedenie kontaktov do skupín, emailov klient, atď.

V nadväznosti na vyššie uvedené zastávame názor, že mobilný telefón spĺňa pojmové znaky počítačového systému v zmysle čl. 1 písm. a) dohovoru Rady Európy o počítačovej kriminalite, nakoľko predstavuje zariadenie vykonávajúce automatizované spracovávanie údajov na základe programu. V nadväznosti na to a berúc do úvahy čl. 1 písm. b) dohovoru Rady Európy o počítačovej kriminalite, údaje uložené prostredníctvom mobilného telefónu, predstavujúce záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme (teda vhodná aj na spracovanie v samotnom mobilnom telefóne), považujeme za počítačové údaje uložené prostredníctvom počítačového systému, na ktoré možno aplikovať postup podľa § 90 Tr. por.

Pokiaľ na objasnenie skutočností dôležitých pre trestné konanie je nevyhnutné uchovanie kamerového záznamu vyhotoveného mobilným telefónom a uloženého v pamäti mobilného telefónu, telefónneho zoznamu uloženého v mobilnom telefóne, obsahu emailovej správy uloženej v mobilnom telefóne, atď., v nadväznosti na výsledky vyššie uvedenej analýzy hodnotíme ako zákonný príkaz adresovaný osobe, v ktorej držbe sa nachádza mobilný telefón obsahujúci tieto údaje, aby napríklad v zmysle § 90 ods. 1 písm. b) Tr. por. umožnila vyhotovenie a ponechanie si kópie takých údajov alebo v zmysle § 90 ods. 1 písm. e) Tr. por. také údaje vydala na účely trestného konania.

S ohľadom na definíciu pojmov počítačový systém a počítačové údaje v dohovore Rady Európy o počítačovej kriminalite, v nadväznosti na ktorý bol zavedený do nášho právneho poriadku inštitút uchovania a vydania počítačových údajov (§ 90 Tr. por.) a pri zohľadnení okolnosti, že pre technický charakter tohto zariadenia je mobilný telefón podraditeľný pod pojem počítačový systém a údaje uložené prostredníctvom mobilného telefónu pod pojem počítačové údaje tak, ako sú tieto pojmy definované v dohovore, sa nestotožňujeme s názorom, v zmysle ktorého pri výklade § 90 ods. 1 Tr. por. argumentom pre odmietnutie stotožňovania mobilného telefónu a počítača je tiež ponuka a predaj uvedených zariadení ako rozdielnych druhov tovaru.

[5] Dostupné na: https://sk.wikipedia.org/wiki/Program

Máme tiež za to, že ako argument pre odmietnutie zaraďovania údajov uložených prostredníctvom mobilného telefónu pod § 90 Tr. por. nemôže poslúžiť tvrdenie, že mobilný telefón je určený prioritne na uskutočňovanie telefonických hovorov. Použitie takéhoto argumentu totiž nemá oporu v definícii pojmov uvedených v dohovore Rady Európy o počítačovej kriminalite a znamenalo by negáciu čl. 1 písm. a), písm. b) uvedeného dohovoru.

Pri úvahách, aké údaje možno subsumovať pod pojem počítačové údaje v zmysle § 90 ods. 1 Tr. por., nemožno opomenúť ani ďalšie zariadenia, v súvislosti s ktorými je možné uvažovať o použití niektorého z opatrení vymedzených v § 90 ods. 1 písm. a) – e) Tr. por.

Tablet je počítač, ktorý je celý integrovaný v displeji. Vzhľadom na technický charakter tohto zariadenia máme za to, že tablet spĺňa definičné znaky počítačového systému v zmysle čl. 1 písm. a) dohovoru Rady Európy o počítačovej kriminalite a údaje zaznamenané prostredníctvom tabletu sú podraditeľné pod pojem počítačové údaje v zmysle dohovoru. Údaje uložené prostredníctvom tabletu preto považujeme za spôsobilé byť predmetom príkazu uvedeného v § 90 Tr. por.

Ak by sme akceptovali názor, podľa ktorého údaje uložené v mobilnom telefóne nie sú počítačovými údajmi v zmysle § 90 Tr. por., potom s ohľadom na existenciu ďalších obdobných zariadení (napr. tablet) by bolo nevyhnutné sa vysporiadať s otázkou, či údaje uložené prostredníctvom týchto ďalších zariadení majú charakter počítačových údajov uložených prostredníctvom počítačového systému a stanoviť kritériá umožňujúce vymedziť hranicu medzi údajmi majúcimi charakter počítačových údajov v zmysle § 90 Tr. por. a údajmi, ktoré takýto charakter nemajú. Takéto kritériá však nestanovuje judikatúra prezentujúca názor, podľa ktorého údaje uložené v mobilnom telefóne nie sú počítačovými údajmi v zmysle § 90 Tr. por. Zástancovia názoru, podľa ktorého údaje uložené prostredníctvom mobilných telefónov predstavujú počítačové údaje v zmysle § 90 Tr. por. sa pochopiteľne stanovovaním takýchto kritérií nezaoberajú, nakoľko vzhľadom na argumenty, ktoré ich viedli k takémuto stotožneniu, považujú aj údaje uložené prostredníctvom obdobných zariadení (napr. tablet) za počítačové údaje.

Získavanie počítačových údajov zo zaistených zariadení

Medzi subjektami aplikujúcimi trestné právo neexistuje názorová zhoda na postup pri získavaní údajov zo zariadení (napr. počítačov, mobilných telefónov), ktoré už boli zaistené orgánmi činnými v trestnom konaní, prípadne súdom, napríklad na základe výzvy na vydanie veci podľa § 89 ods. 1 Tr. por. Spornou je odpoveď na otázku, či po zaistení zariadení, v ktorých sú uložené údaje, predstavujúce predmet záujmu orgánov činných v trestnom konaní, prípadne súdov, je potrebné vydať aj príkaz podľa § 90 Tr. por., resp. podľa § 116 Tr. por. na zákonné získanie samotných údajov, ktorých nositeľmi sú tieto zariadenia.

Pre zástancov názoru, podľa ktorého údaje uložené prostredníctvom mobilného telefónu, nemajú charakter počítačových údajov podľa § 90 Tr. por. samozrejme odpadajú úvahy o tom, či údaje zo zaistených mobilných telefónov je potrebné získavať postupom podľa § 90 Tr. por.

Možno konštatovať, že orgány činné v trestnom konaní pri získavaní údajov uložených v zaistených počítačoch a mobilných telefónoch zvykli uplatňovať ešte následný postup podľa § 90 Tr. por.

K uvedenej otázke však zaujala stanovisko judikatúra Najvyššieho súdu SR.

Podľa R 47/2017 „na zabezpečenie informácií z mobilného telefónu, ktorý bol vydaný alebo odňatý ako vec dôležitá pre trestné konanie podľa § 89 a § 91 Trestného poriadku, a to aj pri domovej prehliadke alebo prehliadke iných priestorov alebo pozemku v zmysle § 105 ods. 4 Trestného poriadku, alebo ak je mobilný telefón zaistený ako vecná stopa pri obhliadke podľa

§ 154 Trestného poriadku, nie je potrebné (duplicitné) vydanie príkazu na zistenie a oznámenie údajov o telekomunikačnej prevádzke podľa § 116 (ods. 2) Trestného poriadku.“ [6]

V zmysle odôvodnenia rozsudku Najvyššieho súdu SR z 26. novembra 2014, sp. zn. 2To 9/2014 vydanie a odňatie veci je tradičný trestnoprocesný inštitút, ktorý nie je potrebné dopĺňať príkazom na vydanie počítačových údajov, nakoľko po vydaní veci je už zákonne súladným spôsobom zabezpečený aj príslušný údaj (po jeho bežnou manipuláciou vyvolanom zobrazení na zariadení, resp. zistení znaleckým dokazovaním).

V odôvodnení naposledy uvedeného rozsudku je taktiež konštatované, že „ak ide o samotného páchateľa (obvineného), takým spôsobom (príkazom) by nebolo možné údaje spoľahlivo zabezpečiť, nakoľko po jeho obdržaní (bez súčasného odňatia veci) by mal páchateľ možnosť údaje odstrániť, alebo zničiť samotné zariadenia. Preto je odňatie počítačových údajov v zmysle § 91 Tr. por. možné len ako súčasť odňatia veci (zariadenia s údajmi), čomu však predchádza výzva na vydanie veci (§ 89 ods. 1 Tr. por.), nie príkaz podľa § 90 ods. 1 písm. e/ Tr. por.“[7]

Možno sa stotožniť s argumentáciou použitou v rámci vyššie uvedenej judikatúry, v zmysle ktorej pokiaľ sa zariadenie, ktoré je nositeľom počítačových údajov, dostalo zákonným spôsobom do dispozície orgánov činných v trestnom konaní alebo súdu, nie je potrebné na zabezpečenie samotných údajov v ňom uvedených uplatňovať ešte postup podľa § 90 Tr. por., resp. podľa § 116 Tr. por. Argumentáciu Najvyššieho súdu SR použitú v označenej judikatúre vo vzťahu k získavaniu údajov zo zaistených zariadení možno považovať za logickú a presvedčivú.

Pokiaľ možno dôvodne predpokladať, že na dosiahnutie účelu trestného konania postačuje zabezpečiť počítačové údaje na základe príkazu v zmysle § 90 Tr. por., je potrebné uprednostniť takýto postup pred zaistením celého zariadenia. Zaistenie celého zariadenia predstavuje totiž výrazne citeľnejší zásah do práv užívateľa zariadenie a prípadne aj ďalších osôb ako selektívne zabezpečenie údajov postupom podľa § 90 Tr. por.

Zabezpečovanie obsahových údajov z doručenej, avšak nestiahnutej emailovej komunikácie

Za problematickú oblasť možno považovať voľbu procesného postupu zameraného na získanie dôkazov z obsahu emailových správ (vrátane ich príloh) doručených do emailovej schránky adresáta, ktorú však adresát nestiahol do počítača, prípadne iného obdobného zariadenia.

Naznačenú problematiku podrobne spracoval P. Šamko, podľa ktorého „v prípadoch už zrealizovanej emailovej komunikácie, ktorá je uložená v emailovej schránke prichádza do úvahy pri zisťovaní jej obsahu použitie príkazu podľa § 116 ods. 6 TP, ktorý umožňuje získavať údaje prenášané prostredníctvom počítačového systému, t.j. aj obsahové údaje, ktoré sa prenášajú cez počítačovú sieť medzi počítačmi, resp. údaje, ktoré "zostávajú" uložené v rámci počítačovej sieti na serveri poskytovateľa emailových služieb (emailová komunikácia a pod.). Vydanie takéhoto príkazu má svoje špecifiká, pretože, na rozdiel od príkazu podľa § 116 ods. 2 TP nesmeruje voči poskytovateľovi emailovej služby, pretože ten nedisponuje obsahom emailových správ (či ich príloh), ktoré sa nachádzajú v emailovej schránke. Podstatou príkazu podľa § 116 ods. 6 TP bude teda súdny pokyn orgánom činným v trestnom konaní, aby vnikli do konkrétnej emailovej schránky, zistili jej obsah a zaistili (stiahli) ten obsah, ktorý je relevantný pre trestné konanie (napr. faktúru, zmluvu, konverzáciu medzi účtovníkom a

[6] Podľa R 47/2017

[7] rozsudok Najvyššieho súdu SR z 26. novembra 2014, sp. zn. 2To 9/2014

podozrivou osobou a pod.).“[8]

K vyššie citovanému zastávame názor, že postupom podľa § 116 Tr. por. nemožno zisťovať obsahové údaje. To platí pre zistenie a oznámenie údajov o telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva, alebo na ktoré sa vzťahuje ochrana osobných údajov podľa § 116 ods. 1, ods. 2 Tr. por. a obdobne aj pre postup podľa § 116 ods. 2, ods. 6 Tr. por. V tejto súvislosti považujeme za rozhodujúce v § 116 ods. 1 Tr. por. použité slovné spojenie „príkaz na zistenie a oznámenie údajov **o** telekomunikačnej prevádzke“, ktoré je potrebné aplikovať primerane na postup v zmysle § 116 ods. 2, ods. 6 Tr. por. Zámerom zákonodarcu nebolo umožniť postupom podľa § 116 ods. 6 Tr. por. získať údaje odlišného charakteru od údajov, ktoré možno získať príkazom vydaným podľa § 116 ods.1, ods. 2 Tr. por. (s výnimkou rozdielu vyplývajúceho z faktu, že postup podľa § 116 ods. 1, ods. 2 Tr. por. sa vzťahuje na telekomunikačnú prevádzku a postup podľa § 116 ods. 2, ods. 6 Tr. por. na údaje prenášané prostredníctvom počítačového systému). Názor, podľa ktorého postupom podľa § 116 Tr. por. nemožno získavať obsahové údaje je možné identifikovať aj v rámci odbornej literatúry.[9]

Vyššie uvedené úvahy uzatvárame, že postupom podľa § 116 ods.2, ods. 6 Tr. por. nemožno zákonne získať obsahové údaje z emailových správ doručených do emailovej schránky adresáta, ktoré však neboli stiahnuté (uložené) do počítača.

Máme za to, že obsah takýchto emailových správ je možné pre účely trestného konania zabezpečovať príkazom podľa § 90 Tr. por., nakoľko sa jedná o počítačové údaje uložené prostredníctvom počítačového systému (servera) s tým, že adresátom príkazu bude majiteľ emailovej schránky, resp. iná osoba majúca legálny prístup do emailovej schránky. Argument, podľa ktorého „ak orgán činný v trestnom konaní nemá prístup do emailovej schránky podozrivej osoby, nemá ani reálnu možnosť posúdiť, či podozrivá osoba takýto príkaz (podľa § 90 Tr. por. – pozn. autorov) rešpektovala a niektorú emailovú poštu jednoducho neodstránila“[10], na ktorý poukazuje P. Šamko, podľa nášho názoru, s ohľadom na vyššie uvedené dôvody, nič nemení na konštatovaní, že postupom podľa § 116 Tr. por. nemožno zabezpečiť obsahové údaje.

Záver

Predkladaný príspevok poukazuje len na niektoré interpretačné problémy vyplývajúce z trestnoprocesnej právnej úpravy vzťahujúcej sa na zabezpečovanie počítačových údajov. Napriek tomu však naznačuje, že táto oblasť právnej úpravy vytvára značný priestor pre rôzny výklad príslušných zákonných ustanovení. Na tomto fakte sa podieľa vo významnej miere technická zložitosť postupov, ktoré sú predmetom posudzovanej časti právnej úpravy. Vychádzajúc z výsledkov analýzy obsiahnutej v príspevku autori majú za to, že názory prezentované v rámci judikatúry, podľa ktorých údaje uložené v mobilnom telefóne nie sú počítačovými údajmi v zmysle § 90 Tr. por., možno považovať za problematické a autori sa a nimi nestotožňujú. Naopak stotožňujú sa s názormi judikatúry, z ktorých vyplýva, že na získanie počítačových údajov zo zariadení už zaistených orgánmi činnými v trestnom konaní zákonným spôsobom, nie je potrebné vydávať príkaz v zmysle § 90 Tr. por., resp. podľa § 116 Tr. por. Postup podľa § 116 ods. 2, ods. 6 Tr. por. nepovažujú za zákonný prostriedok na zabezpečovanie obsahových údajov z doručenej, avšak do počítača ešte nestiahnutej emailovej komunikácie. Takéto obsahové údaje možno zabezpečovať postupom podľa § 90 Tr. por.

---

[8] ŠAMKO, P. Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestnom konaní. Klientsky program ONLINE Aspi. In: Zo súdnej praxe. 2017, č. 6/2017.

[9] Napr. IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné*. 1. Bratislava: Wolters Kluwer, s.r.o., 2017. ISBN 978-80-8168-593-4. s. 393.

[10] ŠAMKO, P. Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestnom konaní. Klientsky program ONLINE Aspi. In: Zo súdnej praxe. 2017, č. 6/2017.

Zoznam použitej literatúry:

IVOR, J., POLÁK, P., ZÁHORA, J. *Trestné právo procesné. 1.* Bratislava: Wolters Kluwer, s.r.o., 2017. ISBN 978-80-8168-593-4.
ŠAMKO, P. *Poznámky k aplikačným problémom pri zaisťovaní počítačových údajov v trestnom konaní.* Klientsky program ONLINE Aspi. In: Zo súdnej praxe. 2017, č. 6/2017.
Judikatúra:
R 47/2017 (Uznesenie Najvyššieho súdu Slovenskej republiky z 23. marca 2017, sp. zn. 5 Tdo 7/2017)
rozsudok Najvyššieho súdu Slovenskej republiky sp. zn. 2To 9/2014 zo dňa 26.11.2014 Právne predpisy
zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
dohovor Rady Európy o počítačovej kriminalite, prijatý členskými štátmi Rady Európy dňa 23.11.2001 v Budapešti (oznámenie MZV SR č. 137/2008 Z.z.).
Internetové a iné zdroje:
wikipedia
Dôvodová správa k zákonu č. 301/2005 Z. z. Trestný poriadok

Kontaktné údaje:

JUDr. Remig Kubička
prokurátor
Okresná prokuratúra Bratislava IV
Kuklovská 64
841 05 Bratislava
t. č. 0905 825 013
remigkubicka@gmail.com

MUDr. Oliver Kubička
Nám. sv. Františka 8
841 04 Bratislava

Aktuálne trendy súvisiace s využívaním moderných technológií

Jana Kuchtová

Abstrakt:
Autorka príspevku sa snaží poukázať na vybrané aktuálne trendy súvisiace s využívaním technológií 21. storočia vychádzajúce z hardware a software zariadení, prostredníctvom ktorých tvoríme, prijímame, ukladáme, posielame alebo inak spracovávame osobné a iné citlivé údaje. Tie sú častým predmetom útokov páchateľov kybernetickej kriminality za účelom ich zneužívania, či už vo vlastný prospech alebo poskytnutie tretím osobám. Cieľom príspevku je poukázať nielen na novinky zo sveta technológií ale aj na reálne existujúce nebezpečenstvá a poskytnúť východiská a odporúčania na zlepšenie súčasného stavu.
Kľúčové slová:
Internet vecí, (IoT), inteligentné zariadenia, smart zariadenia, kybernetická kriminalita, inteligentné mestá

Abstract:
The author of the paper tries to provide an overview of the selected current trends related to the use of 21st century technologies based on hardware and software devices, through which we form, receive, store, send or otherwise process personal and other sensitive data. These are often the subject of attacks by cybercriminals for their misuse, whether for their own benefit or provide to a third party. The aim of the paper is to highlight not only the new technologies but also the real existing dangers and provide the basis and recommendations for improving the current state.
Key words:
Internet of Things, (IoT), smart devices, cyber criminality, smart cities

Úvod

V posledných rokoch prichádza na trh neuveriteľné množstvo technologických noviniek a inteligentných zariadení, ktoré je možné vzájomne prepájať a využívať plné rozhranie aplikovateľné tak v pracovnej, ako aj súkromnej sfére života. Prichádzajú čoraz inovovanejšie a inteligentnejšie zariadenia, ktoré sú prispôsobované požiadavkám užívateľov. Či už ide o výkonné počítače, ultra tenké notebooky a inteligentné smatrphone zariadenia, alebo IoT smart zariadenia – televízie, routre, kamery, chladničky a mnoho ďalšieho, je najzásadnejšou otázkou súčasnosti bezpečnosť. Je nutné neustále skúmať zabezpečenie technológií, ich chyby a nedostatky aby tak bolo možné odhaľovať spáchanú, prebiehajúcu alebo plánovanú nelegálnu činnosť vykonávanú za účelom neoprávneného získavania osobných údajov, hesiel a ďalších informácií. Existuje nespočetné množstvo dôvodov páchania kybernetickej kriminality a úlohou štátu je prostredníctvom legislatívnych ustanovení a výkonných zložiek zabezpečovať ochranu obyvateľov pred týmto rozrastajúcim sa negatívnym fenoménom 21. storočia. Je nutné zameriavať sa na bezpečnostné testovanie daných zariadení ešte skôr, ako sa dostávajú ku koncovým Používateľom a nekontrolovateľne sa šíria medzi ľuďmi, pretože často krát sme svedkami toho, ako prichádzame na nedostatky príliš neskoro. Aj keď v relatívne krátkej chvíli prichádzajú inštitúcie s „náplasťami“ a opravami, škody ktoré boli spôsobené sú mnoho krát veľmi závažné a kvôli vysokej latentnosti páchania nie je často možné zistiť úplný dopad na spoločnosť. Snahou tohto príspevku je oboznámiť čitateľa s rozširujúcim sa trendom najmä v oblasti Internetu veci, poukázanie na prípadné bezpečnostné riziká spojené s jeho využívaním a zároveň možnosti použitia vybraných inteligentných zariadení v rámci Policajného zboru.

Zabezpečenie počítačov, notebookov, smartphone zariadení, tabletov a mnohých ďalších zariadení modernej technológie sa stáva jednou z najdôležitejších oblastí súčasnosti. Okrem predchádzania poškodeniam spomínaných technológií ide hlavne o ochranu obsahu nachádzajúceho sa na ich úložiskách. Často krát ide o citlivé informácie, know-how, súkromné údaje, heslá, poznámky a iné dáta, ktoré sa snažia útočníci získavať či už pre vlastnú potrebu, alebo predaj tretím osobám. Tak ako sa na ochranu cenností využívajú trezory, ochranu bytov bezpečnostné dvere, ochranu domov alarmy, tak sa na ochranu zariadení využívajú rôzne

antivírusové programy akými sú napríklad Norton, BullGuard, Avast, Eset, AVG či iné, disponujúce rôznymi funkciami, napríklad Software Updater, čistenie prehliadačov, skartovanie dát, SecureLine VPN, Sandbox, Firewall, Anti-Spam[1] a mnoho ďalšieho. Sieťové funkcie ako VPN či firewall chránia sieť do ktorej sú pripojené domáce zariadenia, vrátane inteligentných IoT technológií. Otázka však znie, či je táto ochrana pre počítače dostačujúca a či po zakúpení relatívne drahých licencií od renomovaných spoločností distribuujúcich antivírusové programy nastane dostatočná ochrana užívateľského počítača. Je zrejmé, že ani trezory alebo bezpečnostné dvere neposkytujú 100% účinnú ochranu a viac menej len predlžujú čas páchateľa snažiaceho sa osvojiť si cudzí majetok. To isté platí aj pre antivírusové programy, ktoré musia čeliť novým formám vírusov, ktoré sú čoraz viac sofistikované a ťažšie odhaliteľné. Spoločnosti reagujú na všetky takéto hrozby aktualizáciami svojich antivírusových programov, šírením povedomia o nových útokoch a o možnostiach prevencie. V súvislosti s uvedením je preto nutné zamyslieť sa nad tým, či riešenie vzájomne prepojených zariadení (prostredníctvom siete) je dostatočne bezpečné.

Internet vecí

Prvý krát bol tento pojem použitý už v roku 1999 ako snaha poukázať na to, že nie len počítače, ale aj internet sú závislé na informáciách ktoré zadávajú, zaznamenávajú alebo vytvárajú ľudia. Tí však nemôžu sledovať a spracovávať všetko, riešením čoho má byť práve IoT – Internet of Things (Internet vecí). Umožnilo by to zariadeniam „vedieť" viac o veciach z údajov, ktoré by si zhromažďovali, ukladali a analyzovali samé, bez obmedzenia spracovávania len tých údajov, ktoré im zadá človek.[2] Internet vecí možno chápať ako prepojenie akéhokoľvek elektrického zariadenia s internetom alebo navzájom, nad rámec bežných zariadení akými sú stolné počítače, notebooky, smartphone zariadenia a tablety, do tradičných zariadení a bežných objektov. Či už ide o zámky dverí, chladničku, auto, svietidlá alebo mnoho iného, všetky tieto zariadenia ktoré majú internetové pripojenie patria do skupiny IoT.

<u>4 hlavné súčasti systému IoT:</u>

1. Zariadenie,
2. miestna (lokálna) sieť,
3. internet,
4. cloudové služby umožňujúce vytvárať záložné verzie aplikácií.

Okrem pripojenia samotného hardware do internetovej siete majú tieto technológie vlastný software. Prostredníctvom internetu môžu byť takéto zariadenia monitorované, kontrolované a ovládané na diaľku prostredníctvom bezdrôtových mostov. Ide o rôzne formy hardware podpory premostenia bezdrôtovej siete:

- hardware umožňujúci klientom Wi-Fi pripojiť sa k sieti Ethernet,

[1] **Software Updater** - slúži na aktualizovanie software čím chráni zariadenie pred hrozbami a útočníkmi využívajúcimi chyby staršieho software.
Čistenie prehliadačov - slúži na odstránenie problémových doplnkov prehliadačov.
Skartovanie dát - trvalé odstraňovanie súborov ktoré nie je možné obnoviť a zneužiť.
SecurLine VPN – ide o virtuálnu privátnu sieť šifrujúcu dáta a zabezpečujúcu pripojenie verejných sietí Wi-Fi.
Sandbox – bezpečné izolované prostredie umožňujúce bezpečnejšie prehliadanie webových stránok a spúšťanie aplikácií.
Firewall – ochrana pred neoprávneným vstupovaním do komunikácie medzi zariadením a vonkajším svetom.
Anti-Spam – ide o ochranu e-mailovej schránky pred nevyžiadanou poštou.

[2] KEVIN, A. *That 'Internet of Things' Thing*. [online]. [cit. 15. 06. 2018]. Dostupné na internete: <http://www.rfidjournal.com/articles/view?4986>

- hardware spájajúci dve siete Wi-Fi za účelom zvýšenia oblasti pokrytia Wi-Fi hotspotu[3],
- prostredníctvom Bluetooth na Wi-Fi ktorá umožňuje komunikáciu medzi Bluetooth gadgets[4] a domácou sieťou Wi-Fi.

Niektoré bezdrôtové mosty podporujú spojenie z jedného bodu do druhého, iné podporujú pripojenie k viacerým sieťam (point to multipoint).[5]

Keďže sa používatelia čoraz viac spoliehajú na pripojené, samo-riadiace a samočinné zariadenia, kľúčové aspekty kvality, ktoré je potrebné zvážiť, sú bezpečnosť, výkonnosť, funkčnosť a použiteľnosť. Tie je nutné neustále testovať a analyzovať, aby sa zisťovalo, či keď jedno zariadenie zlyhá, budú ostatné fungovať.[6]

1. Bezpečnosť

Na zaistenie bezpečnosti IoT zariadení je najlepšie jej testovanie. Vzhľadom na možné riziká straty osobných a citlivých údajov, napadnutia internetovej siete či samotných zariadení je nevyhnutné neustále testovanie, ktoré možno vykonávať prostredníctvom penetračných testov. Na ich základe je možné odhaliť slabiny a zistiť mieru zraniteľnosti a následne tieto nedostatky odstrániť.

2. Výkonnosť

Testovanie výkonnosti slúži na zistenie, či sú všetky údaje a informácie prenášané a ukladané správne a to aj v prípade útoku alebo výpadku systémov. Tým je možné predchádzať strate dôležitých údajov.

3. Funkčnosť

Už z názvu vyplýva, že v tomto prípade ide o testovanie funkčnosti zariadení a ich aplikácií, prostredníctvom pozitívnych a záporných testov. Pozitívnym testovaním sa kontroluje aplikácia na základe platných vstupných údajov, zatiaľ čo pri zápornom testovaní je overovaná nefunkčnosť aplikácií na nesprávne alebo neplatné vstupné údaje.

4. Použiteľnosť

Testovaním použiteľnosti je myslená najmä kompatibilita funkcií zariadení v rôznych konfiguráciách, verziách zariadení, protokolov a iné.[7]

IoT v praxi

Vzhľadom na obrovské množstvo zariadení si v nasledujúcej časti článku rozoberieme vybrané zariadenia týkajúce sa inteligentných domácností, inteligentných miest a možnosti využitia IoT v rámci Policajného zboru. Na jednej strane má možnosť čitateľ oboznámiť sa s pozitívnym prínosom, na strane druhej s bezpečnostnými hrozbami ktoré so sebou táto moderná technológia prináša.

---

[3] **WiFi Hotspot** umožňuje prostredníctvom smartphone zariadenia alebo tabletu zdieľať mobilné pripojenie k internetu a vytvoriť Wifi sieť do ktorej sa môžu zapojiť viacerí používatelia so zariadeniami podporujúcimi Wi-Fi.

[4] **Gadget** – malý technologický objekt s osobitnou funkciou, novinka, vychytávka (za gadget je považovaný napríklad fidget spinner, hľadač kľúčov atď.)

[5] MITCHELL, B. *Wi-Fi Wireless Bridging Explained*. [online]. [cit. 15. 06. 2018]. Dostupné na internete: <https://www.lifewire.com/wireless-bridging-explained-816563>

[6] NOVIK, P. *Testing IoT Devices*. *Key areas.* [online]. [cit. 15. 06. 2018]. Dostupné na internete: <http://www.softwaretestingmagazine.com/knowledge/testing-iot-devices-key-areas/>

[7] NOVIK, P. *Testing IoT Devices*. *Key areas.* [online]. [cit. 15. 06. 2018]. Dostupné na internete: <http://www.softwaretestingmagazine.com/knowledge/testing-iot-devices-key-areas/>

Obrázok 1 Internet vecí

Zdroj http://www.softwaretestingmagazine.com/knowledge/testing-iot-devices-key-areas/

Inteligentné zámky dverí

Inteligentný zámok dverí funguje na základe bezdotykového snímača ako Bluetooth alebo NFC[8], ktorý umožňuje odomknúť dvere po priblížení autorizovaného zariadenia. Užívateľ má možnosť vytvoriť virtuálne „kľúče“ pre rodinu a hostí pričom má k dispozícii okamžité upozornenie na prebiehajúce aktivity. Tieto oprávnenia je možné nastaviť na 24 hodín alebo v rozvrhu. Podľa typu zámku sa na nich nachádza aj možnosť odomykania prostredníctvom zadania v priemere 30 kódov na číselnej klávesnici, odtlačkom prsta alebo štandardným kľúčom. Zámky fungujú na batérie, ktoré vydržia v priemere 3 – 5 mesiacov, následne je nutné dobytie alebo výmena, pričom ich vybitie signalizuje smartphone aj samotný zámok.

Príkladom využitia inteligentného zámku dverí je Amazon Key – diaľkovo ovládaná platforma na prístup k budovám/ domácnostiam, ktorá ma okrem vyššie menovaných funkcií aj možnosť využitia doručovania balíkov z Amazonu až do domácnosti/ firmy, aj keď sa nikto nenachádza doma. Domáce doručovanie funguje na tomto princípe:

- použitím aplikácie a po nakúpení sortimentu pomocou adresy, na ktorej je nainštalovaný Amazon Key, je možnosť zvoliť si bezplatné doručenie do domácnosti.
- V deň doručenia je príjemca dva krát informovaný – ráno a tesne pred doručením, aby si blokoval alebo sledoval prostredníctvom kamery a aplikácie doručenie zásielky až do domu.
- Doručovateľ s povolením od spoločnosti Amazon môže otvoriť zamknuté dvere príjemcovho domu a doručiť mu zásielku.
- Ak si príjemca nechá doručiť balík až do domácnosti, príde mu ďalšie upozornenie o dokončení dodávky a znovu zamknutí dverí. Súčasne má na 24 hodín k dispozícii video záznam zaznamenávajúci vstup osoby do domu.
- Príjemca má vždy možnosť blokovať prístup do domu a zvoliť si inú alternatívu doručenia.[9]

[8] **NFC** je bezdrôtová technológia fungujúca na princípe elektromagnetickej indukcie umožňujúca komunikáciu medzi dvomi zariadeniami na krátku vzdialenosť.

[9] AMAZON. *amazon key.* [online]. [cit. 17. 06. 2018]. Dostupné na internete: <https://www.amazon.com/b?ie=UTF8&node=17861200011>

Obrázok 2 Amazon Key Home Kit
Zdroj https://www.amazon.com/b?ie=UTF8&node=17861200011

Aj keď na jednej strane môže v mnohých prípadoch takáto služba uľahčiť ľuďom život, na druhej strane je nutné uvedomiť si riziká spojené s touto novou technológiou. Firma zameraná na bezpečnosť zistila, že kuriér mohol zmraziť videozáznam a počas toho nerušene chodiť po domácnosti. Takýto útok bolo možné spáchať prostredníctvom Wi-Fi siete, kedy by útočník posielal „deautorizačné" pakety zamerané na kameru pripojenú do siete, vplyvom ktorých by sa pokúšala o opätovnú autentifikáciu a zastavila by používanie prístupového bodu - táto technika sa často využíva na rušenie Wi-Fi. Takto cielený útok na kameru spôsobil, že ostala offline, ale naďalej zobrazovala posledný zachytený snímok. Majiteľa služby však na tento jav nič neupozorňovalo a pri kontrole video záznamu z domácnosti videl kuriéra, ktorý doručil zásielku. Ten následne aktivoval útok a zatiaľ čo aplikácia zobrazovala zamrznutú fotografiu prázdnej domácnosti, kuriér sa mohol nerušene vrátiť do domu. Po zistení týchto nedostatkov bezpečnostnou firmou vyšla aktualizácia, ktorá upozorňuje majiteľov, ak kamera ostane offline a súčasne ak je Wi-Fi alebo kamera v režime offline, systém neumožní iným používateľom odomknúť dvere.[10]

Inteligentné chladničky

Inteligentné chladničky patria medzi známe zariadenia patriace do IoT. Ich hlavnou vlastnosťou je na rozdiel od bežných chladničiek software a pripojenie do siete – v ktorej sú spravidla aj ďalšie zariadenia (počítače, notebooky, smartphone zariadenia, tablety, ďalšie inteligentné technológie).

Obrázok 3 Samsung Smart Refrigerator
Zdroj https://www.samsung.com/us/explore/family-hub-refrigerator/overview/

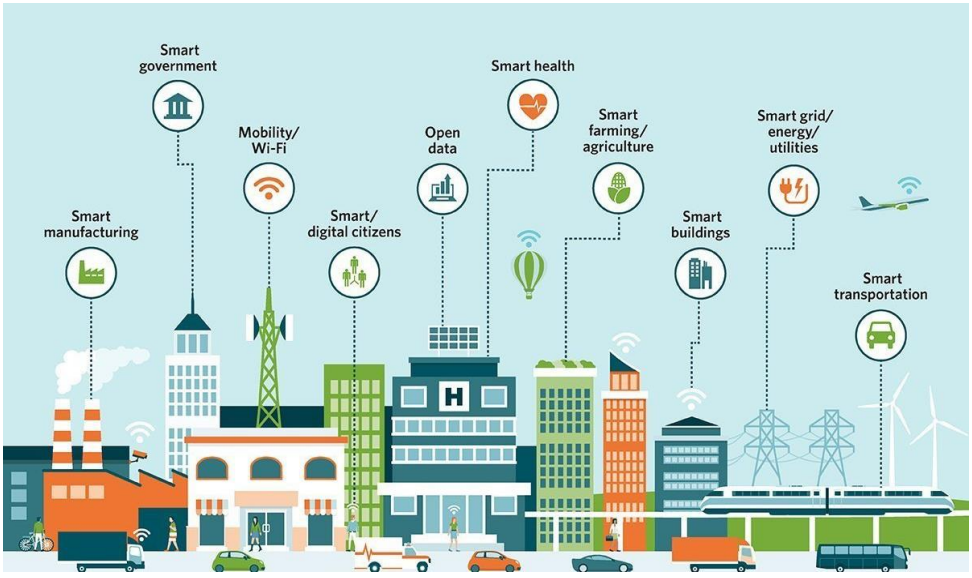
[10] TUNG, L. *Amazon: We're fixing flaw that leaves Key security camera open to Wi-Fi jamming.* [online]. [cit. 18. 06. 2018]. Dostupné na internete: <https://www.zdnet.com/article/amazon-were-fixing-flaw-that-leaves-key-security-camera-open-to-wi-fi-jamming/>

Chladnička je vybavená dotykovou obrazovkou, ktorá umožňuje naplánovať si dopredu jedlá, aktivity, uľahčuje usporiadať domácnosť – disponuje funkciou vytvárania nákupných zoznamov, má funkciu „nazerania“ do chladničky odkiaľkoľvek, upozorňuje na skončenie minimálnej doby trvanlivosti, čím zabezpečuje čerstvosť potravín. Aplikácia nákupný zoznam dokáže synchronizovať rodinných príslušníkov, pričom potraviny je možné nakupovať priamo z dverí chladničky. Medzi prepojenými smartphone zariadeniami je možné zdieľať kalendáre, poznámky, fotografie a iné, samozrejmosťou je tiež možnosť „surfovať“ po internete prostredníctvom dotykového panelu. Okrem iného má funkciu prehrávania hudby, živých prenosov a televízie čo umožňuje aplikácia TV Mirroring a prostredníctvom funkcie S Voice dokáže nahlas „čítať“ recepty a prijímať pokyny.[11]

Problémom týchto inteligentných zariadení sú software aktualizácie na opravu bezpečnostných dier, ktoré sú nedostatočné alebo úplne chýbajú. Následkom toho, že ide o priamy prístup chladničky do siete, je možné šíriť škodlivý software na iné zariadenia v domácnosti. Hacker by sa mohol prostredníctvom útoku na inteligentné domáce systémy dostať k citlivým údajom zo smartphone zariadení, notebookov, tabletov, mohol by sledovať všetko, čo je zdieľané napr. s chladničkou a taktiež by mohol meniť jej nastavenia.

IoT v mestách

Inteligentné mesto je obec, ktorá využíva informačné a komunikačné technológie na zvýšenie prevádzkovej efektívnosti, zdieľanie informácií s verejnosťou a zlepšenie kvality štátnych služieb a blahobytu občanov. Hlavným aspektom je optimalizovať mestské funkcie a stimulovať hospodársky rast a zároveň zlepšiť kvalitu života svojich občanov pomocou inteligentnej technológie a analýzy údajov.



Obrázok 4 Smart city components

Zdroj https://internetofthingsagenda.techtarget.com/definition/smart-city

IoT v mestách môže dopomôcť k riešeniu mnohých problémov, napríklad pomocou inteligentného koša na odpadky pripojeného na internet, vybaveného snímačmi naplnenia, by bolo možné dátové riadiace a logistické platformy priemyslu presúvať do čistejšej a účinnejšej súčasti moderného života. V súčasnosti sa väčšina zberu komunálneho odpadu zameriava na vyprázdňovanie kontajnerov podľa vopred stanovených plánov, čo je neefektívne, pretože

[11] SAMSUNG. *Family hub refrigerator. Connected hub.* [online]. [cit. 18. 06. 2018]. Dostupné na internete: <https://www.samsung.com/us/explore/family-hub-refrigerator/connected-hub/>

vyprázdnené sú často krát polovične naplnené koše. Tým pádom dochádza k zbytočnej spotrebe paliva a ďalším výdavkom. Okrem iného by používaním takýchto zariadení malo dôjsť k zlepšeniu ochrany životného prostredia a zdravia. Ďalším klasickým príkladom inteligentného mesta sú parkovacie snímače, ktoré pomáhajú vodičom pri hľadaní dostupných parkovacích miest a súčasne tento digitálny merač umožňuje digitálnu platbu. Využívanie inteligentných technológií v doprave môže dopomôcť k presnému monitorovaniu a analyzovaniu dopravnej situácie, uplatnenie ktorého by bolo v riešení problémov s preťaženými cestnými komunikáciami. Pomocou inteligentných snímačov na pouličných lampách by bolo možné efektívne využívať energiu, preto že by sa automaticky stimievali v neprítomnosti vozidiel a chodcov. Technológia inteligentného mesta sa čoraz viac využíva na zlepšenie verejnej bezpečnosti, prostredníctvom monitorovania oblastí s vysokou kriminalitou. Inteligentné snímače môžu byť dôležitými súčasťami systému včasného varovania pred suchami, povodňami, zosuvom pôdy alebo hurikánmi, čo povedie k zlepšeniu havarijnej pripravenosti. Snímače umiestnené na budovách a verejnej infraštruktúre sú schopné upozorňovať na ich nevyhovujúci stav.[12]

Príklady inteligentných miest:

- Dubaj

Mesto Dubaj využíva inteligentnú zdravotnú starostlivosť, inteligentné budovy, nástroje, vzdelávanie, cestovný ruch, inteligentné dopravné smerovanie, parkovanie, infraštruktúru a dopravu.

- Barcelona

Barcelona využíva systém inteligentnej dopravy a inteligentné autobusové systémy, ktoré sú doplnené o inteligentné autobusové zastávky, poskytujúce bezplatné Wi-Fi, nabíjacie stanice USB a aktualizácie autobusových plánov pre jazdcov. Mesto používa aj snímače na monitorovanie teploty, znečistenia a hluku, ako aj na monitorovanie vlhkosti a dažďov.

- Singapur

Singapur má k dipozícii snímače a kamery s podporou IoT na monitorovanie čistoty verejných priestorov, hustoty davu a pohybu miestnych registrovaných vozidiel. Jeho inteligentné technológie pomáhajú spoločnostiam a obyvateľom monitorovať spotrebu energie, produkciu odpadu a spotrebu vody v reálnom čase. Singapur tiež testuje autonómne vozidlá, vrátane robotických autobusov s plnou veľkosťou, ako aj starší monitorovací systém na zabezpečenie zdravia a blahobytu svojich seniorov.

- San Diego

San Diego nainštalovalo 3 200 inteligentných snímačov s cieľom optimalizovať prevádzku a parkovanie a zvýšiť verejnú bezpečnosť, povedomie o životnom prostredí a celkovú dostupnosť pre svojich obyvateľov. Súčasne monitorujú dopravu a využívajú systém na zaraďovanie páchateľov k spáchaným zločinom.[13]

Aj napriek tomu, že IoT v mestách môže rovnako ako v domácnostiach pomáhať ľuďom skvalitniť, zjednodušiť a zefektívniť život, je namieste otázka, ako by reálne nakladalo mesto s nazbieranými osobnými údajmi svojich obyvateľov. Aj keď na jednej strane platia pravidlá ochrany osobných údajov, na druhej strane dochádza k ich častému porušovaniu a len málo kedy sme svedkami riešenia takýchto pochybení. O to viac skepticky je nutné pristupovať k vízii bezpečnosti, pretože je logické, že zatiaľ čo by hacker získal z jednej domácnosti len pár

[12] ROUSE, M. *smart city.* [online]. [cit. 19. 06. 2018]. Dostupné na internete: <https://internetofthingsagenda.techtarget.com/definition/smart-city>

[13] ROUSE, M. *smart city.* [online]. [cit. 19. 06. 2018]. Dostupné na internete: <https://internetofthingsagenda.techtarget.com/definition/smart-city>

osobných údajov, z nazbieraných údajov o obyvateľoch celého mesta a z ovplyvňovania jeho inteligentných systémov by mohol mať oveľa väčší úžitok. Vychádzajúc z toho je zrejmé, že by boli zo strany páchateľov neustále pokusy o napádanie takýchto zariadení, pričom náklady na ich ochranu by boli po zakúpení finančne náročných inteligentných zariadení neúnosné.

IoT v Policajnom zbore

Význam Internetu veci a jeho budúcnosť neovplyvňuje len súkromné osoby a firmy, ale jeho využitie by si nepochybne našlo miesto aj v oblasti štátnej sféry - či už ozbrojených silách, polícii, zdravotníctve, hasičov a iných zložiek. Trendy naznačujú, že väčšina zločinov bude schopná využívať internet, alebo vytvoriť nejakú formu digitálnej stopy. Policajné zložky musia preto disponovať zdrojmi a zručnosťami, aby na to boli schopné reagovať. S ohľadom na to by sa mala polícia snažiť o užšiu spoluprácu so súkromným sektorom, s cieľom znížiť riziko a získať správne technológie na efektívnu prácu. Mohlo by to viesť k zmierneniu potenciálnych hrozieb, vyššej efektívnosti a zvýšenej verejnej bezpečnosti. Ľudstvo sa vo všeobecnosti technologicky posúva dopredu, modernizuje sa a digitalizuje, čo znamená nevyhnutnú potrebu orgánov zabezpečujúcich ochranu života, zdravia a majetku držať krok a prispôsobovať sa týmto informačno-technologickým zmenám. Tak ako v iných oblastiach, aj v tejto konkrétnej by Internet vecí mohol pomôcť k zisťovaniu zločinu, napríklad prostredníctvom súkromných bezpečnostných systémov alebo „smart cities“, čo by mohlo viesť k poznaniu kde, s kým a kedy spáchal páchateľ trestný čin, čo pritom robil a mnoho ďalšieho. Už samotné vedomie páchateľa o existencii oveľa vyššieho rizika, že mu na to prídu, môže pôsobiť preventívne. K ľahšiemu odhaleniu páchateľov by mohli prispieť dáta zo systémov rozpoznávajúcich tváre, ktoré by po nahraní do policajných systémov dokázali stotožniť podozrivú osobu s ďalšími evidovanými trestnými činmi, alebo priestupkami. Ďalšie využitie v Policajnom zbore spočíva v dôkladnejšom získavaní, spracovávaní, analyzovaní, ukladaní a využívaní informácií a dát spojených s výkonom služby. Významnou oblasťou sú inteligentné vozidlá a zariadenia, to si však vyžaduje nemalé finančné prostriedky. Riešením častých dopravných nehôd spôsobených rýchlou jazdou policajtov na miesto činu, ktoré keď nastane nehoda často krát končia tragicky, sú prepojené policajné systémy so semaformi, ktoré by sa prispôsobili trase príslušníkov PZ.[14] Ďalším problémom je potreba neustálych školení a vzdelávania príslušníkov PZ a rozvíjania ich vedomostí a schopností pri efektívnom využívaní takýchto technológií. V súčasnosti je problematický záujem odborníkov a špecialistov z IT oblasti pôsobiť v rámci Policajného zboru kvôli nedostatočnému finančnému ohodnoteniu, oproti konkurenčnej a oveľa lepšie ohodnotenej súkromnej sfére. Tento pokrok je však nevyhnutný a je len otázkou času kedy sa bude musieť aplikovať v praxi.

Záver

Po analýze dosiahnutých poznatkov možno konštatovať, že Internet vecí je a do budúcna určite bude tvoriť súčasť tohto storočia. Na jednej strane je to veľký pokrok a uľahčenie nie len bežného života, ale ako bolo uvedené na vybranom príklade aj v rámci Policajného zboru, na strane druhej si zatiaľ nedokážeme predstaviť, aké veľké nebezpečenstvo táto zmena so sebou prináša. Tieto zariadenia môžu na jednej strane dopomôcť k sledovaniu a riešeniu najzávažnejších problémov populácie, akými je deficit neobnoviteľných prírodných zdrojov, znečisťovanie planéty, globálne otepľovanie, vyhynutie živočíchov a rastlín a mnoho ďalšieho, dokážu zvýšiť životný štandard, predchádzať rôznym chorobám a úmrtiam, dopomáhať k zdravej kondícii, mať svoje domácnosti, autá a ďalšie zariadenie pod dohľadom a pod kontrolou. Na strane druhej, zatiaľ čo inteligentné zariadenia a systémy uľahčujú život

[14] LAUCHLAN, S. *The IoT-enabled police officer – building a digital law enforcement future.* [online]. [cit. 20. 06. 2018]. Dostupné na internete: < https://government.diginomica.com/2017/06/29/iot-enabled-police-officer-building-digital-law-enforcement-future/>

pre svojich užívateľov, trvalé prijatie internetu vecí a integrácia inteligentnejších systémov do kritických infraštruktúr spôsobuje, že mnohé odvetvia a spotrebitelia sú viac zraniteľní voči útokom - pravdepodobne život ohrozujúcim. Až praxou a skúsenosťami používateľov sú vytvárané aktualizácie zariadení, u ktorých sú preukázané bezpečnostné problémy alebo u ktorých dôjde k úspešnému útoku páchateľa. Keďže sa v súčasnosti vyvíja veľa IoT zariadení, vyvíjajú sa aj hrozby proti nim – naopak bezpečnosť týchto zariadení sa nevyvíjala rovnakou rýchlosťou. Problémy sa začínajú objavovať často krát až po predaji, následkom čoho je potrebné, aby výrobcovia zdvojnásobili svoje bezpečnostné úsilie. Riešením je neustála analýza a testovanie nie len konceptov, ale aj dostupných zariadení na trhu, napríklad prostredníctvom etického hackingu.

Používatelia, ktorý využívajú IoT by mali dodržiavať tieto hlavné zásady:

- Povoliť všetky funkcie zabezpečenia na všetkých inteligentných zariadeniach,
- vždy aktualizovať firmware zariadenia,
- používať zabezpečené heslá,
- zatvoriť všetky nepoužívané porty zariadení a smerovačov,
- použiť šifrovanie pre všetky siete a zariadenia.

Vždy je nutné uvedomovať si, že aj keď štandardné elektrické zariadenia sú samé o sebe relatívne bezpečné, akonáhle ich pripojíme do internetovej siete stávajú sa veľmi zraniteľnými a tým pádom ich treba považovať za nebezpečné. Pre lepšie pochopenie môžeme použiť ako príklad zbraň - bez nábojov je relatívne bezpečná, nabitá zbraň v rukách zodpovednej osoby je potenciálne riziko, no nabitá zbraň v rukách páchateľa je veľká bezpečnostná hrozba.

Zoznam použitej literatúry:

AMAZON. *amazon key.* [online]. [cit. 17. 06. 2018]. Dostupné na internete: <https://www.amazon.com/b?ie=UTF8&node=17861200011>

KEVIN, A. *That 'Internet of Things' Thing.* [online]. [cit. 15. 06. 2018]. Dostupné na internete: <http://www.rfidjournal.com/articles/view?4986>

LAUCHLAN, S. *The IoT-enabled police officer – building a digital law enforcement future.* [online]. [cit. 20. 06. 2018]. Dostupné na internete: <https://government.diginomica.com/2017/06/29/iot-enabled-police-officer-building-digital-law-enforcement-future/>

MITCHELL, B. *Wi-Fi Wireless Bridging Explained*. [online]. [cit. 15. 06. 2018]. Dostupné na internete: <https://www.lifewire.com/wireless-bridging-explained-816563>

NOVIK, P. *Testing IoT Devices*. *Key areas.* [online]. [cit. 15. 06. 2018]. Dostupné na internete: <http://www.softwaretestingmagazine.com/knowledge/testing-iot-devices-key-areas/>

ROUSE, M. *smart city.* [online]. [cit. 19. 06. 2018]. Dostupné na internete: <https://internetofthingsagenda.techtarget.com/definition/smart-city>

SAMSUNG. *Family hub refrigerator. Connected hub.* [online]. [cit. 18. 06. 2018]. Dostupné na internete: <https://www.samsung.com/us/explore/family-hub-refrigerator/connected-hub/>

TUNG, L. *Amazon: We're fixing flaw that leaves Key security camera open to Wi-Fi jamming.* [online]. [cit. 18. 06. 2018]. Dostupné na internete: <https://www.zdnet.com/article/amazon-were-fixing-flaw-that-leaves-key-security-camera-open-to-wi-fi-jamming/>

Kontaktné údaje:

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

Medzinárodné štandardy kvality kybernetickej bezpečnosti v Slovenskej republike

Milan Marcinek

Abstrakt:
Autor v príspevku popisuje aktuálnu situáciu v oblasti Medzinárodných štandardov kvality kybernetickej bezpečnosti v Slovenskej republike. Rozvoj a nasadzovanie informačných a komunikačných technológií otvára neustále nové bezpečnostné otázky. Štát ako taký je povinný zaisťovať ochranu informačných a komunikačných technológií, ktoré sú v pôsobnosti štátnych orgánov a orgánov samosprávy. Odolnosť sietí a stabilita informačného systému je základným predpokladom hladkého a nerušeného fungovania vnútorného trhu Európskej únie a predpokladom dôveryhodnej medzinárodnej spolupráce.
Kľúčové slová*:*
informácie, bezpečnosť, kybernetická bezpečnosť, kybernetický priestor, dáta,

Abstract:
The author describes the current situation in the field of International Cyber Security Standards in the Slovak Republic. The development and deployment of information and communication technologies opens up new security issues. The state as such is obliged to ensure the protection of information and communication technologies, which are within the competence of state authorities and self-government bodies. Resilience of networks and stability of the information system is a basic prerequisite for a smooth and uninterrupted functioning of the European Union's internal market and a prerequisite for credible international cooperation.
Key words:
information, security, cyber security, cyberspace, data,

Úvod

Počítačová, alebo Informačná bezpečnosť nie je len manažérsky proces vytvárajúci zisk, ale v súčasnosti je nevyhnutným nástrojom pre bezproblémový chod procesov, ktoré sa na vytváraní zisku priamo podieľajú. Pod pojmom zisku sa myslí nielen hmotný, ale aj nehmotný majetok spoločnosti. Náš každodenný život závisí na informačných komunikačných technológiách. Otvorený kybernetický priestor sa aktívne presadzuje na celom svete. Aby tento priestor ostal slobodný, je potrebné uplatňovať rovnaké normy, zásady a hodnoty nielen na internete, ale aj mimo neho. Pre zavedenie systému informačnej bezpečnosti, je potrebné zabezpečiť implementáciu vhodných opatrení ako sú procesy, postupy, politiky, softvérové a hardvérové funkcie.[15]

ISO - svetová normalizačná organizácia a národné technické normy

Pod skratkou ISO sa ukrýva označenie svetovej normalizačnej organizácie (International Organization for Standardization), ktorá vznikla 23. februára 1947 a ihneď uviedla do platnosti celosvetovo platné pravidlá duševného vlastníctva a obchodných normatívov. Sídlom organizácie je Ženeva vo Švajčiarsku. Hoci je ISO mimovládna organizácia, normy a dokumenty vydané v pôsobnosti ISO majú vďaka medzinárodným zmluvám a spolupráci s národnými štandardizačnými úradmi často právnu silu zákonov. ISO vydáva medzinárodné normy pod rovnakým označením ISO. V súčasnosti existuje viac ako 18000 noriem ISO. Medzinárodná organizácia pre normalizáciu má v súčasnosti 162 členov, z toho 105 riadnych členov, 47 korešpondenčných členov a 10 kandidátov na členstvo. Hoci má ISO celosvetovú pôsobnosť, jej rozšírenie je najvýznamnejšie najmä v európskych krajinách.

Možností ako uplatniť ISO normu na Slovensku je niekoľko:

[15] Pre zavedenie systému manažérstva informačnej bezpečnosti boli vytvorené medzinárodné normy (štandardy) radu ISO 27 000, ktoré špecifikujú požiadavky na riadenie informačnej bezpečnosti pre všetky typy a veľkosti organizácií.

1. Ak je príslušná technická norma dostatočne zaujímavá a jestvuje oprávnený predpoklad, že norma nájde širšie uplatnenie v slovenskej praxi, je prevzatá do sústavy Slovenských technických noriem vo forme úplného prekladu do slovenčiny. To je najzložitejší z možných spôsobov, pretože preklad normy je náročná činnosť, podliehajúca istým pravidlám. V skupine odborníkov, členov technickej komisie, ktorí ju dostanú na preklad, sa musí predovšetkým nájsť úplná zhoda v preklade názvoslovia. A po preklade jednotlivých kapitol ešte celý návrh prekladu podlieha povinnej oponentúre na jazykovednom ústave, čo mnohokrát vráti celý preklad na samý začiatok.
2. Druhým spôsobom, ako uplatniť technickú normu na Slovensku je jej prevzatie do sústavy STN bez prekladu, len s tzv. národným predhovorom. V takomto prípade zostane text samotnej normy v origináli, teda v angličtine a k norme je pridaný sprievodný dokument.
3. Tretí spôsob je začať jednoducho bezodkladne uplatňovať požiadavky príslušnej originálnej technickej normy – nezávisle od toho, či je prevzatá do sústavy STN, vzhľadom k tomu že Slovensko je aj jedným z hlasujúcich členov svetovej normalizačnej organizácie.[16]

Medzinárodné normy v oblasti kybernetickej bezpečnosti

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

Štandardy kybernetickej bezpečnosti boli vytvorené relatívne nedávno, pretože práve v posledných rokoch pribúda citlivých informácií uložených v počítačoch, ktoré sú pripojené k internetu. Tiež mnoho úloh, ktoré boli pôvodne spracovávané v papierovej forme sa dnes spracovávajú elektronicky. Zvyšuje sa ich potreba pre informačnú vierohodnosť a bezpečnosť.

Dôležitým aspektom kybernetickej bezpečnosti je ochrana pred krádežou identity. Inštitúcie a firmy majú zvýšenú potrebu k zaisteniu informačnej bezpečnosti. Narastá potreba chrániť obchodné tajomstvá, dôverné informácie a osobné údaje o zákazníkoch, zamestnancoch alebo obchodných partneroch.

V rámci kybernetickej bezpečnosti sa aplikujú normy, ktoré boli odvodené od štandardov BS 7799 vytvorených Britským štandardizačným inštitútom (BSI). Prvou je norma ISO 27 001, ktorá poskytuje model pre zavedenie efektívneho systému riadenia bezpečnosti informácií (ISMS) v organizácii a dopĺňa tak normu ISO 27 002.[17]

Medzinárodná norma ISO 27 000

ISO 27 000 je sústava medzinárodných štandardov zameraná na riadenie informačnej bezpečnosti v organizáciách. Všetky štandardy ISO 27 000 vydáva Medzinárodná organizácia pre štandardizáciu ISO. Jednotlivé štandardy cielia na rôzne aspekty informačnej bezpečnosti v organizáciách. Poskytujú praktické nástroje pre tie organizácie, ktoré chcú identifikovať a riadiť environmentálny dopad svojho správania a trvalo udržiavať a zlepšovať environmentálnu výkonnosť. Medzi hlavné normy z tejto oblasti patria:

- ISO 27 001 - hlavná norma pre Systém riadenia bezpečnosti informácií
- ISO 27 002 - zoznam najlepších praxou pre riadenie informačnej bezpečnosti
- ISO 27 003 - návod na zavedenie systému riadenia informačnej bezpečnosti (ISMS)
- ISO 27 004 - riadenia informačnej bezpečnosti - Meranie
- ISO 27 005 - návod pre riadenie informačnej bezpečnosti v organizácii (ISMS).

[16] MARCINEK, M. Legislatívna úprava v oblasti kybernetickej bezpečnosti Slovenskej republiky, Bratislava 2018, ISBN 978-80-8054-749-3.
[17] http://www.cybersecurity.cz/basic.html

- ISO 27 006 - požiadavky na audítorov a certifikačné autority informačnej bezpečnosti v organizácii
- ISO 27 007 - Informačné technológie - bezpečnostné techniky - Návod pre audit systému riadenia informačnej bezpečnosti
- ISO 27 008 - Informačné technológie - bezpečnostné techniky - Návod pre riadenie systému riadenia informačnej bezpečnosti
- ISO 27 010 - Informačné technológie - bezpečnostné techniky - Riadenie informačnej bezpečnosti pre komunikáciu vo vnútri organizácie a vo vnútri sektora
- ISO 27 011 - Informačné technológie - bezpečnostné techniky - Návod systému riadenia informačnej bezpečnosti pre telekomunikačné spoločnosti založený na ISO 27 002
- ISO 27 031 - pokyny pre pripravenosť ICT na business continuity
- ISO 27 032 - pokyny pre Cybersecurity.
- ISO 27 033 - norma zameraná na bezpečnosť sietí
- ISO 27 034 - pokyny pre bezpečnosť aplikačného softvéru
- ISO 27 035 - Informačné technológie - Bezpečnostné techniky - Riadenie incidentov informačnej bezpečnosti (Information security incident management)
- ISO 27 799 - odporúčanie k riadeniu bezpečnosti informácií vo zdravotníckych zariadeniach založený na ISO 27 002

Medzinárodná norma ISO 27 001

Norma ISO 27 001 poskytuje odporúčanie ako aplikovať ISO 27 002 v rámci procesu ustanovenia, prevádzky, údržby a zlepšovania systému riadenia bezpečnosti informácií v organizácii v súlade so systémami riadenia kvality alebo bezpečnosti prostredia. Informačná bezpečnosť je podľa medzinárodnej normy ISO 27 001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je:
- zaistenie kontinuity obchodných procesov,
- minimalizácia strát a
- maximalizácia návratnosti investícií.

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy. Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky

Predmetná norma teda popisuje vhodný systém riadenia, štruktúru a procesy pre riadenie bezpečnosti informácií podľa opatrení definovaných v ISO 27 002. Systém manažérstva informačnej bezpečnosti podľa ISO 27 001 je určený k ochrane informácií, čiže k zvládnutiu rizík, ktoré tieto informácie môžu eventuálne ohrozovať. Dôležitou súčasťou uvedenej normy je popis pre vybudovanie prevádzky systému riadenia bezpečnosti informácií. Organizácie musia realizovať analýzu rizík, aby bolo možné určiť špecificky optimálne bezpečnostné ciele a opatrenia, zaviesť ich a použiť podľa vlastných požiadaviek. Po identifikácii bezpečnostných cieľov je potrebné ich zrozumiteľne zdokumentovať pre všetky osoby v organizácii. Tieto podklady musia byť dostupné pre manažérov, zamestnancov a rovnako vybraným nezávislým stranám (interný audítori, certifikačný audítor, atď.). S

prehlbujúcou sa informatizáciou spoločnosti sú v organizáciách zavádzané zložité informačné systémy. S tým súvisí snaha organizácií chrániť si dôležité informácie, informácie partnerských organizácií a informácie zákazníkov. Systém manažérstva bezpečnosti informácií (SMIB) poskytuje celistvý model upravujúci hodnotenie rizík, návrh a zavedenie bezpečnosti informácií, riadenie bezpečnosti informácií a opätovné hodnotenie bezpečnosti informácií. Návrh a zavedenie SMIB v organizácií je podmienené potrebami a cieľmi činností organizácie a z toho vyplývajúcich požiadaviek na bezpečnosť, používanými procesmi, veľkosťou a štruktúrou organizácie. SMIB zabezpečuje primerané bezpečnostné kontroly, adekvátne chrániace informačné aktíva a poskytuje zodpovedajúcu istotu zákazníkom a iným zainteresovaným stranám. Norma ISO 27 001 je takisto ako všetky ISO štandardy medzinárodne platným štandardom. Spoločnosť, ktorá získa certifikát v jednej krajine, nemusí opäť preukazovať splnenie požiadaviek v inej krajine. Certifikáciou podľa ISO 27 001 deklaruje organizácia zabezpečenie požiadaviek systému manažérstva bezpečnosti informácií.[18]

Medzinárodná norma ISO 27 002:2013

ISO 27 002:2013 je zbierka najlepších bezpečnostných praktík a môže byť využitá ako kontrolný zoznam všetkého správneho, čo je nutné pre bezpečnosť informácií v organizácii uskutočniť. Dokument je určený vedúcim a riadiacim zamestnancom, špecialistom a odborníkom pracujúcim v oblasti bezpečnosti informačných systémov.[19]

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

Norma popisuje aj praktiky pre zaistenie bezpečnosti informácií, ktoré by organizácia mala brať do úvahy pre zaistenie kontrolných cieľov. Nová verzia normy obsahuje 113 základných opatrení, ktoré sa ďalej rozdeľujú na stovky špecifických bezpečnostných opatrení. Rozhodnutie, ktoré opatrenia sa majú aplikovať je ponechané na organizácii. Vhodné opatrenia sú vyberané na základe hodnotenia rizík a ich implementácia je závislá na konkrétnej situácii. Cieľom nie je implementovať všetko, čo norma popisuje, ale skôr naplniť všetky aplikovateľné ciele opatrení.[20]

Medzinárodná norma ISO 27 032:2012

ISO 27 032:2012 Information technology - Security techniques - Guidelines for cybersecurity znamená v preklade „Informačné technológie - Bezpečnostné techniky - Návody pre kybernetickú bezpečnosť„

Ako už z názvu vyplýva, dokument je určený vedúcim a riadiacim zamestnancom, špecialistom a odborníkom pracujúcim v oblasti bezpečnosti informačných systémov, ako odborná publikácia, obsahujúca interpretáciu prístupu k zachovaniu dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore. Pričom kybernetický priestor (cyberspace) je definovaný ako komplexné virtuálne prostredie, vyplývajúce z interakcie ľudí, softvéru a služieb na internete vykonávanej pomocou technológií, zariadení a sietí k nemu pripojených, nezávisle od ich fyzickej formy.[21]

Ďalšie právne normy SR v priestore kybernetickej bezpečnosti

Digitálny priestor Slovenskej republiky je súčasťou globálneho, celosvetového digitálneho priestoru. Vďaka vzájomnej previazanosti informačných a komunikačných technológií je nevyhnutná aj medzinárodná koordinácia ochrany globálneho digitálneho

[18] www.iso27001security.com/html/27001.html
[19] www.iso27002security.com/html/27002.html
[20] www.rac.cz/rac/homepage.nsf/CZ/27002
[21] www.iso27032security.com/html/27032.html

priestoru. Na riešenie bezpečnostných problémov digitálneho priestoru bola zriadená uznesením vlády č. 479/2009 jednotka pre riešenie počítačových incidentov (CSIRT.SK) v Slovenskej republike. Aby si táto jednotka pre riešenie počítačových incidentov mohla plniť stanovené úlohy v domácom aj medzinárodnom meradle, je potrebné legislatívne vymedziť jej kompetencie a vzťahy k ostatným štátnym orgánom Slovenskej republiky. S postupujúcou informatizáciou spoločnosti narastá počet informačných a komunikačných technológií a používateľov služieb informačnej spoločnosti. Potrebnú úroveň ochrany digitálneho priestoru nie je možné dosiahnuť bez dostatočného bezpečnostného povedomia používateľov a udržiavania primeraných znalostí tých, ktorí informačné a komunikačné technológie spravujú a rovnako aj tých, ktorí zodpovedajú za ich ochranu.

V júli 2016 bola prijatá smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“). Smernica NIS predstavuje prvú celoeurópsku legislatívnu úpravu v oblasti kybernetickej bezpečnosti, ktorá sa zameriava na posilnenie právomocí príslušných vnútroštátnych orgánov, zvyšuje ich vzájomnú koordináciu a predstavuje bezpečnostné podmienky pre kľúčové sektory. Cieľom smernice NIS je zaručiť spoločnú bezpečnosť sietí a informačných systém v rámci Európskej únie, prostredníctvom zvýšenia bezpečnosti internetu a súkromných sietí a informačných systémov, na ktorých je do značnej miery postavené fungovanie hospodárskych a spoločenských záujmov. Významným subjektom v priestore kybernetickej bezpečnosti v Európskej únii je Európska agentúra pre bezpečnosť sietí a informácií (ENISA), ktorá prispieva k zabezpečovaniu vysokého stupňa bezpečnosti a v spolupráci s európskymi krajinami vytvára spoločnú kultúru bezpečností sietí a informačných systémov v Európskej únii. Povinnosti členských štátov vyplývajúce zo smernice NIS sú nastavené na najnižšej prijateľnej úrovni nevyhnutnej k dosiahnutiu požadovanej pripravenosti a k zabezpečeniu medzištátnej spolupráce založenej na dôvere. Členské štáty môžu v rámci prijatých opatrení zohľadňovať svoje vnútroštátne špecifiká a každý členský štát v tomto smere transponuje smernicu NIS s ohľadom na reálne, skutočné riziká vyskytujúce sa v spoločnosti. Smernica NIS najmä:

- ukladá členským štátom povinnosť prijať národnú stratégiu kybernetickej bezpečnosti,
- ukladá členským štátom povinnosť určiť vnútroštátne príslušné orgány, jednotné kontaktné miesta a bezpečnostné tímy jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“),
- stanovuje sieť jednotiek CSIRT, ktorej účelom je prispievať k budovaniu dôvery medzi členskými štátmi a podporovať účinnú spoluprácu.
- zavádza bezpečnostné požiadavky a požiadavky na hlásenie kybernetických bezpečnostných incidentov pre prevádzkovateľa základných služieb (ďalej len „PZS“) a pre poskytovateľa digitálnych služieb (ďalej len „PDS“),
- ustanovuje skupinu pre spoluprácu, s cieľom podporovať strategickú spoluprácu a výmenu informácii medzi členskými štátmi a budovať vzájomnú dôveru.

Národný bezpečnostný úrad, ako ústredný organ štátnej správy pre kybernetickú bezpečnosť, pripravil na základe schváleného programového vyhlásenia vlády Slovenskej republiky na roky 2016-2020 a v súlade so schválenou Koncepciou kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a Akčným plánom realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020[22] návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“), ktorým do národného právneho poriadku transponuje smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148, Národná rada Slovenskej republiky 30. januára 2018 schválila návrh zákona pod č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

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

s účinnosťou od 25. mája 2018. Základným cieľom Zákona o kybernetickej bezpečnosti je zvýšiť bezpečnosť kybernetického priestoru a predovšetkým sa snažiť ochrániť tú časť infraštruktúry, ktorá je pre fungovanie štátu dôležitá a ktorej narušenie by viedlo k poškodeniu alebo ohrozeniu záujmov štátu. Cieľom zákona je vytvoriť ucelený, koordinovaný a efektívny systém ochrany informačných systémov Slovenskej republiky. Keďže informačné systémy sú súčasťou širšieho digitálneho priestoru, ktorého značná časť je v súkromných rukách, zákon vytvára podmienky na zvyšovanie úrovne informačnej bezpečnosti v celom digitálnom priestore Slovenskej republiky prostredníctvom štandardizácie informačnej bezpečnosti.

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

Záver

Rozvoj a nasadzovanie informačných a komunikačných technológií otvára neustále nové bezpečnostné otázky, ktoré je potrebné analyzovať a prijímať primerané riešenia ešte pred tým, ako nedostatky týchto technológií spôsobia bezpečnostné problémy pri ich používaní. Štát ako taký je povinný zaisťovať primeranú ochranu informačných a komunikačných technológií, ktoré sú v pôsobnosti štátnych orgánov a orgánov samosprávy. Kybernetická bezpečnosť je jednou zo špecifických oblastí informačnej bezpečnosti. Odborná disciplína informačná bezpečnosť sa zaoberá otázkou zaručenia dôvernosti, integrity, dostupnosti a sledovateľnosti informačných aktív všeobecne, zatiaľ čo kybernetická bezpečnosť sa venuje bezpečnosti iba určitej časti informačných aktív, ktoré sú spracúvané vo virtuálnom priestore, kybernetickom priestore. Siete a informačné systémy hrajú významnú úlohu pri slobodnom pohybe a často sú spájané internetom ako svetovým nástrojom. Narušenie siete a informačných systémov v jednom členskom štáte sa dotýka ďalších členských štátov a celej Európskej únie. Odolnosť sietí a stabilita informačného systému je základným predpokladom hladkého a nerušeného fungovania vnútorného trhu Európskej únie a predpokladom dôveryhodnej medzinárodnej spolupráce. Investovanie do kybernetickej bezpečnosti znamená investície do budúcnosti a ekonomického rastu štátu. Úroveň kybernetickej bezpečnosti je súhrnom všetkých národných a medzinárodných opatrení, ktoré boli prijaté k ochrane dostupnosti informácií komunikačných technológií a integrity, autenticity a dôvernosti dát v kybernetickom priestore.

Zoznam použitej literatúry:

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

BRVNIŠŤAN, M. *Vybrané teoretické a aplikačné výzvy kreovania vzťahu kybernetickej bezpečnosti a krízového manažmentu*. IN: Zborník z medzinárodnej vedeckej video konferencie „Kybernetická bezpečnosť ako nový prvok v realizácií opatrení krízového manažmentu“. Akadémia Policajného zboru v Bratislave , Bratislava 2018, ISBN 978-80-8054-749-3. S 22-30.

DWORZECKI, J., MARCINEK, M. *Technical Aspects of use of Selected Specialist Equipment Intended for Road-Side* Rescuing, 1. edition. New York: Iglobal Writer Inc., Pro Pomerania Foundation Poland, 2015. - 175 s. ISBN 978-83-63680-77-0.
Koncepcia kybernetickej bezpečnosti SR na roky 2015 - 2020, schválená uznesením vlády SR č. 328 zo 17.6.2015, www.nbusr.sk
MARCINEK, M. *The Current Situation in Vehicle Safety System* In: "Dani Arčibalda Rajsa" = "Archibald Reiss Days" : tematski zbornik radova medunarodnog značaja = Thematic Conference Proceedings of International Significance : Tom II = Volume II : Beograd, 10 - 11. mart 2016 = Belgrade, 10 - 11 March 2016. - Beograd = Belgrade : Kriminalističko-policijska akademija = Academy of Criminalistic and Police Studies, 2016. - ISBN 978-86-7020-357-0. - pp. 462-472.
MARCINEK, M. *Legislatívna úprava v oblasti kybernetickej bezpečnosti Slovenskej republiky*. IN: Zborník z medzinárodnej vedeckej video konferencie „Kybernetická bezpečnosť ako nový prvok v realizácií opatrení krízového manažmentu“. Akadémia Policajného zboru v Bratislave, Bratislava 2018, ISBN 978-80-8054-749-3. S 44-55.
MARCINEK, M. *Linka tiesňového volania eCall v podmienkach Slovenskej republiky/The emergency line eCall in the Slovak Republic.* In: Bezpečnostné fórum 2015. I. zväzok : zborník vedeckých prác. - Banská Bystrica : Belianum. Vydavateľstvo Univerzity Mateja Bela v Banskej Bystrici, 2015. - ISBN 978-80-557-0849-2. - S. 161-165.
OLEJÁR, D. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. 164 s. (online). Dostupné na internete: http://www.informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s
www.cybersecurity.cz/basic.html
www.govcert.cz/download/nodeid-727/
www.epravo.sk/top/clanky/zakon-o-kybernetickej-bezpecnosti758.html
www.euractiv.sk/veda-a-inovacie/kybernetickabezpecnost-na-slovensku-a-v-europe-000338/
www.isoauditor.sk/iso-iec-27001
www.iso27000security.com/html/27000.html
www.iso27032security.com/html/27032.html
www.iso27001security.com/html/27001.html
www.kiwiki.info/index.php/Syst%C3%A9m_A9rstva_informa%C4Dnej_bezpe%C4%8Dnosti
www.linuxservices.cz/kyberneticka-bezpecnost.
www.rac.cz/rac/homepage.nsf/CZ/27002
www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum187874?prefixFile=m_
www.tsoft.cz/zakon-o-kyberneticke-bezpecnosti/
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Kontaktná adresa

Ing. Milan Marcinek, PhD.
Katedra verejnej správy a krízového manažmentu
Akadémia PZ v Bratislave
milan.marcinek@minv.sk

Súčasný stav a východiská počítačovej kriminality v právnom poriadku Slovenskej republiky

Veronika Marková

Abstrakt*:*
Autorka sa v príspevku venuje trestnoprávnym otázkam počítačovej kriminality, pričom autorka článku uvádza aj vymedzenie základného pojmového aparátu vo vzťahu k počítačovej kriminalite, ako aj jej klasifikáciu. Podrobne sa venuje východiskám a dopadu medzinárodných dokumentov a právnych predpisov EU na súčasné znenie skutkových podstát trestných činov.
Kľúčové slová*:*
počítačová kriminalita, počítačové trestné činy, Dohovor o počítačovej kriminalite, Trestný zákon.

Abstract:
Author of this paper deals in the article with some question of cybercrime and the criminal law. The author of the paper also describes the definition of basic concepts of computer crime as well as its classification. The paper addresses in detail the implications and impact of international documents and EU legislation on the current wording of the facts of the offenses.
Key words:
Cybercrime, computer crime, The Convention on Cybercrime, Criminal Code

Úvod

V dnešnom svete informatizácie, počítačov a permanentného vývoja informačných technológií na úrovni komunikácie a získavania nových informácií prináša pre spoločnosť najmä podstatné zefektívnenie a zjednodušenie mnohých činností a iné pozitíva, ktoré však na strane druhej negujú riziká spojené s ich využívaním. Internet, ktorý predstavuje najdôležitejšiu sieť slúžiacu na prenos dát rôzneho obsahu a významu, slúži na komunikačné účely, obchodné účely (legálne aj nelegálne), správu rôznych oblastí, ale v neposlednom rade aj na zábavu. Všetky pozitívne vlastnosti internetových sietí sú však v poslednej dobe prevažované množstvom negatív, ktoré sú spojené ich používaním. Môžeme skonštatovať, že keď niekto prišiel s nápadom na zjednodušenie, či pomoc pri realizácii bežných každodenných spoločenských, či pracovných činností, prišiel zároveň aj niekto iný, kto využíva pozitívne vlastnosti systému na svoje vlastné negatívne činnosti, ktoré v konečnom dôsledku môžu predstavovať trestnoprávne posúdenie. Niektoré protiprávne konania, ktoré sa do určitého času realizovali len v rámci skutočného (reálneho) života, počítačové siete priniesli väčšiu anonymitu, čím sa zvýšila latentnosť páchania trestnej činnosti a minulosti boli páchatelia viac možností, ako orgány činné v trestnom konaní, nakoľko sa v tomto smere vyvíjali rýchlejšie. Spoločnosť však musela reagovať na čoraz častejšie protiprávne konania, ktorých závažnosť bola mimoriadne vysoká, a ktoré vyžívali práve pozitíva počítačových systémov a sietí na ich páchanie. Je možné skonštatovať, že práve počítačová kriminalita je najrýchlejšie sa rozvíjajúca kriminalita, ktorá rastie v priamej úmere s rozvojom počítačových sietí a zároveň staršie spôsoby páchania trestnej činnosti sa presúvajú do tohto anonymného prostredia, čím sa ešte počet trestných činov navyšuje. Veľkou výhodou počítačovej kriminality je jej sofistikovanosť a v minulosti sa stávalo, že právny poriadok nestíhal reagovať na tento typ protiprávneho konania, čo znižovalo zároveň aj objasnenosť. Z pohľadu vymedzenia určitých spoločných čŕt má počítačová kriminalita:

- globálny (nadnárodný) charakter, ktorý presahuje hranice jednotlivých štátov,
- výrazné prvky organizovanosti,
- dynamický rozvoj, ktorý je priamo úmerný dynamike vývoja počítačových technológií
- interdisciplinárny charakter, nakoľko zasahuje nielen do oblasti spoločenskej, ale aj trestnoprávnej, kriminologickej, kriminalistickej apod.,

- štruktúrovaný charakter.[1]

Dr. Kolouch vo svojom diele CyberCrime[2] poukazuje na súčasný stav v oblasti počítačových systémov a prirovnáva ich k úryvku z filmu Minority Report z roku 2002 (dej filmu sa odohráva v roku 2054), pričom hlavný hrdina prechádza obchodným centrom a dostáva ponuky, ktoré sú cielené na jeho osobu vo vzťahu k nákupu komodít rôzneho druhu, pričom tieto údaje vychádzajú z jeho zvyklostí, posledných nákupov a pod. Uvedená skutočnosť je súčasťou už dnešnej reality, kedy je každý z nás konfrontovaný s reklamou na určité výrobky v rámci našich smartofónov a počítačov (funkcia cookies[3]). Taktiež aj lokalizačné služby, v rámci ktorých naše smartfóny odosielajú informácie o konkrétnom mieste, na ktorom sa nachádzame, prípadne nás žiadajú o tieto informácie, ak na základe našej polohy zistia, kde sa nachádzame a pod.

Počítačová kriminalita a jej definovanie[4]

Kedy vlastne vznikla počítačová kriminalita? Ako forma spáchanie trestného činu vznikla súbežne so vznikom počítačov, resp. ak by sme to mali upresniť tak môžeme použiť argumentáciu autorov Smejkal a Porada, podľa ktorých počítačová kriminalita vznikla v okamihu, keď sa počítače začali meniť z matematických strojov v pôvodnom slova zmysle na mnohoúčelovo použiteľné zariadenia, ktoré boli schopné prevziať najrôznejšiu agendu.[5] Zároveň v súvislosti s tým prišiel niekto s myšlienkou, že modifikáciou programov, prípadne dát, ktoré boli spracované prostredníctvom počítača, je možno spôsobiť niekomu škodu alebo inému neoprávnený prospech.

Pojem „počítačová kriminalita“ síce existuje, ale neexistuje jednotná definícia, hoci sú snahy o jej terminologické vymedzenie. Ide o obdobný pojem ako je násilná kriminalita, kriminalita mladistvých a pod., v rámci ktorých sú definované skupiny trestných činov, ktoré svojím charakterom predstavujú najčastejšie spôsoby páchania, pričom však vzhľadom na charakter počítačovej kriminality ide o veľmi širokú skupinu trestných činov, ktoré spája jeden spoločný faktor (menovateľ) – počítačový systém. Pri vymedzovaní termínu počítačová kriminalita (kybernetická kriminalita) je potrebné brať do úvahy tú skutočnosť, že s možnosťou rasti informačných a komunikačných technológií rastie tiež možnosť ich zneužívania na páchanie trestnej činnosti. Preto v podstate neexistuje univerzálna definícia, ktorá by rozsah

[1] ROMŽA, S. Počítačová kriminalita ako spoločenský fenomén a osobitosti odhaľovania a objasňovania jej jednotlivých foriem. In. ROMŽA, S., FERENĆÍKOVÁ, S. a MICHAĽOV, L. (eds.). *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach. s. 7. ISBN 978-80-8152-146-1

[2] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC. ISBN 978-80-88168-18-8.

[3] funkcia cookies predstavuje určitý fingerprint (odtlačok) užívateľovho počítačového systému, čo predstavuje v protokole http malé množstvo stavových dát, ktoré www server posiela webovému prehliadaču počas prehliadania webovej stránky daného webového sídla, ak toto používa cookies (množné číslo od cookie). Ak sú cookies v prehliadači povolené, uložia sa na počítači používateľa, zvyčajne ako krátky textový súbor na zvolené miesto. Pri každej ďalšej požiadavke na stránku z toho istého webového sídla potom prehliadač tieto dáta posiela späť serveru, v prípade dočasných cookies len po dobu trvania aktuálnej návštevy (session), v prípade permanentných aj pri každej ďalšej návšteve. Cookies majú viaceré výhody ale môžu byť aj zneužité na nepriame sledovanie užívateľa, preto je dôležité rozumieť ich účelu, čo umožňuje zvoliť správne nastavenie prehliadača a rozhodnutie o tom či prijať alebo zamietnuť prijatie cookie v konkrétnom prípade. – Zdroj: https://sk.wikipedia.org/wiki/HTTP_cookie

[4] Termín počítačová kriminalita býva u niektorých autorov prezentovaná ako kyberkriminalita, cybercrime, a pod., čo vyplýva z anglického prekladu CyberCrime, ako aj rôznych právnych dokumentov z tejto oblasti v rámci Európskej únie. V podmienkach SR je zaužívaný termín počítačová kriminalita.

[5] SMEJKAL, V., PORADA, V. Vybrané aspekty metodiky vyšetřování kybernetické kriminality. In. ROMŽA, S., FERENĆÍKOVÁ, S., MICHAĽOV, L. (eds.). *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 64. ISBN 978-80-8152-146-1

tohto pojmu úplne pokryla. Podľa autora publikácie Cybercrime[6] je použitie pojmu „počítač" v súvislosti s touto trestnou činnosťou nevhodný pojem a pre súčasné možnosti by mal byť používaný výraz informačné a komunikačné technológie (*Information and Communication Technology* – ICT), resp. trestné činy v ICT.

Najvšeobecnejšie je možné **počítačovú kriminalitu** definovať tiež ako konanie, namierené proti počítaču, prípadne počítačovej sieti, alebo ako konanie, pri ktorom je počítač použitý ako nástroj pre páchanie trestnej činnosti, pričom základnou skutočnosťou, ktorá je v danom prípade podstatná, že prostredie, v ktorom sa trestná činnosť realizuje môžeme nazvať „kyberpriestor." Samotný pojem počítačovej kriminality však veľmi úzko súvisí aj s termínom kriminalita. Pod týmto pojmom chápeme všetky protiprávne konania, ktoré je možno kvalifikovať v zmysle ustanovení osobitnej časti Trestného zákona, čiže subsumovať pod príslušnú skutkovú podstatu trestného činu.

Po pojmom **počítačová kriminalita** môžeme chápať trestnú činnosť v rámci ktorej figuruje určitým spôsobom počítať, ako súhrn technického a programového vybavenia vrátane dát, alebo iba niektorý z jeho komponentov, prípadne väčšie množstvo počítačov samostatných alebo prepojených do počítačovej siete a to buď:

- ako **predmet** tejto trestnej činnosti, s výnimkou tej trestnej činnosti, ktorej predmetom sú popísané zariadenia ako veci hnuteľné alebo
- ako **nástroj** na páchanie trestnej činnosti.[7]

Ďalší autori[8] definujú **počítačovú kriminalitu** ako „konanie páchateľa za použitia informačnej techniky, ktorým sú naplnené znaky skutkovej podstaty počítačového trestného činu, pričom práve skupiny trestných činov počítačovej kriminality je možné vnímať ako vhodnú alternatívu pojmu počítačová kriminalita. Je však namieste spomenúť fakt, že čo bude v tejto fakt, že čo bude v tejto súvislosti považované za počítačový trestný čin.

V ďalších odborných publikáciách[9] je **počítačová kriminalita** označená ako kriminálne konanie, pri ktorom sú prostriedky informačných a komunikačných technológií použité ako:

- *nástroj na spáchanie trestného činu,*
- *cieľom útoku páchateľa, pričom tento útok je trestným činom.*

Uvedená definícia počítačovej kriminality j však stále ešte nedostatočná, nakoľko by do takejto definície spadali aj tie protiprávne konania, kedy by došlo k použitiu informačnej technológie na spáchanie trestného činu, ale nie v kontexte bežného požívania tohto systému, ale iným spôsobom – napr. by páchateľ použil monitor, počítač, či jeho iné zariadenie ako zbraň[10] a spôsobil by tým ublíženie na zdraví. Pri vyšetrovaní takéhoto druhu trestnej činnosti by sa uplatnila napr. metodika vyšetrovania napr. násilnej trestnej činnosti a nie metodika počítačovej kriminality.

Aby teda bolo možné hovoriť o počítačovej kriminalite, v takom prípade, ak sú prostriedky informačných a komunikačných technológií:

- použité ako nástroj na spáchanie trestného činu
- a zároveň sú aj cieľom útoku páchateľa pričom tento útok je trestným činom, za podmienky, že tieto prostriedky sú použité alebo zneužité *v informačnom, systémovom, programovom, či komunikačnom prostredí (čiže v kyberpriestore).*

---

[6] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC. s. 32. ISBN 978-80-88168-18-8.

[7] SMEJKAL, V., PORADA, V. Vybrané aspekty metodiky vyšetřování kybernetické kriminality. In. ROMŽA, S., FERENČÍKOVÁ, S. a MICHAĽOV, L. (eds.), 2014. *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 65. ISBN 978-80-8152-146-1

[8] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 25. ISBN 978-80-8168-538-5.

[9] Bližšie pozri tiež KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, s. 35. ISBN 978-80-88168-18-8.

[10] V zmysle § 122 ods. 3 zákona č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov – *čokoľvek, čím možno urobiť útok voči telu dôraznejší.*

Počítačová kriminalita teda nemusí byť nutne spätá s počítačom v užšom slova zmysle, ale k jej páchaniu dochádza aj pomocou obdobných technológií. Počítače sú spojené pomocou sietí, najmä vďaka tej nevýznamnejšej, a to internetu.[11] Toto prepojenie počítačov pomocou sietí vytvára takzvaný „kyberpriestor", ktorým sa rozumie určitá forma paralelného sveta vedome vytváraného užívateľom siete, takzvaný virtuálny svet.[12] Kyberpriestor, pre ktorý je vlastná jeho rýchla interakcia, zdieľanie dát, globálnosť, otvorenosť, bohatosť na informácie, sa tak stáva vhodným prostredím pre páchanie trestnej činnosti. V súvislosti so vznikom kyberpriestoru používa rada autorov pojem kybernetická kriminalita alebo v súvislosti s internetom ako súčasťou kyberpriestoru možno vymedziť pojem internetová kriminalita. Základným faktorom počítačovej kriminality je počítač, ako zariadenia rôznej povahy, ktoré sú schopné medzi sebou komunikovať v rámci kyberpriestoru.

Na základe toho, že súčasťou páchania trestnej činnosti v určitom kybernetickom prostredí, kde cieľom sú informácie, môžeme konštatovať, že termín počítačová kriminalita v tomto smere je pojem zastaraný a je potrebné hľadať vhodnejšiu alternatívu pomenovania trestnej činnosti, ktorej špecifickou črtou je to, že sa odohráva v tomto prostredí a počítač je len prostriedok na páchanie tejto trestnej činnosti. Autori Smejkal a Porada[13] ju charakterizujú aj na základe foriem a oblastí, ktoré môže táto kriminalita zasiahnuť. Ide predovšetkým o:

- „informačnú kriminalitu", ktorej cieľom sú informácie, bez ohľadu na to, akým spôsobom sú spracované a akým spôsobom sú použité na páchanie trestnej činnosti – môže ísť o rôzne útoky, pri ktorých je dôležitý obsah informácie – napr. ako je trestný čin Ohovárania podľa § 373 TZ alebo
- *Informatická kriminalita* – v uvedenom prípade ide o širšie vymedzenie pojmu počítačová kriminalita, nakoľko nástrojom, prípadne cieľom sú informačné systémy a ich komponenty (počítač, program, dáta, telekomunikácie apod.), pričom táto forma trestnej činnosti pravdepodobne najviac zodpovedá zahraničnému vymedzenie pojmu „cybercrime."

Od „klasickej" trestnej činnosti sa počítačová kriminalita odlišuje celým radom **osobitostí**. Najdôležitejšia osobitosť tohto typu kriminality je skutočnosť, že trestný čin môže byť spáchaný v priebehu niekoľkých sekúnd bez toho, aby bol páchateľ trestného činu priamo prítomný na mieste. Rovnako dôležitý prvok v tejto oblasti je aj postavenie poškodeného, ktorý sa o tejto trestnej činnosti nemusí dozvedieť v okamihu jeho spáchania. Ďalším dôležitým prvkom páchania počítačovej trestnej činnosti je aj fakt, že následkom trestného činu môžu byť veľké finančné straty, prípadne zásah do osobnostných práv poškodeného, ktoré nie je jednoduché vyčísliť v zmysle ustanovení Trestného zákona. Taktiež dôležitou súčasťou páchania trestnej činnosti v kybernetickom priestore je tiež medzinárodný rozmer, nakoľko trestná činnosť je páchaná prostredníctvom počítačovej siete, ktorá presahuje hranice jednotlivých štátov (nielen v rámci Európskej únie, ale taktiež aj v rámci celého sveta).

Rovnako je možno skonštatovať, že **neexistuje právna definícia**, ktorá by vyplývala z určitého právneho predpisu v rámci SR, medzinárodnej zmluvy, či právnych predpisov EU, hoci v jednotlivých dokumentoch môžeme nájsť zmienku o počítačovej kriminalite. Ide napr. o:

- **Manuál OSN o prevencii a kontrole trestných činov spojených s počítačom** (Havana 1990)[14] – v tejto súvislosti ide o prvý dokument, ktorý skonštatoval nejednotnosť právnej

[11] HOLCR, K. *Kriminológia,* s. 350.
[12] GŘIVNA, T. *Kyberkriminalita a právo*, s.198.
[13] SMEJKAL, V., PORADA, V. Vybrané aspekty metodiky vyšetřování kybernetické kriminality. In. ROMŽA, S., FERENĆÍKOVÁ, S., MICHAĽOV, L. (eds.). *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 66. ISBN 978-80-8152-146-1
[14] United Nations Manual on the prevention and control of computer-related crime [online]. [cit. dňa 15. 3. 2018]. Dostupné na internete:

úpravy jednotlivých krajín, v dôsledku čoho môže byť ochrana počítačových systémov a dát neefektívna, pričom ide o medzinárodný problém. Manuál skonštatoval, že počítačová kriminalita (v zmysle anglickej verzie manuálu ide o „computer crime“) je nová forma nadnárodnej kriminality a efektívne riešenie tohto problému si vyžaduje koordinovanú medzinárodnú spoluprácu, čo môže byť dodržané len pri zachovaní spoločného postupu riešenia problému.

- **Zmluva o fungovaní Európskej únie**[15] - v zmysle tohto dokumentu patrí počítačová kriminalita medzi tzv. „*európske trestné činy*“,[16] pričom však absentuje definícia tohto pojmu – počítačová kriminalita. V zmysle čl. 83 ods. 1 však vyplýva potreba harmonizácie tohto druhu trestnej činnosti.
- **Dohovor Rady Európy o počítačovej kriminalite** – (Budapešť 23. 11. 2001) uvedený názov dohovoru je všeobecne zaužívaným prekladom vo vzťahu k počítačovej kriminalite.[17] Uvedený dohovor však nevymedzuje pojem počítačovej kriminality, ale sa zamerala na opatrenia, ktoré by mali byť prijatí na vnútroštátnej úrovni. V oblasti trestného práva hmotného, ide o vymedzenie trestných činov z predmetnej oblasti.
    - **dodatkový protokol k Dohovoru** (prijatý 23. 1. 2003) rozširuje rámec trestných činov, ktoré spočívajú v šírení určitého „závadného materiálu“, pričom konkrétne ide o šírenie materiálov s rasistickým, xenofóbnym alebo iným nenávistným, prejavom.[18]

Počítačová kriminalita a jej trestnoprávne posúdenie

Z pohľadu počítačovej kriminality je teda významné miesto na páchanie trestnej činnosti kybernetický priestor, ktorý je k dispozícii užívateľom prostredníctvom internetu, ako verejnej siete, dostupnej širokému množstvu ľudí. Najdôležitejším prvkom v internetovej oblasti je informácia, ktorá v sebe zahŕňa viaceré zložky, pričom koncový užívateľ z tohto celého systému vyberie len to, čo je pre neho dôležité z pohľadu plnenia rôznych úloh. Informácia môže byť vnímaná pozitívne, čiže obsahuje prvky, ktoré majú pomáhať hľadať ďalšie riešenia, ale môže byť vnímaná aj negatívne a obsahuje prvky, ktoré nemajú slúžiť na pomoc, ale na „rozvrátenie“ užívateľa. Priestor na páchanie počítačovej kriminality je mimoriadne široký, nakoľko dnešná spoločnosť je informatizovaná a veľká väčšina činností sa realizuje prostredníctvom výpočtovej techniky, čiže jej dostupnosť je už od prvých okamihov života človeka.

Z pohľadu trestnoprávneho posúdenia počítačovej kriminality sú v súčasnosti jednotlivé krajiny závislé od vnútroštátnej legislatívy, ktorá však je ovplyvnená legislatívou Európskej únie, či iných medzinárodných orgánov (ako je napr. Rada Európy, OSN apod.) Pristupovaním k medzinárodným zmluvám sa Slovenská republika zaväzuje k prijímaniu účinných opatrení za účelom efektívneho boja proti nadnárodnej trestnej činnosti, kam počítačová kriminalita nesporne patrí. Z tohoto pohľadu môžeme práve vyzdvihnúť trestnoprávny rámec (hmotnoprávny, či procesnoprávny) jedného z najdôležitejších dokumentov v boji proti počítačovej kriminalite a to už spomínaný **Dohovor Rady Európy o počítačovej kriminalite**

---

http://216.55.97.163/wpcontent/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf pozri tiež aj KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, s. 35. ISBN 978-80-88168-18-8.

[15] Konsolidované znenie Zmluvy o Európskej únii a Zmluvy o fungovaní Európskej únie 2012/C 326/01 [online].]. [cit. dňa 15. 3. 2018]. Dostupné na internete: http://eurlex.europa.eu/legalcontent/SK/TXT/?uri=celex%3A12012E%2FTXT

[16] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 20. ISBN 978-80-8168-538-5.

[17] V rámci SR sa všeobecne zaužíval pojem počítačová kriminalita pri preklade viacerých dokumentov, či príspevkov v anglickom jazyku, pričom príkladom je aj uvedený dohovor (v anglickej verzii ide o Convention on Cybercrime), zároveň sa môžeme stretnúť aj s terminológiou „kybernetická kriminalita“, „kyberkriminalita“, „cybercrime“ „computer crime“ a pod.

[18] KOLOUCH, J. *CyberCrim*e. Praha: CZ.NIC. s. 334. ISBN 978-80-88168-18-8.

zo dňa 23. 11 2001, ktorý upravil základný právny rámec postihovania protiprávnych konaní, kde sa počítačový systém zneužíva na páchanie trestnej činnosti, pričom ide o nasledovné skupiny protiprávnych konaní:

- Trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov *(Offences against the confidentiality, integrity and availability of computer data and systems*):
  - nezákonný prístup, nezákonné zachytenie údajov, zasahovanie do údajov, zasahovanie do systému a zneužitie zariadení:
- Počítačové trestné činy (*Computer –related offences*)
  - falšovanie počítačových údajov, počítačový podvod.
- Trestné činy týkajúce sa obsahu (*Content-related offences*)– trestné činy týkajúce sa detskej pornografie.
- Trestné činy týkajúce sa porušenia autorských a príbuzných *práv (Offences related to infringements of copyright and related rights)*
- Pokus, napomáhanie a navádzanie na niektorý z uvedených trestných činov *(Ancillary liability and sanctions)*

28. januára v roku 2003 bol vyhotovený **Dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov.** Vo vzťahu k dodatkovému protokolu ide o rozšírenie skupín trestných činov o nasledovné:

- Rozširovanie a rasistických a xenofóbnych materiálov prostredníctvom počítačových systémov *(Dissemination of racist and xenophobic material through computer systems)*
- Rasisticky a xenofóbne motivované vyhrážanie *(Racist and xenophobic motivated threat*)
- Rasistické a xenofóbne motivované útoky (*Racist and xenophobic motivated insult)*
- Popieranie, znižovanie, schvaľovanie alebo ospravedlňovanie genocídia alebo zločinov proti ľudskosti (*Denial, gross minimisation, approval or justification of genocide or crimes against humanity)*[19]

Z tohto pohľadu nám teda dokument upravil skupiny trestných činov, v rámci ktorých zaviedol prvú klasifikáciu počítačovej trestnej činnosti v rámci určitého právneho predpisu.

Okrem takejto právnej klasifikácie môžeme spomenúť aj napr. jednu z prvých klasifikácií, ktorú zaviedol prof. trestného práva **Carter**, ktorý počítačovú kriminalitu roztriedil do 6. kategórií:

- **Prvá kategória** zahŕňa akcie, ako krádež informácií, krádež plánov nových produktov, krádež zoznamov zákazníkov a pod. Pre tieto akcie sa ponúka globálnejšie označenie pod pojmom priemyslová špionáž. Do tejto kategórie patrí aj vydieranie založené na informáciách získaných odcudzením súborov, napríklad z lekárskych alebo bankových serverov.
- **Druhou kategóriou** je úmyselné poškodenie dát alebo systému, neautorizované prístupy k súborom orgánov štátnej a verejnej správy za účelom modifikácie údajov, napríklad v trestnom registri alebo pre nové alebo opätovné získanie dokladov (vodičský preukaz, pas, identifikačnú kartu a pod.)
- **Tretia kategória** predstavuje akcie spojené s deštrukciou údajov, či už náhodnou alebo nie, bez presne stanoveného cieľa alebo s obyčajným pokúšaním sa o prienik do systému, len tak pre zábavu a získanie sebavedomia z úspešného pokusu o prienik, bez zámeru čokoľvek odcudziť.
- **Štvrtá kategória** zahŕňa prípady, kedy počítač slúži ako nástroj a uľahčuje prácu pri páchaní trestných činov. Patrí sem spreneverenie fondov, ktorého príkladom môže byť prípad

[19] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. crime [online]. [cit. dňa 15. 3. 2018]. Dostupné na internete: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

bývalého zamestnanca Francúzskej zdravotnej poisťovne, autora programu pre platby, ktorý spreneveril prostredníctvom tohto programu 3 milióny euro, ale aj vražda spôsobená zmenou dávkovania liekov v počítačoch nemocnice. Ďalším prípadom spadajúcim do tejto kategórie je aj prípad amerického manžela bez škrupúl, ktorý sa zo svojho počítača pripojil na počítač nemocnice, kde bola ošetrovaná jeho manželka. Prostredníctvom počítača jednoducho odpojil prístroje, ktoré udržiavali pri živote jeho ženu, a to bez toho, aby vstúpil do izby pacientky.

- **Do piatej kategórie** patria počítačové trestné činy páchané aj pomocou serverov poskytujúcich nelegálne dáta. Za najzávažnejšie je považované posielanie a šírenie stránok a obrazových dát o detskej pornografii, nacizme, rasizme a xenofóbii.
- **Šiestou kategóriou** sú takzvané „klasické" trestné činy prispôsobené novým počítačovým a komunikačným technológiám. Patria sem nelegálne kópie softvéru, fyzické krádeže hardvérových a sieťových komponentov, ale aj falšovanie a odcudzenie identity a webových stránok.[20]

Na rozdiel od náročnosti jednotnej definície pojmu sa odborná literatúra zjednotila pri rozdelení trestných činov, ktoré môžeme zaradiť medzi skupiny trestných činov počítačovej kriminality. Sú to:[21]

- trestné činy, ktorých cieľom je počítač,[22]
- trestné činy, pri ktorých sa počítač používa ako nástroj na ich spáchanie,[23]
- trestné činy, pri ktorých má počítač len vedľajšiu príležitostnú úlohu pri ich páchaní.[24] [25]

Jednotlivé spôsoby páchania trestnej činnosti v zmysle terminológie informačných technológií môžeme zaradiť:

- **Hacking** – ide o najstarší spôsob páchania počítačovej kriminality, ktorý spočíva v preniknutí do počítačového systému
- **Cracking** – obchádzanie ochranných prvkov počítačového programu alebo systému v úmysle ich neoprávnen používať
- **Warez** – (linking) – najčastejšie v súvislosti s porušovaním autorských práv
- **Torrent**-y – taktiež ide najčastejšie o porušovanie autorských práv
- Malware – ide o škodlivý softvér, ktorý negatívne zasahuje do chodu počítačov. Ide predovšetkým o počítačové vírusy, trojské kone, či spyware
- **Phishing / pharming** – ide o zavádzajúce, podvodné praktiky, na základe ktorých sú od užívateľov vylákané citlivé osobné údaje
- **Sniffing** – cieľom je neoprávnené zachytávanie údajov od užívateľov internetu,
- **Skimming** – neoprávnené kopírovanie údajov z prúžku platobnej karty.[26]

Základný právny rámec postihovania trestnej činnosti v súvislosti s počítačovou kriminalitou v rámci EU

Vzhľadom ku skutočnosti, že počítačová kriminalita zasahuje svojím charakterom viaceré členské krajiny EU, bolo potrebné prijímať účinné opatrenia, aby sa zabezpečila

[20] KOSTRECOVÁ, E., JOKAY, M., KOSTREC, M. *Počítačová kriminalita*. Bratislava: Slovenská technická univerzita v Bratislave, s. 2. ISBN 978-80-227-3410-3.

[21] BRENNER, S. W. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger, 2010, s. 39.

[22] V tomto prípade páchateľ prenikol do počítača za účelom krádeže dát, súborov, dokumentov. Dochádza k „hackerstvu" alebo „pirátstvu".

[23] Počítač je tu akýsi pomocník na uľahčenie trestného činu, napr. falšovanie peňazí, úradných listín, výroba detskej pornografie, nelegálne kópie CD, DVD nosičov.

[24] V tomto prípade počítač zohráva malú úlohu, napr. napísanie vydieračského alebo výhražného listu.

[25] BENEDEKOVÁ, D. Právna úprava počítačovej kriminality. In: MARKOVÁ, V. ed. *Aktuálne otázky trestného práva v teórii a praxi: Zborník príspevkov z 4. roč. interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou.* Bratislava: Akadémia Policajného zboru v Bratislave, s. 20 – 26. ISBN 978-80-8054-682-3.

[26] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 29-52. ISBN 978-80-8168-538-5.

efektívna spolupráca a zároveň postih páchateľov počítačovej kriminality. Základný prostriedok pre zjednocovanie práva jednotlivých členských krajín EU sú predovšetkým rámcové rozhodnutia, smernice, prípadne ďalšie dokumenty EU. Z pohľadu počítačovej kriminality ide predovšetkým o uvedené dokumenty:

- Rámcové rozhodnutie Rady 2001/413/SVV z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov
- Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV
- Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV
- Smernica Európskeho parlamentu a Rady 2009/24/ES z 23. apríla 2009 o právnej ochrane počítačových programov (kodifikované znenie) (Ú. v. EÚ L 111, 5. 5. 2009).

Rámcové rozhodnutie Rady 2001/413/SVV z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov (Mimoriadne vydanie Ú. v. EÚ, kap. 15/zv. 6; Ú. v. ES L 149, 2. 6. 2001).

V zmysle uvedeného rámcového rozhodnutia sa členské krajiny zaväzujú prijať potrebné opatrenia na zabezpečenie toho, aby sa konanie považovalo za trestný čin, ak je spáchané úmyselne, pričom ide o trestné činy ktoré sa dotýkajú nasledovných kategórií:

- Platobných nástrojov – v tomto smere ide predovšetkým o kreditné karty, eurošekové karty, karty vydávané finančnými inštitúciami a pod.
- Počítačov a zvláštne upravených zariadení.

Právna úprava vo vzťahu k uvedenému Rámcového rozhodnutiu sa dotýka predovšetkým trestného činu v zmysle **§ 219 TZ - Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty**. Uvedeného trestného činu sa dopustí ten kto:

1) 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, potrestá sa odňatím slobody na jeden rok až päť rokov.
2) neoprávnene vyrobí, prechováva, obstará si alebo inak zadováži alebo poskytne inému nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v odseku 1, potrestá sa odňatím slobody až na tri roky.

Objektom trestného činu je vlastnícke právo, najmä výkon vlastníckeho práva slúžiaci na využívanie platobných prostriedkov vymenovaných v tomto ustanovení, ale zároveň objektom sú aj bezhotovostné platobné prostriedky zaisťujúce platobný styk.

Medzi okolnosti, ktoré podmieňujú požitie vyššej trestnej sadzby patria spáchanie trestného činu závažnejším spôsobom konania, vo väčšom rozsahu a z osobitného motívu, pričom ešte prísnejšie sa páchateľ potrestá, ak spácha čin vo veľkom rozsahu, prípadne ako člen nebezpečného zoskupenia

Uvedené ustanovenie bolo novelou č. 492/2009 Z. z. upravené a pojem „elektronický platobný prostriedok“ sa nahradil pojmom upraveným v zákone o platobných službách a to „platobný prostriedok a elektronické peniaze“.

Uvedený trestný čin svojím charakterom patrí medzi trestné činy, pri ktorých sú prvky informačných a komunikačných technológií terčom útoku páchateľa (ods. 1), ale zároveň ak trestným činom, pri ktorom sú informačné a komunikačné technológie použité ako nástroj, ktorý umožňuje spáchanie takéhoto trestného činu (ods. 2).

Právnická osoba sa ho dopustiť nemôže.

Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14. 8. 2013).

Uvedená smernica je základným právnym nástrojom ochrany proti útokom na informačné systémy, pričom táto smernica stanovuje minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti týchto útokov ako aj zlepšenie spolupráce medzi príslušnými orgánmi. Uvedená Smernica svojím charakterom nadväzuje na Dohovor Rady Európy o počítačovej kriminalite z roku 2001, ktorý je na medzinárodnej úrovni považovaný za najkomplexnejšiu medzinárodnú normu, keďže poskytuje komplexný a ucelený rámec zahŕňajúci viaceré aspekty počítačovej kriminality, pričom sa táto skutočnosť uvádza aj priamo v Smernici.

Na základe týchto spomínaných aktov sa právna úprava trestných činov, ktoré súvisia s útokom na informačné a komunikačné technológie zmenila novelou Trestného zákona – zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov s účinnosťou od 1. 1. 2016.

Medzi trestné činy, ktoré svojím charakterom patria medzi trestné činy, ktoré útočia na informačné a komunikačné technológie, môžeme zaradiť predovšetkým:

§ 226 Neoprávnené obohatenie

1) *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.*

V danom prípade ide o právnu úpravu z roku 1999, pričom v rámci rekodifikácie, prešlo ustanovenie len malou nevýraznou zmenou a v toto znení je účinné aj v súčasnosti.

Objektom trestného činu je vlastnícke právo v súvislosti s automatizovaným predajom tovaru, s automatizovaným poskytovaním platených výkonov, služieb, informácií či iných plnení alebo automatizovaným výberom peňazí. Objektívna stránka spočíva v tom, že páchateľ seba alebo iného na škodu cudzieho majetku obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia dosiahne neoprávnene určitú výhodu (tovar, služby alebo informácie získa bez požadovanej úhrady, alebo získa peniaze) a tým na cudzom majetku spôsobí malú škodu.

Medzi okolnosti, ktoré podmieňujú požitie vyššej trestnej sadzby patrí spôsobenie väčšej škody, spáchanie trestného činu z osobitného motívu, prípadne závažnejším spôsobom konania a prísnejšie sa páchateľ potrestá, ak činom spôsobí značnú škodu, prípadne škodu veľkého rozsahu a tiež aj ako člen nebezpečného zoskupenia, či za krízovej situácie.

Z pohľadu aplikačnej praxe ide najčastejšie o zneužívaní tzv. výherných automatov, či neoprávnené zásahy do telefónnych automatov. Taktiež aj niektoré súdy v rámci svojej rozhodovacej činnosti neoprávnené používanie SIM karty posudzujú ako tento trestný čin a niektoré súdy ako trestný čin v zmysle § 219 TZ. Taktiež niektoré súdy to kvalifikujú ako súbeh týchto dvoch trestných činov

Právnická osoba sa ho dopustiť nemôže

Pravdepodobne najväčší zásah do právnej úpravy trestných činov počítačovej kriminality majú ustanovenia **§ 247 - § 247d.** Ide práve o spomínanú novelu TZ (zákon č. 398/2015 Z. z.), ktorou sa vykonáva transpozícia smernice 2013/40/EÚ do právneho poriadku Slovenskej republiky a to doplnením a rozšírením existujúcej trestnoprávnej úpravy v oblasti počítačovej kriminality. Súčasne boli novou úpravou zo skutkových podstát trestného činu porušovania tajomstva prepravovaných správ podľa § 196 a nasledujúcich Trestného

zákona vyňaté konania týkajúce sa prenosu informácií prostredníctvom elektronickej komunikačnej služby a prenosu počítačových údajov v rámci počítačového systému, ktoré boli doplnené do nového ustanovenia, ktorým sa definuje trestný čin neoprávneného zachytávania počítačových údajov v novonavrhovanom § 247c. Novo navrhovaná systematika trestných činov týkajúcich sa počítačovej kriminality sleduje požiadavky smernice kladené na členské štáty Európskej únie v oblasti monitorovania a zberu štatistických údajov o tomto druhu trestnej činnosti v zmysle čl. 14 smernice. Z tohto dôvodu sa navrhuje systematiku trestných činov týkajúcich sa počítačovej kriminality zosúladiť so systematikou predstavenou v smernici, ktorá vychádza z Dohovoru Rady Európy o počítačovej kriminalite. (ozn. č. 137/2008 Z. z.)

V zmysle novej právnej úpravy sa teda za počítačové trestné činy považujú:

- § 247 - Neoprávnený prístup do počítačového systému,
- § 247a - Neoprávnený zásah do počítačového systému,
- § 247b - Neoprávnený zásah do počítačového údaja
- § 247c - Neoprávnené zachytávanie počítačových údajov
- § 247d - Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov

V zmysle zákona č. 91/2016 Z. z. môže byť páchateľom všetkých týchto trestných činov aj právnická osoba, ak spĺňa podmienky stanovené týmto zákonom vo vzťahu k trestnej zodpovednosti.[27]

§ 247 - Neoprávnený prístup do počítačového systému

1) Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.

V súvislosti s transpozíciou smernice EP a Rady 2013/40/EÚ sa modifikovala existujúca právna úprava skutkovej podstaty trestného činu zneužitia záznamu na nosiči informácií podľa § 247 Trestného zákona. Pôvodná právna úprava síce tiež vychádzala z medzinárodných dokumentov (predovšetkým z Dohovoru o počítačovej kriminalite), ale najnovšou úpravou sa právna úprava precizovala a rozdelila v zmysle rôznych protiprávnych konaní do viacerých trestných činov.[28] Individuálnym objektom trestného činu je v tomto prípade ochrana počítačového systému ako celku alebo akejkoľvek jeho časti, pričom trestná zodpovednosť páchateľa je podmienená prekonaním bezpečnostného opatrenia. Získaním prístupu do počítačového systému sa rozumie akékoľvek konanie, ktoré páchateľovi umožní neoprávnenú dispozíciu počítačovým systémom, resp. jeho časťou a využitie jeho informačného obsahu. Z hľadiska subjektívnej stránky sa vyžaduje úmyselné zavinenie. Trestný čin neoprávneného prístupu do počítačového systému je vo svojej základnej skutkovej podstate prečinom.

Z pohľadu prísnejšieho postihu je páchateľ trestne zodpovedný, ak spôsobí svojím protiprávnym konaní značnú škodu, prípadne škodu veľkého rozsahu alebo ako člen nebezpečného zoskupenia.

---

[27] § 4 zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov

[28] Pôvodné znenie § 247 Poškodenie a zneužitie záznamu na nosiči informácií - (1) Kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a a) jeho informácie neoprávnene použije, b) také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, c) urobí zásah do technického alebo programového vybavenia počítača, alebo d) vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo, potrestá sa odňatím slobody na šesť mesiacov až tri roky.
(2) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1 a) neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo b) zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

§ 247a - Neoprávnený zásah do počítačového systému

1) Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti

a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo

b) tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,

potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Táto skutková podstata zakladá trestnú zodpovednosť páchateľa, ktorý obmedzí alebo preruší fungovanie počítačového systému prostredníctvom manipulácie s počítačovými údajmi, t. j. ich neoprávneným vložením, prenosom, poškodením, vymazaním, zhoršením ich kvality, pozmenením, potlačením alebo ich zneprístupnením, alebo neoprávnenou manipuláciou s tzv. hardwarovým alebo softwarovým vybavením počítača. Počítačom sa v zmysle tohto ustanovenia rozumie každá funkčná jednotka, ktorá môže vykonávať výpočty všetkých číselných aritmetických a logických operácií bez ľudského zásahu a podľa určitého programu.[29] **Objektom** trestného činu je obdobne ako v predchádzajúcom ustanovení integrita počítačového systému ako celku, resp. akejkoľvek jeho časti, ako aj jeho riadne fungovanie.

Technickým vybavením počítača (tzv. hardware) sa rozumejú všetky technické prostriedky umožňujúce funkciu a využite počítača vrátane jeho príslušenstva, t.j. tlačiareň, polohovacie zariadenie (myš), plotter, skener, modem a pod. Programové vybavenie počítača (tzv. software) tvoria programy, procedúry, pravidlá a príslušná dokumentácia systému spracovania informácií (systémový software a aplikačný software). Zásahom do technického alebo programového vybavenia sa rozumie akékoľvek neoprávnené konanie vo vzťahu k týmto predmetom. Marenie funkčnosti počítačového systému je fakticky deštrukcia pôvodných počítačových dát niektorou z foriem uvedených v tomto ustanovení. Na trestnosť páchateľa stačí, ak koná niektorým z uvedených spôsobov, pričom v istých prípadoch môže ísť aj o kumuláciu týchto spôsobov konania. Z hľadiska subjektívnej stránky sa vyžaduje úmyselné zavinenie.

Prísnejšie sa páchateľ bude posudzovať ak spácha takýto čin a spôsobí ním značnú škodu, prípadne škodu veľkého rozsahu, či ako člen nebezpečného zoskupenia, ale taktiež ak spôsobí vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci, či tak, že zneužije osobné údaje iného s cieľom získať dôveru tretej strany, či vážnu poruchu v kritickej infraštruktúre.

§ 247b - Neoprávnený zásah do počítačového údaja

1) Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Uvedená skutková podstata kriminalizuje neoprávnené poškodenie, vymazanie, potlačenie, zneprístupnenie alebo zhoršenie kvality počítačových údajov, ktoré ako širší pojem zahŕňajú aj počítačové informácie. Počítačové údaje predstavujú interpretovateľnú a formalizovanú reprezentáciu informácie vhodnej na komunikáciu, interpretáciu alebo spracovanie. Na trestnosť páchateľa stačí, ak koná niektorým z uvedených spôsobov, pričom v istých prípadoch môže ísť aj o kumuláciu týchto spôsobov konania. **Objektom trestného činu** riadna ochrana počítačového údaja ako citlivej a zneužiteľnej informácie, do ktorej je neoprávnený zásad neakceptovateľný.[30]

V tejto súvislosti je potrebné podotknúť, že zákonodarca pri tomto trestného čine v zmysle skutkovej podstaty opomenul slovko neoprávnene (zachoval ho len v názve), čo práve

[29] Dôvodová správa k návrhu zákona č. 398/2015 Z. z.

[30] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 173. ISBN 978-80-8168-538-5.

zdôrazňuje Smernica a zároveň aj Dohovor, že ide o neoprávnené zásahy. Je preto vhodné *de lege ferenda* riešiť otázku zmeny tohto ustanovenia v kontexte iných trestných činov počítačovej kriminality.[31]

Z hľadiska subjektívnej stránky sa vyžaduje úmyselné zavinenie, ktoré je v prípade tohoto trestného činu zdôraznené (hoci z pohľadu konštrukcie skutkovej podstaty z hľadiska zavinenia v zmysle § 17 TZ to nie je potrebné).[32]

Okolnosti, ktoré podmieňujú požitie vyššej trestnej sadzby sú podobné ako pri predchádzajúcom trestnom čine.

§ 247c - Neoprávnené zachytávanie počítačových údajov

1) *Kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody na šesť mesiacov až tri roky.*
2) *Kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody na jeden rok až päť rokov.*

Uvedený novo koncipovaný trestný čin nie je novým ustanovením Trestného zákona, nakoľko v znení TZ účinného do 31. 12. 2015 boli čiastočne tieto protiprávne konania vyjadrené v § 196 - § 198 (Porušovanie tajomstva prepravovaných správ) v kombinácii v predchádzajúcim znením § 247. Z pôvodného znenia boli vyňaté konania týkajúce sa prenosu informácií prostredníctvom elektronickej komunikačnej služby a prenosu počítačových údajov v rámci počítačových systémov, resp. skutková podstata § 198 bola zrušená, pričom touto zmenou sa sledovalo zjednotenie právnej úpravy vo vzťahu k trestnej činnosti týkajúcej sa informačných a komunikačných technológií.

Individuálnym **objektom** tohto trestného činu je ochrana tajomstva informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo tajomstva neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci. Spôsobenie škody sa v základnej skutkovej podstate nevyžaduje, no v prípade, že páchateľ spôsobí značnú škodu, alebo škodu veľkého rozsahu ide o okolnosti, ktoré podmieňujú použitie vyššej trestnej sadzby. Taktiež medzi tieto môžeme zaradiť aj spáchanie trestného činu z osobitného motívu, závažnejším spôsobom konania, prípadne ako člen nebezpečného zoskupenia.

§ 247d - Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov

1) *Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní*
   a) *zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo*
   b) *počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti,*
2) *potrestá sa odňatím slobody až na dva roky.*

---

[31] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 176. ISBN 978-80-8168-538-5.

[32] Úmyselné zavinenie sa zvykne v zmysle trestného práva zdôrazňovať v prípadoch, že existuje skupina podobných trestných činov z hľadiska objektu a objektívnej stránky, ktoré sa od seba odlišujú len formou zavinenia – napr. vražda (kto iného úmyselne usmrtí) a usmrtenie (kto inému z nedbanlivosti spôsobí smrť).

Z pohľadu vytvorenia tejto novej skutkovej podstaty trestného činu je možné skonštatovať, že rôzne softvéry, heslá, prístupové kódy, či iné nástroje používané na páchanie počítačovej kriminality predstavujú veľmi výnosné nelegálne obchody. **Objektom** tohto trestného činu je zabezpečenie riadneho fungovania a ochrana počítačového systému ako celku alebo akejkoľvek jeho časti v dôsledku možného ohrozenia v súvislosti s distribúciou, či držbou prostriedkov, ktorými sa neoprávnene zasahuje do tohto systému.

Zariadením sa rozumie akékoľvek technické zariadenie umožňujúce neoprávnený prienik do počítačového systému alebo jeho časti. Počítačovým programom sa v tomto prípade rozumie napr. aj tzv. "škodlivý software" (malware), ktorý ovláda funkcie počítača a môže sa aktivizovať na základe použitia USB, resp. E mailu. Počítačové heslo je súbor niekoľkých znakov, ktoré môžu tvoriť kombinácia čísel, písmen a špeciálnych znakov tak, aby toto bolo ťažko zistiteľné. Prístupový kód slúži na automatizáciu v postupe užívateľa pri jeho prístupe do určitej služby, ktorý býva spravidla jednorazový a nemusí byť len číselný, ale môže byť vytvorený aj formou určitého obrazu (ide napr. o PIN kód).

Z pohľadu precizovania skutkovej podstaty by bolo možné do budúcnosti v zmysle návrhov *de lege ferenda* uvažovať podobne ako pri § 247b a zdôrazniť protiprávnosť konaní vymedzených v tomto ustanovení.

Okolnosťami podmieňujúcimi použitie vyššej trestnej sadzby je spôsobenie značnej škody alebo škody veľkého rozsahu, alebo je páchateľ členom nebezpečného zoskupenia.

Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17. 12. 2011).

V rámci trestnej činnosti, pri ktorej sú prostriedky informačných a komunikačných technológií použité ako prostriedok na spáchanie trestného činu je nevyhnutné zdôrazniť úlohu tejto Smernice, ktorá predstavuje na úrovni EU hlavné legislatívne opatrenie harmonizujúce sexuálne zneužívanie detí a detskú pornografiu pre jednotlivé členské štáty. Smernica stanovuje minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti sexuálneho zneužívania a sexuálneho vykorisťovania detí, detskej pornografie a oslovovania detí na sexuálne účely**.** Uvedená trestná činnosť je vo vzťahu k počítačovej kriminality mimoriadny problémom, nakoľko používaním nových technológií a internetu táto trestná činnosť narastá a rozširuje sa.

Právna úprava tejto trestnej činnosti bola aj v skoršom znení Trestného zákona upravená, pričom však novelou Trestného zákona – zákonom č. 204/2013 Z. z., ktorou sa do nášho právneho poriadku transponovala uvedená smernica, sa právna úprava zmenila a precizovala. Za základe smernice boli vytvorené kategórie trestných činov a to:

- Trestné činy súvisiace so sexuálnym zneužívaním
- Trestné činy súvisiace so sexuálnym vykorisťovaním
- Trestné činy súvisiace s detskou pornografiou
- Kontaktovanie detí na účely ich sexuálneho zneužitia

Medzi protiprávne konania, pri ktorých sa výrazne využívajú informačné a komunikačné technológie na spáchanie trestného činu je predovšetkým vedomé získavanie prístupu k detskej pornografii prostredníctvom týchto technológií, pričom ide o protiprávne konania, ktoré súvisia s detskou pornografiou. Osobitnou kategóriou je kontaktovanie detí na účely ich sexuálneho zneužitia, pričom práve pri takýchto protiprávnych konaniach sú počítačové siete prostriedkom na vytváranie vhodného priestoru, nakoľko páchateľ získava určitú anonymitu a môže zatajovať svoju skutočnú identitu a osobnostné vlastnosti.

V zmysle ustanovení Trestného zákona má uvedená smernica odraz predovšetkým pri trestných činoch týkajúcich sa detskej pornografie, pričom je možné konštatovať, že právna úprava účinná do novely TZ vo vzťahu k detskej pornografii, ktorá by mohla byť páchaná

prostredníctvom informačných a komunikačných technológií bola pomerne dobre upravená a novelou sa precizovala a upravila. Trestné činy, ktoré môžu byť spáchané prostredníctvom informačných a komunikačných technológií vo vzťahu k tejto smernici sú:

- § 368 - Výroba detskej pornografie
- § 369 - Rozširovanie detskej pornografie
- § 370 - Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení,
- § 201a - Sexuálne Zneužívanie - kontaktovanie detí prostredníctvom elektronickej komunikačnej služby na účely ich sexuálneho zneužitia

Všetkých trestných činov sa môže dopustiť aj právnická osoba

Vo vzťahu k novele TZ bola upravená definícia detskej pornografie - § 132 ods. 4 TZ - ide o *„zobrazenie skutočnej alebo predstieranej súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku s dieťaťom alebo osobou vyzerajúcou ako dieťa alebo zobrazenie obnažených častí tela dieťaťa alebo osoby vyzerajúcej ako dieťa smerujúce k vyvolaniu sexuálneho uspokojenia inej osoby.“* Nový pojem sa v tomto prípade rozšíril aj o protiprávne konanie, ktorým sa len predstiera určitý sexuálny styk s dieťaťom, ako aj protiprávne konanie, pri ktorom osoba predstiera, že je dieťa, aj napriek tomu, že je staršia ako 18 rokov.

Výroba[33] a rozširovanie[34] detskej pornografie v zmysle § 368 a § 369 sú trestné činy, proti ktorých sa informačné a komunikačné technológie používajú ako nástroj na zaznamenávanie a prípadnú úpravu, ako aj následné rozširovanie prebieha za ich použitia (kopírovaním, ukladaním na DVD nosiče, USB a pod, prípadne rozširovanie prostredníctvom siete). Zároveň sa ustanovenia § 368 dotýka aj zneužitia dieťaťa na účel výroby detského pornografického predstavenia. V zmysle § 132 ods. 5 TZ sa ním rozumie „*živé predstavenie určené publiku, a to aj s využitím informačno-technických prostriedkov, v ktorom je dieťa zapojené do skutočného alebo predstieraného sexuálneho konania alebo v ktorom sú obnažované časti tela dieťaťa smerujúce k vyvolaniu sexuálneho uspokojenia inej osoby*.“

§ 370 - Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení

1) *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.*
2) *Rovnako ako v odseku 1 sa potrestá, kto sa úmyselne zúčastní detského pornografického predstavenia.*

Výrazne sa novela dotkla ustanovenia § 370 TZ, ktorej skutkový podstata sa rozšírila o konanie páchateľa, ktorý koná v úmysle získať prístup k detskej pornografii prostredníctvom elektronickej komunikačnej siete. Ide o také konanie ktoré preukázateľne smeruje k vedomému, teda nie nevyžiadanému/náhodnému získaniu prístupu k detskej pornografii, t. j. najmä vykonaním registrácie, odoslaním požiadavky na prístup, alebo uhradením platby za prístup na internetovú stránku s detskou pornografiou. Ide o protiprávne konanie, kde prostriedky informačných a komunikačných technológií sú hlavným prostriedkom na páchanie trestného činu. Vo vzťahu k úmyslu získať prístup k detskej pornografii musí osoba mať v úmysle otvoriť si stránku s detskou pornografiou a zároveň vedieť, že sa práve na tejto stránke nachádzajú príslušné vyobrazenia. V prípade nedbanlivostného zavinenia sa nepredpokladá trestné stíhanie za tento trestný čin.

[33] 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.

[34] Kto rozmnožuje, prepravuje, zadovažuje, sprístupňuje alebo inak rozširuje detskú pornografiu, potrestá sa odňatím slobody na jeden rok až päť rokov.

Opatrenia Európskej únie však smerovali aj k právnickým osobám, ktoré by taktiež mali niesť zodpovednosť v prípade, že sa dopustia trestných činov z tejto oblasti, prípadne nebudú realizovať dostatočnú kontrolu, čím sa umožní páchanie takejto trestnej činnosti. Ide predovšetkým o prevádzkovanie internetových stránok, kde sa takýto obsah môže nachádzať, prípadne komunikačné služby zamerané na tento spôsob komunikácie s cieľom získať snímky, či záznamy s takýmto obsahom. Je však potrebné zdôrazniť, že servery takýchto internetových stánok sú umiestnené v tretích krajinách, ktoré nechcú spolupracovať. Snahy by v takýchto prípadoch mali byť zamerané na zablokovanie takýchto internetových stránok. V súvislosti s trestnoprávnou zodpovednosťou právnickej osoby už aj Slovenská republika prijala zákon, za základe ktorého už aj právnickú osobu je možné trestne stíhať za trestné činy, pričom medzi tieto sú zaradené viaceré trestné činy vzťahujúce sa na ochranu detí, ako je napr. sexuálne zneužívanie, či obchodovanie s ľuďmi.

§ 201a – Sexuálne zneužívanie - nová skutková podstata trestného činu vo vzťahu k počítačovej kriminalite.

„Kto prostredníctvom elektronickej komunikačnej služby navrhne dieťaťu mladšiemu ako 15 rokov osobné stretnutie v úmysle spáchať na ňom trestný čin sexuálneho zneužívania alebo trestný čin výroby detskej pornografie, pričom sám nie je dieťaťom, potrestá sa odňatím slobody na šesť mesiacov až tri roky.“

Uvedená skutková podstata súvisí s čl. 6 Smernice[35], ako aj s Dohovorom Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním[36], ktorý bol prijatý Výborom ministrov Rady Európy v Lanzarate dňa 25. 10. 2007 a ktorý Slovenská republika podpísala dňa 9. 9. 2009. Cieľom dohovoru je zabezpečiť ochranu práv dieťaťa pred sexuálnym vykorisťovaním a zneužívaním a trestnosť takéhoto konania zo strany štátov ako zmluvných strán tejto multilaterálnej zmluvy, a to prostredníctvom prijatia účinných opatrení v rámci ich vnútroštátneho práva. Dohovor podpísal prezident Andrej Kiska dňa 27.1.2016, pričom pre Slovenskú republiku nadobudne platnosť 1. júla 2016.

Vo vzťahu k tomuto trestnému činu TZ neobsahuje názov, ale priraďuje ho k trestnému činu sexuálneho zneužívania. V tomto smere neexistuje ani jednotná definícia názvu trestného činu v zmysle Smernice a v zmysle uvedeného Dohovoru (v zmysle slovenského ekvivalentu). Smernica totiž uvádza – „kontaktovanie detí na účely ich sexuálneho zneužitia“ a dohovor (jeho slovenský ekvivalent „navádzanie detí na sexuálne účely“ Anglický ekvivalent je v tomto prípade rovnaký – „*Solicitation of children for sexual purpose.“*[37]

Subjektom tohto trestného činu môže byť len osoba, ktorá sama nie je dieťaťom.[38] Z pohľadu vyvodzovania trestnej zodpovednosti z hľadiska veku teda zákonodarca stanovuje nové vymedzenie subjektu pri tomto trestnom čine, čiže osoba, ktorá sama nie je dieťaťom.

V zmysle protiprávneho konania ide teda o návrh dospelej osoby, ktorý bude realizovaný pomocou informačných a komunikačných technológií (rôzne online chaty, prípadne facebook a podobné stránky), posudzovať ako trestný čin, pričom je nevyhnutné stanoviť hranicu trestnej sadzby najmenej na jeden rok. Je však potrebné zdôrazniť, že takémuto protiprávnemu konaniu musia nasledovať faktické činy, ktoré by viedli k takémuto stretnutiu.[39] Právna úprava SR však túto požiadavku neuvádza a zmysle objektívnej stránky by stačilo na naplnenie len kontaktovanie prostredníctvom správy s návrhom na osobné stretnutie v úmysle, ktoré predpokladá skutková podstata, pričom v obsahu samotnej správy ani nemusí

[35] Kontaktovanie detí na účely ich sexuálneho zneužitia.

[36] Článok 23 – Navádzanie detí na sexuálne účely.

[37] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 274. ISBN 978-80-8168-538-5

[38] Za dieťa sa považuje osoba mladšia ako 18 rokov, ak tento zákon neustanovuje inak. - § 127 ods. 1 TZ

[39] Uvedená konštatácia, ktorá vychádza zo Smernice, ako aj z Dohovoru však nie je súčasťou objektívnej stránky skutkovej podstaty tohto trestného činu, pre trestnosť v zmysle slovenskej právnej úpravy stačí, že páchateľ správu odošle.

byť tento úmysle vyjadrený, čo môže následne spôsobiť nárast tejto trestnej činnosti. Z môjho pohľadu by bolo efektívnejšie, aby sa právna úprava upravila v zmysle Smernice[40] a súčasťou objektívnej stránky skutkovej podstaty trestného činu by mala byť aj skutočnosť, že po tomto návrhu nasledovali faktické činy vedúce k takémuto stretnutiu (sexuálnemu). Je však nevyhnutné zdôrazniť aj to, že takýto typ úmyslu, ako obligatórneho znaku skutkovej podstaty trestného činu, je následne veľmi ťažké páchateľovi aj dokázať.

Ďalšia skutková podstata v zmysle § 201b ktorá vyplynula z návrhu zákona č. 204/2013 Z. z. sa už nedotýka trestnej činnosti, ktorá je spájaná s informačnými a komunikačnými technológiami.

Smernica Európskeho parlamentu a Rady 2009/24/ES z 23. apríla 2009 o právnej ochrane počítačových programov (kodifikované znenie) (Ú. v. EÚ L 111, 5. 5. 2009).

Vzhľadom ku skutočnosti, že existovali určité rozdiely v právnej úprave členských štátov EU vo vzťahu k právnej ochrane počítačových programov, uvedená smernica mala za cieľ harmonizovať tieto vnútroštátne predpisy, aby bolo možné zefektívniť boj proti ich neoprávnenému rozmnožovaniu. Počítačový program zahŕňa programy v akejkoľvek forme vrátane tých, ktoré sú včlenené do technického vybavenia počítača (hardvéru). Tento pojem zahŕňa aj prípravnú koncepčnú prácu vedúcu k vyvinutiu počítačového programu pod podmienkou, že na základe jej povahy bude možné v neskoršom štádiu vytvoriť počítačový program. Počítačový program je chránený, ak je pôvodný v tom zmysle, že je autorovým vlastným duševným výtvorom.[41]

V zmysle právneho poriadku SR ide o oblasť, ktorá je primárne upravená zákonom č. 185/2015 Z. z. Autorským zákonom v znení neskorších predpisov, ktorý stanovuje v § 87[42], že *„počítačový program, ktorým je súbor príkazov a inštrukcií vyjadrených v akejkoľvek forme použitých priamo alebo nepriamo v počítači alebo v podobnom technickom zariadení, je chránený podľa tohto zákona, ak je výsledkom tvorivej duševnej činnosti* autora.“ Uvedená právna úprava odráža všetky medzinárodné záväzky v oblasti ochrany autorských práv vo vzťahu k počítačovému systému

Vo vzťahu k postihovaniu protiprávnych konaní, ktorými sa porušujú ustanovenia Trestného zákona je v TZ vymedzený trestný čin podľa **§ 283 – Porušovanie autorského práva**. Ide o blanketnú skutkovú podstatu, ktorá odkazujú na už spomínaný zákon. Skutková podstata znie:

1) *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.*

Objektom trestného činu je autorské právo a právo súvisiace s týmto právom. Predmetom je dielo z oblasti literatúry, umenia alebo vedy, ktoré je jedinečným výsledkom tvorivej duševnej činnosti autora vnímateľným zmyslami, bez ohľadu na jeho podobu, obsah, kvalitu, účel, formu jeho vyjadrenia alebo mieru jeho dokončenia (§ 3 ods. 1 Autorského zákona). Za dielo sa považuje aj počítačový program. Medzi práva, ktoré súvisia s autorským právom patria práva umelca realizujúceho umelecký výkon, práva výrobcu zvukového záznamu

[40] Čl. 6 Smernice - Členské štáty prijmú opatrenia potrebné na zabezpečenie toho, aby sa toto úmyselné konanie považovalo za trestný čin: Návrh dospelej osoby, uskutočnený pomocou informačných a komunikačných technológií, na stretnutie s dieťaťom, ktoré nedosiahlo vek, v ktorom je spôsobilé dať súhlas na pohlavný styk, s cieľom spáchať niektorý z trestných činov uvedených v článku 3 ods. 4 a článku 5 ods. 6, ak po tomto návrhu nasledovali faktické činy vedúce k takémuto stretnutiu, sa trestá odňatím slobody s hornou hranicou trestnej sadzby najmenej jeden rok.

[41] V súlade s touto zásadou autorského práva nie sú myšlienky a princípy, ktoré tvoria základ logiky, algoritmov a programovacích jazykov, chránené podľa tejto smernice. V súlade s právnymi predpismi a judikatúrou členských štátov, ako aj s medzinárodnými dohovormi o autorských právach, je autorskými právami chránené vyjadrenie týchto myšlienok a princípov – Preambula Smernice.

[42] Ide o druhý oddiel, siedmej hlavy Osobitné ustanovenia o niektorých dielach

alebo zvukovo-obrazového záznamu, ako aj práva vysielateľa (rozhlasového a televízneho). Subjektom môže byť fyzická osoba subjektívna stránka predpokladá úmyselné zavinenie.

Medzi okolnosti, ktoré podmieňujú požitie vyššej trestnej sadzby patrí spôsobenie väčšej škody, spáchanie trestného činu z osobitného motívu, prípadne závažnejším spôsobom konania a tiež ak je trestný čin spáchaný prostredníctvom počítačového systému, prípadne je páchateľ členom nebezpečného zoskupenia.

Medzi najčastejšie formy a spôsoby páchania tejto trestnej činnosti je možné zaradiť rôznu protiprávnu činnosť, ktorá sa označuje ako tzv. „softvérové pirátstvo." Ide o neoprávnené používanie alebo kopírovanie počítačových programov, ktoré sú chránené prostredníctvom práva duševného vlastníctva.[43] Z pohľadu porušovania autorského práva môžeme túto formu trestnej činnosti zaradiť medzi „najmladšie." Z pohľadu určitej klasifikácie protiprávnych konaní vo vzťahu k softvérovému pirátsku je možné zaradiť:

- nelegálny zásah do softvéru – môže ísť o tzv. plagiátorstvo (úprava pôvodného softvéru), prípadne možnosť tvorby tzv. „národných" verzií softvéru bez povolenia pôvodného autora a pod.
- nelegálna výroba softvéru
- nelegálne rozširovanie softvéru – napr. prostredníctvom warez stránok, prípadne prostredníctvom torrent klientov,
- nelegálne používanie softvéru – môže ísť o používanie legálneho softvéru, ale v rozpore s licenčnými podmienkami (napr. viacnásobná inštalácia), resp. používanie softvéru bez príslušnej licenčnej zmluvy.[44]

Právna úprava počítačovej kriminality v Slovenskej republike je teda už v zmysle uvedených skutočností založená predovšetkým na nasledovných zákonoch:

- Trestný zákon – zákon č. 300/2005 Z. z. v znení neskorších predpisov;
- Zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb v znení neskorších predpisov
- Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov,
- Zákon č. 185/2015 Z. z. autorský zákon v znení neskorších prepisov
- Zákon č. 351/2011 o elektronických komunikáciách v znení neskorších predpisov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií)
- Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov
- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
- Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov[45]
- a iné.

Vo všeobecnosti teda platí, že základný právny rámce je síce vymedzený právnymi normami z rôznych oblastí spoločenského života, ale postihovanie takéhoto protiprávneho konania je vyslovene otázkou trestného práva. Za tým účelom je potrebné, aby trestné právo vytvorilo skutočne silný zákonný podklad na to, aby sme mohli protiprávne konania, ktoré patria medzi trestné činy počítačovej kriminality, trestné stíhať. Ak by sme vychádzali z trestného práva medzi trestné činy, ktoré je možné zaradiť medzi trestné činy počítačovej

[43] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 326. ISBN 978-80-8168-538-5.

[44] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer, s. 327-330. ISBN 978-80-8168-538-5

[45] Zákon bol schválený v NR SR dňa 30. 1. 2018 a do dnešného dňa (16. 3. 2018) nevyšiel v zbierke zákonov. Jeho účinnosť je od 1. 4. 2018.

kriminality (resp. trestné činy pri ktorých sa využíva informačná a komunikačná technika) je potrebné tieto rozdeliť na:

- trestné činy, pri ktorých sú prvky informačných a komunikačných technológií **terčom útoku** páchateľa, čiže z hľadiska skutkovej podstaty trestného činu predstavujú individuálny objekt, resp. sa prejavujú na hmotnom predmete útoku
- trestné činy pri ktorých sú informačné a komunikačné technológie **použité ako nástroj**, ktorý umožňuje spáchanie takéhoto trestného činu.

Je však možné konštatovať, že niektoré z trestných činov svojím charakterom patria do obidvoch skupín trestnej činnosti, vzhľadom k tomu, že sú chránené ustanoveniami Trestného zákona prostriedky, ale zároveň obsahujú z hľadiska objektívnej stránky aj možnosti zneužitia týchto prostriedkov

Do prvej skupiny môžeme zaradiť napr.:

- § 196 a § 197 Porušovanie tajomstva prepravovaných správ
- § 215 Neoprávnené užívanie cudzej veci
- § 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty
- § 228 Poškodzovanie cudzej veci
- § 247 Neoprávnený prístup do počítačového systému
- § 247a Neoprávnený zásah do počítačového systému
- § 247b Neoprávnený zásah do počítačového údaja
- § 283 Porušovanie autorského práva
- § 291 Ohrozenie bezpečnosti vzdušného dopravného prostriedku a lode
- § 319, § 320 Ohrozenie utajovanej skutočnosti
- § 419 Terorizmus a niektoré formy účasti na terorizme

Do druhej skupiny môžeme zaradiť napr.:

- § 174 Šírenie toxikománie
- § 196 a § 197 Porušovanie tajomstva prepravovaných správ
- §201a Sexuálne zneužívanie
- § 212 Krádež
- § 221 Podvod
- § 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty
- § 226 Neoprávnené obohatenie
- § 229 Prevádzkovanie nepoctivých hier a stávok
- § 231 § 232 Podielnictvo
- § 233 § 234 Legalizácia príjmu z trestnej činnosti
- § 247 Neoprávnený prístup do počítačového systému
- § 247c Neoprávnené zachytávanie počítačových údajov
- § 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov
- § 249a Falšovanie predmetov kultúrnej hodnoty
- § 272 Výroba a držba falšovateľského náčinia
- § 281 Porušovanie práv k ochrannej známke, označeniu pôvodu výrobku a obchodnému menu
- § 282 Porušovanie priemyselných práv
- § 283 Porušovanie autorského práva
- § 284 Všeobecné ohrozenie
- § 286 Poškodzovanie a ohrozovanie prevádzky všeobecne prospešného zariadenia
- § 318 Vyzvedačstvo
- § 337 Podnecovanie

- § 338 Schvaľovanie trestného činu
- § 345 Krivé obvinenie
- § 360 Nebezpečné vyhrážanie
- § 360a Nebezpečné prenasledovanie
- § 361 Šírenie poplašnej správy
- § 371 Ohrozovanie mravnosti
- § 373 Ohováranie
- § 374 Neoprávnené nakladanie s osobnými údajmi
- § 368 Výroba detskej pornografie
- § 369 Rozširovanie detskej pornografie
- § 370 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení
- § 377 Porušenie dôvernosti ústneho prejavu a iného prejavu osobnej povahy
- § 419a Účasť na bojovej činnosti organizovanej ozbrojenej skupiny na území iného štátu
- § 421 Založenie, podpora a propagácia hnutia smerujúceho k potlačeniu základných práv a slobôd
- § 422 Prejav sympatie k hnutiu smerujúcemu k potlačeniu základných práv a slobôd
- § 422b Rozširovanie extrémistických materiálov
- a mnohé ďalšie.

Pri charakterizovaní jednotlivých znakov skutkových podstát trestných činov, ktoré je možné označiť ako počítačové trestné činy, resp. ako trestné činy, ktoré sú spáchané v určitom kybernetickom priestore, prípadne s použitím informačných a komunikačných technológií Trestný zákon uvádza viacero pojmov, ktoré sú s tým spájané. Ako základný termín pre spáchanie trestného činu v takomto prostredí je spáchanie trestného činu verejne v zmysle § 122 ods. 3. Trestný čin je spáchaný verejne ak je spáchaný

a) obsahom tlačoviny alebo rozširovaním spisu, filmom, rozhlasom, televíziou, použitím počítačovej siete alebo iným obdobne účinným spôsobom
b) pred viac ako dvoma súčasne prítomnými osobami

Medzi ďalšie pojmy, ktoré sa spomínajú v súvislosti s páchaní takejto trestnej činnosti uvádzajú v ustanoveniach TZ patrí napr.: elektronická komunikačná služba, počítačový program, počítač, počítačový systém, počítačový údaj, technické vybavenie počítača, programové vybavenie počítača a mnohé ďalšie.

Záver

Je možné konštatovať, že žiadna iná kriminalita nepresahuje hranice jednotlivých štátov takým spôsobom ako počítačová kriminalita, čo predpokladá, že jednotlivé orgány činné v trestnom konaní následne aj súdy jednolistých členských krajín Európskej únie budú presadzovať spoločný postup v prípade riešenia tohto druhu trestnej činnosti. V zásade to predpokladá zjednotenie a zharmonizovanie právnej úpravy v tejto oblasti, k čomu majú pomôcť predovšetkým medzinárodné zmluvy, ako aj právne predpisy Európskej únie.

Základným problémom v tejto oblasti je vymedzenie samotného pojmu počítačová kriminalita, resp. jej niektorý iný ekvivalent, nakoľko odborná literatúra sa ani v tejto oblasti nezjednotila, pričom z môjho pohľadu je nevhodnejšie túto oblasť trestnej činnosti nedefinovať pojmom počítačová kriminalita, ale definovať ju ako kriminalitu, pri ktorej sa prostriedky informačných a komunikačných technológií stávajú jednak cieľom protiprávnych konaní, ako aj prostriedkom na páchanie trestnej činnosti, pričom trestná činnosť sa realizuje v určitom kybernetickom priestore.

Trestnoprávna úprava tohto druhu trestnej činnosti v Slovenskej republike je v neustálom vývine, pričom sa snaží reflektovať na dynamiku trestnej činnosti v tejto oblasti. Je možné vyjadriť názor, že súčasná trestnoprávna úprava spĺňa všetky predpoklady, ktoré vychádzajú z Dohovoru o počítačovej kriminalite, ako základného právneho dokumentu v tejto

oblasti, pričom Slovenská republika reagovala aj na právne predpisy Európskej únie a právnu úpravu v rámci určitých konkrétnych zmien upravila v ustanoveniach Trestného zákona. Je však možné poukázať, že tieto zmeny sa nevyhli určitým formálnym a obsahovým nedostatkom, ktoré by bolo potrebné ešte odstrániť, aby skutočne všetky požiadavky boli splnené.[46]

V prípade taxatívne vymedzených trestných činov je možné vidieť, že medzinárodná právna úprava počítačovej kriminality a rovnako právna úprava Európskej únie, sa premietla do novej úpravy Trestného zákona, nakoľko však v prípade počítačovej kriminality ide o vysokú latenciu, je otázne či bude aj účinná.

Zoznam použitej literatúry:

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. [online].]. [cit. dňa 15. 3. 2018]. Dostupné na internete: http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

BENEDEKOVÁ, D. *Právna úprava počítačovej kriminality*. In: MARKOVÁ, V. ed. *Aktuálne otázky trestného práva v teórii a praxi: Zborník príspevkov z 4. roč. interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, s. 20 – 26. ISBN 978-80-8054-

BRENNER, S. W. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger, 2010, ISBN 978-3-313-36546-1.

BROOMHALL, B. *International justice and the international criminal court: between sovereignty and the rule of law*. Oxford: University Press, 2003, ISBN 0-19-925600-4.

Dôvodová správa k návrhu zákona č. 398/20015 Z. z.

GŘIVNA, T., POLČÁK, R. *Kyberkriminalita a právo*, 1. vyd. Praha: Auditorium. ISBN 978-80-903786-7-4.

HOLCR, K. *Kriminológia*, Bratislava: Iura Edition, 401 s. ISBN 978-80-8078-206-1.

KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* Bratislava: Wolter Kluwer. ISBN 978-80-8168-538-5.

KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC. ISBN 978-80-88168-18-8.

Konsolidované znenie Zmluvy o Európskej únii a Zmluvy o fungovaní Európskej únie 2012/C 326/01 [online].]. [cit. dňa 15. 3. 2018]. Dostupné na internete: http://eurlex.europa.eu/legal-content/SK/TXT/?uri=celex%3A12012E%2FTXT

KORGO, D. a kol. *Trestné právo hmotné. Osobitná časť*. 2. aktualiz. a dopln. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, ISBN 978-80-7380-631-6

KOSTRECOVÁ, E., JOKAY, M., KOSTREC, M. *Počítačová kriminalita.* Bratislava: Slovenská technická univerzita v Bratislave. ISBN 978-80-227-3410-3.

ROMŽA, S. *Počítačová kriminalita ako spoločenský fenomén a osobitosti odhaľovania a objasňovania jej jednotlivých foriem.* In. ROMŽA, S., FERENĆÍKOVÁ, S., MICHAĽOV, L. (eds.). *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 7 - 15. ISBN 978-80-8152-146-1

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, ISBN 978-80-7380-501-2.

SMEJKAL, V., PORADA, V. *Vybrané aspekty metodiky vyšetřování kybernetické kriminality.* In. ROMŽA, S., FERENĆÍKOVÁ, S. a MICHAĽOV, L. (eds.). *Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty*, Zborník príspevkov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, s. 60 - 83. ISBN 978-80-8152-146-1

[46] Jedna dôležitá požiadavka by mala smerovať aj na kladenie dôrazu na jednotnosť pri prekladaní rôznych dokumentov z anglických ekvivalentov.

United Nations Manual on the prevention and control of computer-related crime. [online].]. [cit. dňa 15. 3. 2018]. Dostupné na internete: http://216.55.97.163/wpcontent/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf
Zákon č. 300/2005 Z. z. Trestný zákon, v znení neskorších predpisov.
Zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov

Kontaktné údaje:
JUDr. Veronika Marková, PhD.
Katedra trestného práva
Akadémia PZ v Bratislave
veronika.markova@minv.

Zneužívanie osobných údajov v praxi

René Pawera, Peter Veselý

Abstrakt:
Analýza modelov narušenia kybernetickej bezpečnosti za účelom zneužitia osobných údajov, analýza vybraných bezpečnostných incidentov a návrh primeraných opatrení za účelom zníženia rizika daných typov incidentov najmä s využitím open source zdrojov. Analýza prípadných dopadov na organizáciu v súvislosti s nariadením GDPR a smernicou ePrivacy.
Kľúčové slová:
Osobné údaje, kybernetická bezpečnosť, GDPR, ePrivacy

Abstract:
Analysis of cyber security breach models for the purpose of misuse of personal data, analysis of selected security incidents and proposal of appropriate measures to reduce the risk of these types of incidents, especially with the use of open source resources. Analysis of potential impacts on the organization in relation to the GDPR Regulation and the ePrivacy Directive.
Key words:
Personal data, cyber security, GDPR, ePrivacy

Úvod

Zneužívanie osobných údajov si ľudia bežne nevedia vizuálne predstaviť. Všimnú si, že im zmizne nejaká drobnosť, ale zväčša si nevšimnú, že im niekto ukradne všetky osobné údaje z počítača. Prečo by vlastne aj mali toto zneužitie osobných údajov vidieť, keď sú to iba nuly a jedničky a navyše, súbory sú tam, kde boli. V minulosti jedna nemenovaná štúdia študenta bakalárskeho stupňa v dotazníkovom výskume na neveľkom počte respondentov poukazovala na skutočnosť, že daným respondentom nevadí, že by mali v počítači nainštalovaný tzv. KEYLOGGER, ktorý bude zaznamenávať všetky klávesy, ktoré stlačia, ale vadil by im stav, kedy by ich útočník videl na webkamere na och počítači, prípadne inej kamere. Aj preto je asi pomerne rozšírený zvyk prelepovať webovú kameru – možno s myšlienkou - keď to už robil šéf FBI, tak možno na tom niečo bude.[1]. Tieto závery štúdie sú nedostatočné, ale ako také poukazujú na skutočnosť, že ľudia odlišne vnímajú narušenie svojej osobnej bezpečnosti zneužitím, alebo krádežou elektronických osobných údajov, pričom mnohokrát ani nemajú predstavu, čo sú to vlastne ich osobné údaje a ako vôbec môžu byť zneužité.

Osobné online identifikátory ako osobné údaje

Vysvetlenie, čo sú to osobné údaje a osobné online identifikátory poskytuje nariadenie GDPR a podľa nariadenia GDPR sú za určitých okolností osobné údaje aj osobné online identifikátory pridelené fyzickým osobám technickými prístrojmi, ako sú IP adresy, cookies, RFID, e-mailové adresy, lokalizačné údaje a pod. Napríklad e-mailová adresa môže byť osobným údajom pokiaľ je meno.priezvisko@domena.prípona unikátnym a určiteľným e-mailom. Podľa nariadenia GDOR je možné považovať e-mailovú adresu za osobný údaj ak prostredníctvom tej e-mailovej adresy možno vypátrať osobu jednoducho prostredníctvom verejne dostupných databáz. Vlastník e-mailovej adresy by mal byť buď vlastníkom webovej domény a v jeho SK-nic handle, čo je osobný údaj, keďže je prísne spojený s konkrétnou osobou, je možné vyčítať konkrétnu osobu. Ďalšia možnosť je, že vlastník e-mailovej adresy si píše blog a po zadaní do google.com ho možno jasne identifikovať a niekedy aj s fotografiou, prípadne vo facebook.com alebo v inej sociálnej sieti, alebo má vlastník e-mailovej adresy na internete inzerát s pripojeným telefónnym číslom či uvedenou adresou. IP adresa za podobných

[1] Šéf FBI má webkameru prelepenú páskou a vy by ste mali tiež | pc.sk. In: [cit. 02.07.2018]. Dostupné na internete: http://pc.zoznam.sk/novinka/sef-fbi-ma-webkameru-prelepenu-paskou-vy-ste-mali-tiez

okolností môže byť v podobe statickej pevnej adresy, ktorá je zmluve priradená ISP priamo k fyzickej osobe, ktorej totožnosť je overená zákonným spôsobom.

Modely narušenia kybernetickej bezpečnosti

Informačná bezpečnosť a ochrana dát vo firme zahŕňa všetky procesy a aktivity ochrany vedomostí, informácií alebo dát bez ohľadu na to, v akej forme a podobe sa vo firme nachádzajú. Počítačová bezpečnosť predstavuje súhrn prostriedkov zabezpečujúcich bezpečnú prevádzku počítača a ochranu dát uchovávaných a spracúvaných na danom počítači. Kybernetická bezpečnosť je jednou zo špecifických subdomén informačnej bezpečnosti. Odborná disciplína informačná bezpečnosť sa zaoberá otázkou zaručenia dôvernosti, integrity, dostupnosti a sledovateľnosti informačných aktív všeobecne, zatiaľ čo kybernetická bezpečnosť sa venuje bezpečnosti iba určitej časti informačných aktív, konkrétne tých, ktoré sú spracúvané vo virtuálnom priestore, zvanom kybernetický priestor.[2]

Existujú vo všeobecnosti dva základné modely narušenia kybernetickej bezpečnosti, a to narušenie pasívnym útokom a narušenie kybernetickej bezpečnosti aktívnym útokom. Pasívny útok je len veľmi ťažko zistiteľný, detegovanie takéhoto druhu narušenia kybernetickej bezpečnosti býva extrémne zložité, ale existuje voči nemu jednoduchá obrana založená na proaktívnom šifrované osobných údajov. Narušiteľ kybernetickej bezpečnosti tak dostane zašifrované osobné údaje, kde dešifrovanie týchto údajov ho bude stáť priveľké zdroje vzhľadom k predpokladanému zisku za zneužité osobné údaje. Aktívne narušenie kybernetickej bezpečnosti je založené na viacerých prvkoch, ktoré sú potrebné na prevedenie daného aktívneho útoku na informačný systém. Spôsobov a metód prevedenia útokov je množstvo a stále pribúdajú. Základným prvkom aktívneho narušenia kybernetickej bezpečnosti je predpoklad existencie zraniteľnosti.[3]

Nariadenie GDPR vytvára dve základné roviny prístupu k problematike bezpečnosti spracúvania osobných údajov. Prvou koncepciou nariadenia GDPR je tzv. štandardná ochrana osobných údajov („data protection by default“)[4]. V rámci koncepcie štandardnej ochrany osobných údajov musia *všetky organizácie, ktorých sa nariadenie GDPR týka, vždy a za každých okolností zabezpečiť a reálne prijať také bezpečnostné opatrenia vo svojej organizácii, ktoré z hľadiska množstva, rozsahu a doby spracúvania minimalizujú osobné údaje na nevyhnutné minimum, ktoré je u konkrétnej organizácie potrebné na dosahovanie ním stanovených účelov spracúvania. Ide najmä o prípady spracovania osobných údajov v nevyhnutnej miere potrebných iba pre účely výkonu predmetu podnikania konkrétnej organizácie (napr. proces riadenia údajov obsiahnutých v objednávke tovaru od ich získavania, sprístupňovania obchodným partnerom pri doručovaní, opätovnom prijatí pri vybavovaní reklamácie až po ich likvidáciu).*[5] Štandardná koncepcia ochrany osobných údajov sa nevyhnutne týka každej organizácie spracúvajúcej osobné údaje. Druhou koncepciou je špecifická ochrana osobných údajov („data protection by design“)[2]. Táto koncepcia špecifickej ochrany osobných údajov vyžaduje od všetkých *organizácií spracúvajúcich osobné údaje, aby už pri určovaní prostriedkov spracúvania osobných údajov, teda už vo fáze vývoja novej aplikácie alebo zavádzaní novej služby, zmeny informačného systému, implementovali také technické a bezpečnostné opatrenia, ktoré vzhľadom na najnovšie poznatky („state of art“)*

[2] Kyber-niečo. In: *Preventista.sk* [online] [cit. 02.07.2018]. Dostupné na internete: http://preventista.sk/info/kyber-nieco/

[3] AKANE. IPS/IDS ochrana. In: *Jak na webové stránky* [online] [cit. 04.12.2017]. Dostupné na internete: http://timehosting.cz/ipsids-ochrana/

[4] TREND.SK. Privacy by design by default kde končí filozofia a začína prax? In: *blog.etrend.sk* [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

[5] Základní příručka k GDPR: Úřad pro ochranu osobních údajů. In: [cit. 12.02.2018]. Dostupné na internete: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744

a náklady na ich realizáciu, budú funkčné počas celého procesu spracúvania osobných údajov. Pri prijímaní bezpečnostných opatrení bude každá organizácia, ktorej sa nariadenie GDPR týka, musieť zohľadniť povahu, rozsah, kontext a účely spracúvania osobných údajov ako aj riziká zásahu do takýchto osobných údajov[6]. Úvodné ustanovenia GDPR („recitals"), ktoré sú výkladovým návodom k nariadeniu GDPR, v tejto súvislosti kladú dôraz na čo najskoršiu pseudonymizáciu údajov, transparentnosť k dotknutým osobám, minimalizáciu údajov a flexibilitu podnikateľa z hľadiska jeho možností na dopĺňanie a zlepšovanie bezpečnostných prvkov7.

Vybrané prípady zneužívania osobných údajov v praxi

Americká internetová spoločnosť Facebook pravdepodobne neodškodní zhruba 2,7 milióna svojich európskych používateľov, ktorých osobné údaje zneužila analytická spoločnosť Cambridge Analytica. Nešlo totiž o citlivé bankové údaje, uviedla v stredu firma prevádzkujúca rovnomennú sociálnu sieť.[8] Toľko z oficiálnych médií. Problém nastal ešte v úvode roku 2014, kedy Cambridge Analytica podľa dostupných informácií začala využívať dáta z aplikácie This Is Your Digital Life[9] - digitálny prieskum, v podobe osobnostného testu, pre používateľov Facebooku, ktorý vytvoril akademik z Univerzity v Cambridge Aleksandr Kogan. Ľudia súhlasili, že vývojári môžu pristupovať k niektorým osobným údajom ako sú miesto bydliska alebo informácie o sledovaných stránkach na najväčšej sociálnej sieti. Autori aplikácie tvrdili, že údaje budú použité pre výskum. Používatelia sami odsúhlasili zbieranie týchto osobných údajov, išlo teda o legálny zber osobných údajov v tejto fáze. Problém nastal, keď Aleksandr Kogan tieto údaje poskytol tretím stranám, medzi ktorými bola aj spoločnosť Cambridge Analytica. Túto organizáciu vlastnil v danej americký miliardár Robert Mercer a jedna z jeho spoločností spolupracovala na predvolebnej kampani Donalda Trumpa počas prezidentských volieb 2016. Práve predmetné osobné údaje z aplikácie This Is Your Digital Life podľa dostupných informácií zohrávali dôležitú úlohu pri zostavovaní personalizovaných reklám pre voličov. Aplikáciu si malo celkovo stiahnuť viac ako 270 000 používateľov, ale vývojári zozbierali aj osobné údaje iných osôb - zbierali aj informácie o priateľoch na Facebooku, ktorí mali povolené takéto zdieľanie (respektíve ho nemali zakázané). Celkovo sa tak mala Cambridge Analytica dostať k údajom až 50 miliónov používateľov sociálnej siete Facebook. Kontroverziu vyvoláva fakt, že Facebook mal o všetkom vedieť už od roku 2015[10].Po odhalení sa akcie Facebooku okamžite znížili o 58 miliárd USD.

Okrem toho ale vyššie spomenutá sociálna sieť mala viacero závažných bezpečnostných incidentov, najzávažnejší z pohľadu zraniteľnosti bol ten, kedy v rámci chybného kódu na stránke sa prípadný útočník mohol dostať až k údajov dvoch miliárd užívateľov. [11] Druhý menší problém[12] spočíva v pravidelnom uverejňovaní rôznych návodov a aplikácií na hacknutie osobných údajov na danej sociálnej sieti, väčšina z nich je funkčná, dokonale ukradne identitu užívateľa, ktorý si danú aplikáciu spustia.

---

[6] Desatero omylů o GDPR: Dokumenty k GDPR: Úřad pro ochranu osobních údajů. In: [cit. 07.12.2017]. Dostupné na internete: https://www.uoou.cz/desatero%2Domylu%2Do%2Dnbsp%2Dgdpr/d-23799/p1=4720

[7] [CSL STYLE ERROR: reference with no printed form.]

[8] Facebook sa nechystá odškodniť Európanov za zneužitie ich dát. In: *Pravda.sk* [online] [cit. 02.07.2018]. Dostupné na internete: https://spravy.pravda.sk/svet/clanok/470832-facebook-sa-nechysta-odskodnit-europanov-za-zneuzitie-ich-dat/

[9] [CSL STYLE ERROR: reference with no printed form.]

[10] Facebook má tajný súbor, v ktorom o vás zbiera všetky informácie: TAKTO sa k nemu môžete dostať. In: *Topky.sk* [online] [cit. 27.03.2018]. Dostupné na internete: http://www.topky.sk/cl/13/1694159/

[11] ŽIVÉ.SK. Dve miliardy účtov na Facebooku sa dali ľahko hacknúť. In: *Živé.sk* [online] [cit. 13.03.2018]. Dostupné na internete: https://www.zive.sk/clanok/130942/dve-miliardy-uctov-na-facebooku-sa-dali-lahko-hacknut/

[12] Expert odhalil, ako okradnúť Google, Microsoft či Facebook | Živé.sk. In: [cit. 22.07.2016]. Dostupné na internete: http://www.zive.sk/clanok/116492/expert-odhalil-ako-okradnut-google-microsoft-ci-facebook#

Dopad na bezpečnosť

Nariadenie GDPR je platné pre obrovské množstvo organizácií v rámci EÚ. Týka sa najmä práv občanov, teda fyzických osôb. Povinnosti ochraňovať ich práva majú najmä organizácie v súkromnom sektore, avšak nie len tie. Nariadenie GDPR sa týka aj organizácií verejného ako aj štátneho sektora. Niektorých organizácií sa však netýka priamo, majú svoju právnu úpravu – SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. [2] Táto smernica vyžaduje, aby členské štáty do 06.05.2018 prijali a uverejnili zákony a iné právne predpisy a správne opatrenia na dosiahnutie súladu s touto smernicou, pričom tieto ustanovenia sa uplatňujú od 06.05.2018

V súčasnej právnej úprave sa však stáva, že jednotlivé štáty EÚ spôsobom porušujú práva fyzických osôb. Príkladom je aj nedávno zverejnený prípad,[13] kedy súdy v Spojenom kráľovstve (UK) vyhlásili v odvolacom konaní za nezákonný Program masového sledovania (UK mass surveillance programm) s odôvodnením na porušovanie ľudských práv verejnosti. Tento rozsudok sa dá chápať ako jasný odkaz príslušným ministrom vlády, aby dodržiavali legislatívny rámec. Sudcovia uviedli, že zákon DRIPA (Data Retention and Investigatory Power Acts 2014) porušuje právo EÚ, pretože umožňoval zozbieranie údajov z iných dôvodov, než je boj proti závažnej trestnej činnosti. Tento zákon umožňoval tiež policajným a iným orgánom, aby si vytvorili svoj vlastný prístup, pričom sa vyhli predchádzajúcemu súhlasu súdu alebo nezávislého orgánu. Zákon DRIPA bol kritizovaný aj v minulosti, vláda UK spravila úpravy s cieľom legitimizovať časti nezákonného postupu, avšak jadro problému zostalo neošetrené a vytvorilo podľa občianskych aktivistov otvorenú dieru v právach verejnosti. Tento zákon umožňuje vláde UK, aby prinútilo komunikačné spoločnosti uchovávať podrobné informácie o umiestneniach a používaní telefónov a komunikačných zariadení. O tomto tvrdil poslanec Mr. Watson (LABOUR MP), že práve toto je v rozpore so základnými právami britských občanov. Úrady naopak tvrdia, že práve táto právomoc je kľúčová pre trestné stíhanie nebezpečných páchateľov vrátane známeho pedofila Iana Watkinsa. Podľa ministra vnútra je toto často jediný spôsob, ako identifikovať pedofilov, ktorí sa podieľajú na zneužívaní detí na internete, pretože je možné zistiť, kde a kedy sa tieto hrozné činy stali.[14]

V tomto kontexte je možné spomenúť aj kauzy na našom území – údajné odpočúvanie Vojenským spravodajstvom,[15] ktoré sa ale oficiálne nepotvrdili Takýto vyššie spomenutý prípad masového odpočúvania je nutné uviesť v prípade nariadenia GDPR, pretože sa vzťahuje na ochranu práv občanov EÚ, avšak nie je všeliekom na všetky práva občanov EÚ a sama EÚ vydala ďalšiu smernicu, kde vlastne vo svojej podstate povoľuje porušovanie práv občanov EÚ.

[13] UK mass surveillance programme ruled unlawful as campaigners call for overhaul of "snooper's charter" | The Independent. In: [cit. 07.02.2018]. Dostupné na internete: http://www.independent.co.uk/news/uk/home-news/uk-surveillance-digital-gchq-snooping-charter-court-unlawful-intelligence-security-services-a8185176.html

[14] UK mass surveillance programme ruled unlawful as campaigners call for overhaul of "snooper's charter" | The Independent [online] [cit. 07.02.2018]. Dostupné na internete: http://www.independent.co.uk/news/uk/home-news/uk-surveillance-digital-gchq-snooping-charter-court-unlawful-intelligence-security-services-a8185176.html

[15] Vojenské spravodajstvo nie je len na odpočúvanie. In: [cit. 07.02.2018]. Dostupné na internete: https://komentare.hnonline.sk/komentare/548154-vojenske-spravodajstvo-nie-je-len-na-odpocuvanie

V konečnom dôsledku teda bremeno nariadenia GDPR bude uvalené iba na súkromné organizácie, občan v EÚ sa bude cítiť relatívne bezpečne.[16]

Prevencia pred únikom a zneužitím osobných údajov

Jedným zo systémov vhodným ako prevencia pred únikom a zneužitím osobných údajov je aj DLP – Data Loss Prevention[17]. Tento systém už v samotnom názve naznačuje, že danú požiadavku zabezpečí. DLP vlastne pokrýva všetky kanály úniku údajov v organizácii a šetrí náklady potrebné na nápravu straty údajov. Taktiež identifikuje podozrivé aktivity predstavujúce potencionálne bezpečnostné riziko skôr, než spôsobia stratu času a financií a tak znižuje náklady na personál identifikovaním problémov s produktivitou a zvyšovaním pracovnej výkonnosti. Systém DLP taktiež dokáže odhaľovať útoky pracujúce na princípe sociálneho inžinierstva a taktiež aj pokusy o vydieranie už v ich začiatkoch a nedovolí im ohroziť organizáciu. Celý disk alebo vybrané súbory zostávajú zašifrované a potencionálny útočník ich nedokáže prečítať, resp. dešifrovanie údajov bude veľmi náročné vzhľadom na dostupné zdroje. Okrem toho systém DLP dokáže kontrolovať používanie tlačiarní, aplikácií a obmedziť nadmerné online aktivity. Napríklad náš slovenský popredný výrobca antivírusových systémov v rámci komplexnej podpory pre zákazníkov kúpil popredného českého výrobcu DLP[18] a teraz integruje produkty DLP pre svojich zákazníkov tak, aby bolo možné splniť aj toto nariadenie GDPR alebo smernicu o kybernetickej bezpečnosti.

Všeobecné nariadenie GDPR a ani smernica o kybernetickej bezpečnosti neukladajú priamo povinnosť použiť na zabezpečenia spracovávania osobných údajov niektoré špecifické opatrenia ako je napríklad šifrovanie[19]. Na druhej strane, pri stanovení povinnosti správcu a spracovateľa osobných údajov zabezpečiť osobné údaje, sa všeobecné nariadenie GDPR vyslovene odvoláva na *stav techniky, náklady na prijatie a prevedenie jednotlivých technických a organizačných opatrení k zabezpečeniu osobných údajov, povahe, rozsahu, kontextu a účelom samotného spracúvania a taktiež k pravdepodobným rizikám pre práva a slobodu, ktoré spracúvanie so sebou nesie*.[20] Vlastná povinnosť potom zahrňuje zavedenie vhodných technických a organizačných opatrení a začlenenia do spracovania nevyhnutných záruk, a to ako v dobe určenia prostriedkov pre spracúvanie, tak v dobe vlastného spracúvania. Šifrovanie je uvedené ako jedno z vhodných opatrení. Pri posudzovaní úrovne bezpečnosti sa zohľadnia najmä riziká, ktoré predstavujú spracúvanie, náhodné alebo protiprávne zničenie, strata, pozmeňovanie, neoprávnené sprístupnenie osobných údajov a neoprávnený prístup k takým osobným údajom. Šifrovanie sa tak javí ako vhodné riešenie, otázka je, ako sa dá implementovať v existujúcom informačnom systéme[21] S témou šifrovania osobných údajov je spojená napríklad aj implementácia EndPoint Security[22] nástrojov na ochranu pracovných

[16] INFOGRAFIKA: Veľký brat sa pozerá. Čo všetko o vás Google vie? | Magazín.sk. In: [cit. 07.02.2018]. Dostupné na internete: https://magazin.centrum.sk/techmag/infografika-velky-brat-sa-pozera-co-vsetko-o-vas-google-vie/861723.html

[17] Je data loss prevention opravdová prevence? In: [cit. 04.12.2017]. Dostupné na internete: http://www.systemonline.cz/it-security/je-data-loss-prevention-opravdova-prevence.htm

[18] ESET do svojej Technologickej aliancie pridáva spoločnosť Safetica, lídra v oblasti prevencie úniku dát. In: [cit. 08.12.2017]. Dostupné na internete: https://www.eset.com/sk/o-nas/press-centrum/produkty/eset-do-svojej-technologickej-aliancie-pridava-spolocnost-safetica-lidra-v-oblasti-prevencie-uniku-d/

[19] Desatero omylů o GDPR: Dokumenty k GDPR: Úřad pro ochranu osobních údajů [online] [cit. 07.12.2017]. Dostupné na internete: https://www.uoou.cz/desatero%2Domylu%2Do%2Dnbsp%2Dgdpr/d-23799/p1=4720

[20] Základní příručka k GDPR: Úřad pro ochranu osobních údajů [online] [cit. 12.02.2018]. Dostupné na internete: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744

[21] MANSFIELD-DEVINE, S. Meeting the needs of GDPR with encryption. In: *Computer Fraud & Security* [online]. 2017, roč. 2017, č. 9. DOI: 10.1016/S1361-3723(17)30100-8

[22] Všeobecné nariadenie EÚ GDPR a čo to pre vás znamená. In: [cit. 07.12.2017]. Dostupné na internete: https://encryption.eset.com/sk/?gclid=EAIaIQobChMI6ue9gYb51wIV4xbTCh2yGAs7EAAYASAAEgI77_D_BwEintroduction

staníc a implementácia šifrovania údajov a diskov na pracovných staniciach, serveroch a pri ich prenose. Nie je možné však spoliehať sa na to, že šifrovanie disku alebo https komunikácie je úplne bezpečné. Napríklad systém BitLocker vo Windows už bol viackrát prelomený[23] a z tohto pohľadu už nepredstavuje vysokú úroveň ochrany. Alebo známy prípad chyby kryptografickej knižnice OpenSSL pod názvom Hearthbleed.[24]

Záver

Zneužívanie osobných údajov v praxi sa skutočne deje, ako nám dejiny už viackrát ukázali. Problémom preto nie je otázka, či budú zneužité osobné údaje, ale skôr otázka kedy sa tak stane a aký to bude mať dopad. Vhodnou obranou je teda napríklad používanie nástrojov typu DLP alebo šifrovanie. Popisovaný prípad Cambridge Analytica a Facebook ukazuje, že existujú aj iné prípady zneužitia osobných údajov, pričom však tieto prípady nevieme ovplyvniť nastavením bezpečnosti svojho počítača, ale výlučne bezpečným správaním sa na sociálnych sieťach.

Zoznam použitej literatúry:

AKANE. IPS/IDS ochrana. In: *Jak na webové stránky* [online] [cit. 04.12.2017]. Dostupné na internete: http://timehosting.cz/ipsids-ochrana/

KRYVINSKA, Natalia, AUER, Lukas, STRAUSS, Christine. An Approach to Extract the Business Value from SOA Services. In: SNENE, Mehdi, RALYTÉ, Jolita, MORIN, Jean-Henry. eds. *Exploring Services Science* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, zv. 82, s. 42-52 [cit. 16.05.2016]. ISBN 978-3-642-21546-9. Dostupné na internete: http://link.springer.com/10.1007/978-3-642-21547-6_4

MANSFIELD-DEVINE, Steve. Meeting the needs of GDPR with encryption. In: *Computer Fraud & Security* [online]. 2017, roč. 2017, č. 9, s. 16-20. ISSN 1361-3723. DOI: 10.1016/S1361-3723(17)30100-8

PORÁZIKOVÁ, Eva, VOJTECHOVSKÝ, Jaroslav. Trends in e-business and their application in development of SMEs in Slovakia. In: *Management in theory and practice [elektronický zdroj]*. Praha: Newton College, 2016, s. S. 106-112. ISBN ISBN 978-80-87325-08-7.

PORÁZIKOVÁ, Eva, VOJTECHOVSKÝ, Jaroslav, STUDENIČOVÁ, Andrea. Sociálne médiá a firmy. In: *Make it digital : Support for e-business in the V4 countries : Zborník z vedeckej konferencie : [elektronický zdroj]*. Bratislava: Univerzita Komenského v Bratislave, 2016, s. nestr. ISBN ISBN 978-80-223-4219-3.

TREND.SK. Privacy by design by default kde končí filozofia a začína prax? In: *blog.etrend.sk* [online] [cit. 21.01.2018]. Dostupné na internete: https://blog.etrend.sk/martin-sasinek/privacy-by-design-by-default-kde-konci-filozofia-a-zacina-prax.html

VOJTECHOVSKÝ, Jaroslav, PROKSOVÁ, Marianna, PORÁZIKOVÁ, Eva. Elektronické podnikanie. In: *Trendy v online marketingu [elektronický zdroj]*. Bratislava: Univerzita Komenského, 2016, s. nestr. ISBN ISBN 978-80-223-4106-6.

ŽIVÉ.SK. Dve miliardy účtov na Facebooku sa dali ľahko hacknúť. In: *Živé.sk* [online] [cit. 13.03.2018]. Dostupné na internete: https://www.zive.sk/clanok/130942/dve-miliardy-uctov-na-facebooku-sa-dali-lahko-hacknut/

Desatero omylů o GDPR: Dokumenty k GDPR: Úřad pro ochranu osobních údajů. In: [cit. 07.12.2017]. Dostupné na internete: https://www.uoou.cz/desatero%2Domylu%2Do%2Dnbsp%2Dgdpr/d-23799/p1=4720

ESET do svojej Technologickej aliancie pridáva spoločnosť Safetica, lídra v oblasti prevencie úniku dát. In: [cit. 08.12.2017]. Dostupné na internete: https://www.eset.com/sk/o-nas/press-

[23] It is terrifyingly easy to bypass BitLocker in Windows 10. In: [cit. 07.12.2017]. Dostupné na internete: https://betanews.com/2016/11/30/windows-10-bypass-bitlocker/

[24] Heartbleed Bug. In: [cit. 07.12.2017]. Dostupné na internete: http://heartbleed.com/

centrum/produkty/eset-do-svojej-technologickej-aliancie-pridava-spolocnost-safetica-lidra-v-oblasti-prevencie-uniku-d/
Expert odhalil, ako okradnúť Google, Microsoft či Facebook | Živé.sk. In: [cit. 22.07.2016]. Dostupné na internete: http://www.zive.sk/clanok/116492/expert-odhalil-ako-okradnut-google-microsoft-ci-facebook#
Facebook má tajný súbor, v ktorom o vás zbiera všetky informácie: TAKTO sa k nemu môžete dostať. In: *Topky.sk* [online] [cit. 27.03.2018]. Dostupné na internete: http://www.topky.sk/cl/13/1694159/
Facebook sa nechystá odškodniť Európanov za zneužitie ich dát. In: *Pravda.sk* [online] [cit. 02.07.2018]. Dostupné na internete: https://spravy.pravda.sk/svet/clanok/470832-facebook-sa-nechysta-odskodnit-europanov-za-zneuzitie-ich-dat/
Heartbleed Bug. In: [cit. 07.12.2017]. Dostupné na internete: http://heartbleed.com/
INFOGRAFIKA: Veľký brat sa pozerá. Čo všetko o vás Google vie? | Magazín.sk. In: [cit. 07.02.2018]. Dostupné na internete: https://magazin.centrum.sk/techmag/infografika-velky-brat-sa-pozera-co-vsetko-o-vas-google-vie/861723.html
It is terrifyingly easy to bypass BitLocker in Windows 10. In: [cit. 07.12.2017]. Dostupné na internete: https://betanews.com/2016/11/30/windows-10-bypass-bitlocker/
Je data loss prevention opravdová prevence? In: [cit. 04.12.2017]. Dostupné na internete: http://www.systemonline.cz/it-security/je-data-loss-prevention-opravdova-prevence.htm
Kyber-niečo. In: *Preventista.sk* [online] [cit. 02.07.2018]. Dostupné na internete: http://preventista.sk/info/kyber-nieco/
Šéf FBI má webkameru prelepenú páskou a vy by ste mali tiež | pc.sk. In: [cit. 02.07.2018]. Dostupné na internete: http://pc.zoznam.sk/novinka/sef-fbi-ma-webkameru-prelepenu-paskou-vy-ste-mali-tiez
UK mass surveillance programme ruled unlawful as campaigners call for overhaul of "snooper's charter" | The Independent. In: [cit. 07.02.2018]. Dostupné na internete: http://www.independent.co.uk/news/uk/home-news/uk-surveillance-digital-gchq-snooping-charter-court-unlawful-intelligence-security-services-a8185176.html
Vojenské spravodajstvo nie je len na odpočúvanie. In: [cit. 07.02.2018]. Dostupné na internete: https://komentare.hnonline.sk/komentare/548154-vojenske-spravodajstvo-nie-je-len-na-odpocuvanie
Všeobecné nariadenie EÚ GDPR a čo to pre vás znamená. In: [cit. 07.12.2017]. Dostupné na internete:
https://encryption.eset.com/sk/?gclid=EAIaIQobChMI6ue9gYb51wIV4xbTCh2yGAs7EAAYASAAEgI77_D_BwEintroduction
Základní příručka k GDPR: Úřad pro ochranu osobních údajů. In: [cit. 12.02.2018]. Dostupné na internete: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/p1=4744

Kontaktné údaje:

doc. PhDr. René Pawera, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
82005 Bratislava
Thomson Reuters Researcher ID: C-2894-2016
ORCID ID: 0000-0003-0700-8243
Scopus Author ID: 57105605300
rene.pawera@fm.uniba.sk

PhDr. Peter Veselý, PhD.
Fakulta managementu Univerzity Komenského v Bratislave

Odbojárov 10
82005 Bratislava
Thomson Reuters Researcher ID: H-5695-2017
ORCID ID: 0000-0002-7857-6355
Scopus Author ID: 57195951243
peter.vesely@fm.uniba.sk

Úvod do problematiky vydieračského softvéru (ransomware)

Marek Petrik

Abstrakt:
Príspevok sa zaoberá teoretickým a konceptuálnym vymedzením pojmu ransomware. Popisuje procesy viažuce sa k priebehu ransomware útoku a techniky používané na šifrovanie alebo zamknutie zariadenia po úspešnom infikovaní. Analyzuje vektory, prostredníctvom ktorých môže k infikovaniu dôjsť, hlavné ciele, na ktoré mieri a spôsoby platby výkupného. Autor poukazuje aj na rozmáhanie sa trendu ransomware ako služba.
Kľúčové slová:
Malvér, škodlivý softvér, ransomware, ransomware ako služba, výkupné

Abstract:
The paper deals with the theoretical and conceptual definition of the term ransomware. It describes the processes involved in the course of the ransomware attack and the techniques used to encrypt or lock the device after successful infection. It analyzes the vectors through which infection can occur, the main goals to which rates and ransom payment methods. The author also points to the emerging trend of ransomware as a service.
Key words:
Malware, malicious software, ransomware, ransomware as a service, ransom

Úvod

V posledných dvoch rokoch je možné pozorovať extrémny nárast ransomware útokov. Napadnuté boli tisícky zariadení a na obnovu prístupu k strateným súborom bolo vynaložené obrovské množstvo finančných prostriedkov. Taktiež nemalé úsilie muselo byť vynaložené na zlepšenie bezpečnostných opatrení a na obnovu poškodenej reputácie po zasiahnutí predmetnými útokmi. Nové ransomware útoky sú zaznamenávané takmer každým dňom a vytvárajú obrovské zisky pre ich autorov. Zneužívané sú pritom šifrovacie technológie, ktoré boli pôvodne určené na zabezpečenie a ochranu dát. Vplyvom uvedených faktorov sa ransomware stáva jednou z najvýznamnejších hrozieb pre kybernetickú bezpečnosť podnikov, organizácii a jednotlivcov.

Pre lepšie pochopenie súčasného stavu ransomware-u, je potrebné poznať vývoj ransomware-u od jeho skromných začiatkov až po zákerné formy, ktoré môže mať dnes. Jeho pôvod poukazuje na to, ako sa stal jedným z najnepríjemnejších kryptografických problémov, čo viedlo útočníkov k jeho vytvoreniu a čo je možné urobiť pre lepšiu ochranu dát.

Vymedzenie pojmu ransomware

Pojem ransomware sa skladá z dvoch anglických slov a to ransom (výkupné) a software (softvér). V slovenčine sa ransomware označuje tiež aj ako ransomvér alebo vydieračský softvér.[1] Ransomware možno v najvšeobecnejšej rovine popísať ako druh škodlivého softvéru, ktorý limituje alebo priamo blokuje používateľovi prístup k jeho dátam alebo programom, a za obnovenie prístupu požaduje zaplatiť výkupné (ransom).[2] Výkupné je požadované spravidla v kryptomene. Kryptomeny predstavujú formu digitálnych mien, ktoré nie sú vydávané alebo regulované žiadnou centrálnou autoritou (napríklad štátom alebo bankou). Kryptomeny fungujú s cieľom byť decentralizované, bezpečné a anonymné. Vznikajú počas procesu zvaného ťažba, ktorý využíva výpočtový výkon procesora zariadenia, prípadne grafického čipu, na výpočet náročných matematických problémov. Najznámejšou a najvyužívanejšou kryptomenou je Bitcoin, ktorý dosiahol v roku 2017 historické hodnoty nad devätnásť tisíc amerických dolárov za jeden Bitcoin. Ďalšie používané kryptomeny sú napr. Ethereum, Ripple alebo Litecoin.

[1] URBAN, F. *Peniaze alebo dáta: hrozivý vzostup ransomware* [online] [cit. 22.03.2018]. Dostupné na internete: https://touchit.sk/peniaze-alebo-data-hrozivy-vzostup-ransomware/58530
[2] PALISSE, A. et al. *Ransomware and the Legacy Crypto API*. p.2

Ransomware možno rozdeliť do dvoch hlavných typov a to šifrovací (crypto) a zamykací (locker). Zamykací ransomware znemožňuje komunikáciu a prácu s kompromitovaným systémom. Pri šifrovacom type sú napadnuté a zašifrované súbory obete vydierania.[3] Ransomware je možné deliť ďalej na základe jeho druhov, typov alebo rodín.

Locker ransomware (Computer locker)

Locker ransomware je navrhnutý tak, aby odoprel prístup k funkciám počítača. Zvyčajne uzamyká používateľské rozhranie počítača alebo iného zariadenia, kde žiada používateľa o zaplatenie poplatku za účelom obnovenia prístupu. Uzamknutým zariadeniam môže byť ponechaná obmedzená funkčnosť, ako napríklad umožnenie interakcie používateľa s ransomware-om vedúce k zaplateniu výkupného. Prístup k myši môže byť zakázaný a funkčnosť klávesnice môže byť obmedzená na číselné tlačidlá, čo umožní obeti zadávať iba číslice na označenie platby.

Locker ransomware je typicky navrhnutý len na zabránenie prístupu k rozhraniu počítača. Systémové súbory a dáta používateľa ostávajú nedotknuté a po odstránení malware-u je počítač obnovený do pôvodného stavu a dáta opäť prístupné. Z uvedeného dôvodu je locker ransomware menej efektívny pri vymáhaní platby výkupného ako deštruktívnejší krypto ransomware. Technicky zdatnejší používatelia sú často schopní svojpomocne obnoviť prístup pomocou rôznych nástrojov a techník, ktoré sú dostupné online.

Locker ransomware využíva prvky sociálneho inžinierstva a značná časť druhov locker ransomware-u sa maskovala ako správa od štátnych orgánov nesúca upozornenie, že používateľ porušil zákon sťahovaním materiálu chráneného autorskými právami (hudba, filmy, softvér), alebo sledovaním nelegálnych materiálov (napr. detská pornografia). Daný druh ransomware-u bol v najväčšom rozmachu predovšetkým v období rokov 2012-2014.

Locker ransomware môže byť obzvlášť účinný na zariadeniach, ktoré majú obmedzené možnosti pre interakciu s používateľmi. Uvedené predstavuje problémovú oblasť vzhľadom na rozmach nositeľných zariadení a internetu vecí (IoT), kde predmetným typom ransomware-u môžu byť ohrozené milióny pripojených zariadení.

V posledných rokoch je možné pozorovať presun od locker ransomware-u k pôvodnému crypto ransomware-u, ktorý pri zobrazení správy priamo definuje svoje zámery a požiadavky, kde požaduje výkupné výmenou za navrátenie (dešifrovanie) dát.[4]

Crypto ransomware (Data locker)

Tento typ ransomware-u je navrhnutý tak, aby vyhľadal a šifroval cenné dáta uložené v počítači, čím sa stanú nepoužiteľné, kým používateľ nedostane dešifrovací kľúč. Životy ľudí sú čoraz digitálnejšie a ľudia uchovávajú dôležité dáta vo svojich osobných počítačoch a zariadeniach. Mnohí používatelia si neuvedomujú potrebu vytvárať zálohy, ktoré ochránia ich dáta pred zlyhaniami pevného disku, stratou alebo krádežou počítača. A už vôbec nepociťujú potrebu zálohovať dáta pre prípad možných útokov krypto ransomware-u. Používatelia zvyčajne nemajú potrebné vedomosti alebo si jednoducho neuvedomujú hodnotu svojich dát, kým ich nestratia. Efektívny proces zálohovania si vyžaduje určitú námahu a disciplínu, čo pre priemerného používateľa nie je veľmi lákavé. Crypto ransomware zneužíva uvedené nedostatky v typickom bezpečnostnom postoji používateľa. Tvorcovia krypto ransomware-u vedia, že dáta uložené v osobných počítačoch sú pre používateľov pravdepodobne dôležité. Obete môžu byť

[3] PC REVUE. *Trend Micro: Čo je ransomware a prečo by vás mal zaujímať?* [online] [cit. 25.03.2018]. Dostupné na internete: https://www.pcrevue.sk/a/Trend-Micro--Co-je-ransomware-a-preco-by-vas-mal-zaujimat

[4] SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware. Security Response.* [online] [cit. 21.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

zúfalé a aby dostali svoje dáta späť, vyberú si možnosť zaplatenia výkupného za účelom obnovenia prístupu.

Po inštalácii typická hrozba kryptografického ransomware-u ticho vyhľadáva a šifruje súbory. Cieľom je vykonávať uvedené činnosti v tajnosti, kým nedokáže nájsť a šifrovať všetky súbory, ktoré by mohli mať pre používateľa hodnotu. V čase, keď je obeť oboznámená so správou o škodlivom softvéri, ktorá informuje, že jej údaje sú šifrované, škoda sa už stala. Pri väčšine infekcií spôsobených krypto ransomware-om napadnutý počítač naďalej funguje normálne, pretože škodlivý softvér sa nezaoberá kritickými systémovými súbormi ani neodopiera prístup k funkciám počítača. To znamená, že používatelia môžu naďalej používať počítač na vykonávanie celého radu činností okrem prístupu k svojim šifrovaným dátam.[5]

História

Za prvý zdokumentovaný ransomware sa vo všeobecnosti považuje kód, ktorý napísal Dr. Joseph Popp v roku 1989 známy pod názvom AIDS Trojan. Dr. Popp bol evolučný biológ aktívne zapojený do výskumu AIDS. AIDS Trojan sa šíril prostredníctvom diskiet, ktoré boli zaslané všetkým, ktorí sa registrovali do informačného bulletinu o AIDS. Trójsky kôň, ktorý sa na diskete nachádzal, infikoval počítače jednoduchým nahradením dávkového súboru Autoexec.bat. Tváril sa ako špecializovaný softvér, ktorý bude poskytovať aktuálne informácie o výskume AIDS. Počítač ale neskôr začal zobrazovať falošnú licenčnú správu a požadoval platbu vo výške 378 dolárov, ktorá mala byť zaslaná na adresu poštovej schránky v Paname. Trojan následne počítal počet spustení a po deväťdesiatom naštartovaní počítača pozmenil a šifroval názvy súborov na pevnom disku. Používateľ tak v podstate prišiel o prístup k svojim aplikáciám i dátam. [6]

S prvou vlnou moderného ransomware-u šíreného online je možné stretnúť sa v roku 2005 v súvislosti so škodlivým softvérom s názvom Trojan.Gpcoder. Infikoval systémy Windows a cielil na súbory s vybranými príponami. Po ich nájdení súbory skopíroval v šifrovanej podobe a originály odstránil zo systému. Nové šifrované súbory boli uložené na iné miesto a boli nečitateľné. Na domácej obrazovke používateľov bola zobrazená správa, ktorá ich nasmerovala do súboru s príponou .txt umiestneného na ploche, ktorý obsahoval podrobnosti o tom, ako zaplatiť výkupné a odomknúť šifrované súbory.

V roku 2006 sa objavujú ďalšie významné druhy ransomware-u a to Trojan.Cryzip a Trojan.Archiveus, avšak ransomware v tejto dobe bolo spravidla stále jednoduché prekonať, lebo väčšina z nich obsahovala kľúč potrebný na dešifrovanie vo svojom vlastnom kóde. Prvý locker ransomware sa objavuje na začiatku roku 2008 (Trojan.Randsom.C). Uvedený ransomware sa prezentoval ako správa od Windows Security Center (Centrum zabezpečenia) a požadoval od používateľov, aby zavolali na telefónne číslo pre obnovenie licencie k bezpečnostnému softvéru. Akonáhle došlo k telefonátu, počítač sa zamkol.

Zlomovým rokom pre vývoj ransomware-u bol rok 2013 kedy sa objavil ransomware CryptoLocker, ktorý predstavoval novú generáciu ransomware-u. Ako prvý úspešne využíval silné asymetrické šifrovacie metódy v kombinácii s požadovaním platby v novovzniknutej virtuálnej mene Bitcoin. Z ransomware-u CryptoLocker bolo vytvorených mnoho ďalších derivátov vrátane CryptDefense, TorrentLocker, CTB-Locker, CryptoWall, TeslaCrypt a AlphaCrypt. [7]

---

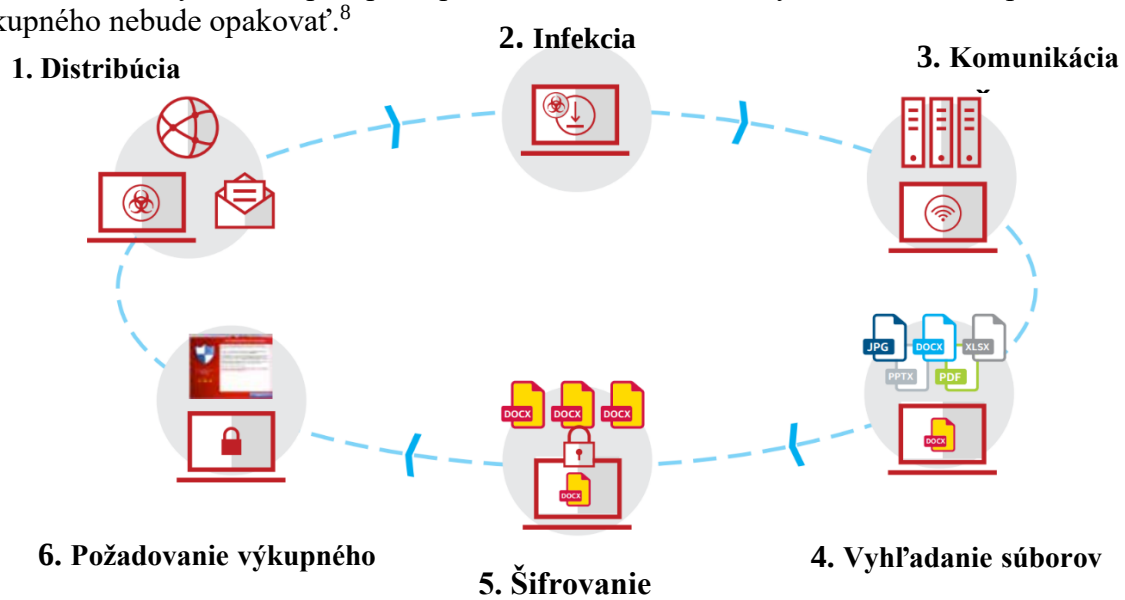
[5] SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware. Security Response*. [online] [cit. 23.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[6] LISKA, A., GALLO, T. *Ransomware: Defending Against Digital Extortion.* p.11

[7] LEONG R. *Understanding ransomware & Startegies to defeat it, Mcafee Labs*. [online] [cit. 26.03.2018]. Dostupné na internete: https://portal.mcafee.com/documents/Show/4121 /Show/4121

Priebeh ransomware útoku

Ransomware útoky sa pochopiteľne líšia v závislosti od ich typov, druhov alebo rodín. V priebehu typického šifrovacieho ransomware útoku však možno identifikovať šesť fáz. Za prvú fázu ransomware útoku možno považovať **distribúciu**. Ransomware používa štandardné spôsoby distribúcie škodlivého kódu. Môže sa šíriť prostredníctvom klasickej phishingovej schémy ako príloha e-mailu. Uvedený spôsob distribúcie je stále pomerne účinný aj napriek opakujúcim sa verejným výzvam a upozorneniam používateľov na riziká spojené s otváraním príloh neznámych e-mailov. Ransomware sa môže stiahnuť a nainštalovať na koncový bod aj prostredníctvom kompromitovanej webovej stránky alebo prostredníctvom drive-by-download. Druhým krokom je **infekcia systému**, kde škodlivý kód v systéme spustí procesy potrebné na dokončenie a maskovanie škodlivých aktivít. Po infikovaní napadnutého zariadenia sa môže začať šíriť na všetky dostupné zariadenia v sieti. V tretej fáze prebieha **komunikácia** so serverom, odkiaľ si škodlivý kód prevezme verejný kľúč potrebný na šifrovanie dát. Pomocou komunikácie s command-and-control serverom je možné odovzdávať ďalšie inštrukcie ako sú napríklad identifikácia typu súborov, ktoré sú cieľom šifrovania, či ako dlho čakať, než sa proces šifrovania začne. Štvrtým krokom je **vyhľadávanie**. Ransomware systematicky prehľadáva súbory a zvyčajne hľadá dáta, ktoré sú dôležité pre používateľa a nemožno ich jednoducho nahradiť. Zameriava sa zvyčajne na súbory s príponami .jpg, .docx, .xlsx, .pptx, .pdf a podobne. V piatej etape dochádza ku **šifrovaniu** vybraných súborov. Cieľové súbory sú najprv presunuté, následne šifrované a premenované. Šiestou a poslednou etapou je **požadovanie výkupného** za obnovenie prístupu k súborom. Po úspešnom ukončení šifrovania sa obeti zobrazí správa, nesúca informácie o kompromitovaní systému a nutnosti zaplatiť požadovanú sumu pre opätovné sprístupnenie súborov. Útočníci používajú rôzne metódy pre vynútenie rýchlej platby, či už je to dešifrovanie náhodného súboru zadarmo alebo zľava pri rýchlom zaplatení. Po zaplatení požadovaného výkupného však nie je žiadna záruka, že napadnuté súbory budú opäť prístupné, alebo že sa samotný útok a znovu požadovanie výkupného nebude opakovať.[8]



Obr. 1 Priebeh ransomware útoku[9]

[8] KREHEĽ, O. *Ransomware - a sneaky, dangerous cyber threat*. [online] [cit. 26.03.2018]. Dostupné na internete: https://www.csoonline.com/article/3170196/security/ransomware-is-a-sneaky-dangerous-cyberthreat.html

[9] LEONG R., 2017. *Understanding ransomware & Startegies to defeat it, Mcafee Labs*. [online] [cit. 26.03.2018]. Dostupné na internete: https://portal.mcafee.com/documents/Show/4121 /Show/412

Techniky používané ransomware-om

Kým všetky typy ransomware-u sú navrhnuté tak, aby získali peniaze od svojich obetí, môžu sa však úplne líšiť v použitých technikách.

Šifrovanie súborov - Moderné typy šifrovacieho ransomware-u používajú symetrické alebo asymetrické šifrovanie. Symetrické šifrovanie používa iba jeden kľúč na šifrovanie aj na dešifrovanie dát, pričom sa počas šifrovania spravidla generuje kľúč na infikovanom počítači a potom je zaslaný útočníkovi, alebo si ho malware vyžiada od útočníka pred šifrovaním súborov. V oboch prípadoch musí útočník zabezpečiť, aby ku kľúču nemal prístup používateľ napadnutého zariadenia. Zjavná nevýhoda symetrického šifrovania spočíva v používaní rovnakého kľúča. Predstavuje však zároveň jednoduchší a rýchlejší spôsob šifrovania veľkého množstva súborov a priečinkov. Asymetrické šifrovanie používa dva kľúče, z ktorých jeden je verejný a druhý súkromný. Verejný kľúč sa používa pre šifrovanie dát a súkromný pre ich dešifrovanie. Znalosť verejného kľúča neumožňuje sprístupnenie dát, ktoré možno dešifrovať iba súkromným kľúčom. Nevýhodou asymetrického šifrovania je nižšia rýchlosť v porovnaní so symetrickým šifrovaním, a teda väčšia šanca, že bude operácia odhalená predtým, než je šifrovanie dokončené. Niektoré šifrovacie typy ransomware-u používajú aj kombináciu symetrickej a asymetrickej techniky šifrovania.

Uzamykanie obrazovky - Väčšina typov locker ransomware-u používa podobnú stratégiu pre uzamknutie obrazovky počítača, kedy sa otvorí okno cez celú obrazovku (fullscreen) využívajúce plochu pre zobrazenie správy. Ransomware si môže vytvoriť okno sám alebo použiť okno prehliadača, ktoré je zobrazené ako jediné okno na virtuálnej ploche vytvorenej ransomware-om. Niektoré druhy locker ransomware-u môžu tiež kontrolovať plochu systému s cieľom uistiť sa, že ich okno zostane jediné aktívne a hlavné. Zobrazená správa sa spravidla stiahne z útočníkovho servera, čo umožňuje vytvárať lokalizované správy používajúce miestny jazyk a obrázky miestnych inštitúcii na základe určenia geografickej polohy podľa IP adresy infikovaného počítača. Ransomware tiež kontroluje procesy a aplikácie na pozadí, napríklad z dôvodu, aby používateľ nebol schopný ukončiť ransomware pomocou správcu úloh.

Uzamykanie prehliadača - Locker ransomware je tiež schopný uzamknúť webový prehliadač. Aby došlo k infikovaniu zariadenia ransomware-om, ktorý uzamyká prehliadač, musí používateľ spravidla cez daný prehliadač navštíviť server hosťujúci tento ransomware. Pôsobenie ransomware-u sa prejaví, keď používateľ chce opustiť stránku, pričom mu daná akcia nie je povolená. V niektorých prípadoch je však možné odísť ukončením procesu v správcovi úloh. Uzamykanie prehliadača nie je veľmi efektívna technika, ale vďaka jej jednoduchosti a univerzálnosti v rámci viacerých platforiem predstavuje pre útočníkov ďalšiu možnosť generovania príjmov.[10]

Uzamykanie Android zariadení - Ďalšia z techník sa týka zariadení, ktoré využívajú operačný systém Android. Ransomware vytvára bežné okná, prostredníctvom ktorých zobrazuje výhražnú správu používateľovi, napríklad s hrozbou, že bude zdieľať používateľove osobné údaje (fotky, správy, históriu webu, e-maily, históriu polohy atď.) so všetkými telefónnymi a e-mailovými kontaktmi. K zobrazovaniu okna dochádza tým, že ransomware neustále kontroluje aktivitu okna, zobrazuje ho a perióda medzi zatvorením a otvorením okna je natoľko krátka, že vytvára ilúziu neustále zobrazeného okna. Ako príklady možno uviesť

[10] SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware. Security Response*. [online] [cit. 27.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

WannaLocker, DoubleLocker, Koler alebo LeakerLocker. Ransomware na Android zariadení môže zmeniť aj bezpečnostný PIN kód na odomknutie zariadenia.[11]

Vektory ransomware útoku

Cieľom autorov ransomware-u je dostať ich škodlivý kód do zariadení potenciálnych obetí a na to, aby to dosiahli, používajú niekoľko metód.

Škodlivé prílohy a odkazy v e-mailových správach – Medzi najvyužívanejšie distribučné kanály patrí nevyžiadaná pošta (spam). Tak ako aj pri iných typoch škodlivého softvéru, sa autori ransomware-u snažia rôznymi spôsobmi presvedčiť používateľov, aby otvorili škodlivú prílohu, alebo klikli na škodlivý odkaz. Nevyžiadaná pošta môže obsahovať škodlivú prílohu ako napríklad súbory JavaScriptu, spustiteľné súbory, dokumenty MS Office s makrami a pod. Otvorením takejto prílohy môže dôjsť priamo k stiahnutiu ransomware-u alebo stiahnutiu tzv. downloaderu, ktorý následne stiahne samotný ransomware. V druhom prípade môže e-mail obsahovať odkaz, ktorý po rozkliknutí začne sťahovanie a následnú inštaláciu ransomware-u. Uvedený odkaz môže tiež viesť na stránku obsahujúcu exploit kit, prostredníctvom ktorého sa ransomware do zariadenia stiahne. Pri distribúcii spamových e-mailov dochádza v širokej miere k využívaniu techník sociálneho inžinierstva. Predmetné e-mailové správy sú napísané v príslušnom jazyku a môžu sa maskovať ako správy odoslané od lokálnych reálnych inštitúcii ako napríklad energetické spoločnosti, polícia, finančný úrad a pod.[12]

Kompromitované webové stránky – Vektorom ransomware útoku môžu byť aj kompromitované webové stránky. Výhodou tohto prístupu je to, že na rozdiel od škodlivých e-mailových správ, sa tu nevyžaduje sociálne inžinierstvo ani iné techniky k presvedčeniu obete kliknúť na škodlivú webovú adresu. Potenciálna obeť môže dobrovoľne navštíviť svoj obľúbený blog alebo inú webovú stránku, kde bude okamžite automaticky presmerovaná na stránku so správou, že aktuálna verzia internetového prehliadača potrebuje aktualizáciu. Následne sa zobrazí výzva na stiahnutie a spustenie aktualizácie softvéru. Po vykonaní tejto akcie sa aktivuje ransomware.

Malvertising - Ďalším bežným spôsobom, ako infikovať počítač ransomware-om, je zneužitie reklamy. Potenciálna obeť navštívi legitímnu stránku, ktorá zobrazuje reklamy poskytované treťou stranou. Ak niektorá zo zobrazených reklám obsahuje škodlivý kód, pokúsi sa v prehliadači používateľa využiť zraniteľnosť, ktorá ešte nebola aktualizáciou odstránená. Môže zneužiť aj zraniteľnosť nultého dňa, na ktorú neexistuje žiadna bezpečnostná záplata. Je menej pravdepodobné, že tento vektor útoku povedie k úspešnému útoku ransomware, pretože závisí od skutočnosti, že používateľ má vo svojom prehliadači nezabezpečenú zraniteľnosť. Na rozdiel od škodlivých príloh alebo odkazov v e-mailových správach k infikovaniu nie je potrebná žiadna aktivita zo strany obete.

Exploit kity - Exploit kit je sofistikovaný kód, ktorý je umiestnený na škodlivých alebo kompromitovaných webových stránkach. Exploit kit skenuje ľubovoľný počítač, ktorý navštívi danú stránku, či neobsahuje niektorú zo známych nezabezpečených zraniteľností, pričom využije akúkoľvek, ktorú nájde k tomu, aby prevzal kontrolu nad počítačom. Prostredníctvom exploit kitov došlo k šíreniu ransomware-u CryptoWall, TeslaCrypt alebo Locky.[13]

---

[11] CORRIGAN, C. *What all Android users need to know about ransomware*. [online] [cit. 29.04.2018]. Dostupné na internete: https://www.avg.com/en/signal/android-ransomware-guide

[12] SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware. Security Response.* [online] [cit. 27.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[13] RUBBENS, P. *Understanding Ransomware Vectors Key to Preventing Attack*. [online] [cit. 29.03.2018]. Dostupné na internete: https://www.esecurityplanet.com/malware/prevent-ransomware-attack.html

Infikované súbory - Vektorom ransomware útoku môže byť aj stiahnutie súboru, ktoré inicioval nič netušiaci používateľ. Ransomware môže byť umiestnený v hudobných alebo filmových súboroch a tiež aj v nelegálnych programoch, ktoré sú sprístupnené na warezových fórach a podobne.

Mobilné aplikácie - Sťahovanie infikovaných súborov vo forme aplikácií môže ovplyvniť aj mobilné zariadenia. Oficiálne obchody s aplikáciami spoločnosti Apple a Google môžu obsahovať škodlivé aplikácie aj napriek tomu, že sú pravidelne kontrolované. Zariadenia s iOS po jailbrake-u a ľubovoľné zariadenie Android môže byť nakonfigurované na prevzatie a inštaláciu aplikácií z tretích strán, ktoré sú mimo kontroly Apple alebo Google.

Aplikácie na odosielanie správ – Útočníci môžu posielať škodlivé správy prostredníctvom chatovacích aplikácií ako napríklad Viber, Whatsapp alebo Facebook messenger. Takáto správa môže obsahovať obrázok vo formáte SVG (Scalable Graphics File), ktorý má v sebe vloženú časť škodlivého kódu v jazyku JavaScript. Otvorenie uvedeného obrázka nasmeruje obeť na video na falošnom webe YouTube, kde následne požaduje inštaláciu kodekov. V skutočnosti je to škodlivé rozšírenie do prehliadača Chrome, ktoré spustí downloader a následne počítač infikuje ransomware-om. Tento vektor útoku využíval ransomware Locky.[14]

Samovoľné šírenie - Nové typy ransomware-u, niekedy nazývané ransomworm alebo ransomware worm, sú schopné po infikovaní jedného systému infikovať ostatné systémy v rámci internej siete spoločnosti. Ako príklady možno uviesť WannaCry, Petya/NotPetya, Bad Rabbit.[15]

Ciele útoku

Kybernetickí zločinci, ktorí stoja za ransomware útokmi, sa nestarajú o to, kto sú ich obete, pokiaľ sú ochotné zaplatiť výkupné. Obeťami ransomware-u sa môžu stať milióny používateľov po celom svete a ak len malé percento z nich zaplatí výkupné, ransomware útok bude úspešný.

Jednotlivci - Ransomware je veľmi efektívny voči jednotlivcom, ktorí nemajú základné bezpečnostné návyky v online prostredí. V súkromných domácich zariadeniach majú používatelia uložené citlivé informácie, súbory a dokumenty, ktoré sú pre nich cenné a nenahraditeľné. Napriek tomu, že uvedené dáta majú hodnotu, domáci používatelia vo väčšine prípadov nemajú žiadnu zálohovaciu stratégiu pre prípad krádeže, straty alebo poškodenia. A už vôbec nemyslia na vytváranie záloh pre úspešnú obnovu súborov po kryptografickom útoku ransomware-u. Aj keď má domáci používateľ vytvorené zálohy, niektoré útoky odstránia všetky druhy záloh na disku, vrátane tieňovej kópie systému Windows, a zašifrujú zálohované súbory na externých pamäťových zariadeniach, ktoré sú pripojené k počítaču. Moderné typy môžu zašifrovať aj zálohy a súbory uložené na cloudovom úložisku alebo na inom zariadení v lokálnej sieti.[16]

Podnikateľské subjekty - Pre mnohé spoločnosti sú informácie a technológie, ktoré používajú, nevyhnutné na vykonávanie ich každodennej činnosti. Počítače v podnikoch obsahujú citlivé údaje a kriticky dôležité dokumenty ako sú zákaznícke databázy, podnikateľské plány, návrhy, správy, zdrojové kódy, formuláre, účtovníctvo a pod. Moderné kryptografické hrozby môžu zasiahnuť a šifrovať všetky dostupné lokálne sieťové jednotky a

[14] RUBBENS, P. *Understanding Ransomware Vectors Key to Preventing Attack*. [online] [cit. 29.03.2018]. Dostupné na internete: https://www.esecurityplanet.com/malware/prevent-ransomware-attack.html

[15] O'BRIEN, D. *Ransomware 2017: An ISTR Special Report.* [online] [cit. 21.03.2018]. Dostupné na internete: https://www.symantec.com/content/dam/symantec/docs/security-center/whitepapers/istr-ransomware-2017-en.pdf

[16] VESELÝ, P., GREGUŠ, M., BEŇOVÁ, E. *Current Approaches to Increased Protection against Trojan Horses in Cloud Server Solutions.* p.1094

servery. To znamená, že jednou crypto ransomware infekciou môžu byť negatívne ovplyvnené viaceré systémy. Strata predmetných informácií má zvyčajne katastrofický vplyv na podnikanie. Organizácie bývajú často oveľa ochotnejšie zaplatiť výkupné, a to aj vo vyšších sumách, než býva požadované pri jednotlivých používateľoch, s cieľom získať späť dáta potrebné na ich prevádzku. Mnohé spoločnosti majú zavedený pomerne efektívny proces zálohovania dát, stále sa však nájde veľké množstvo spoločností, ktoré najmä z ekonomických dôvodov nemajú žiadnu zálohovaciu stratégiu.

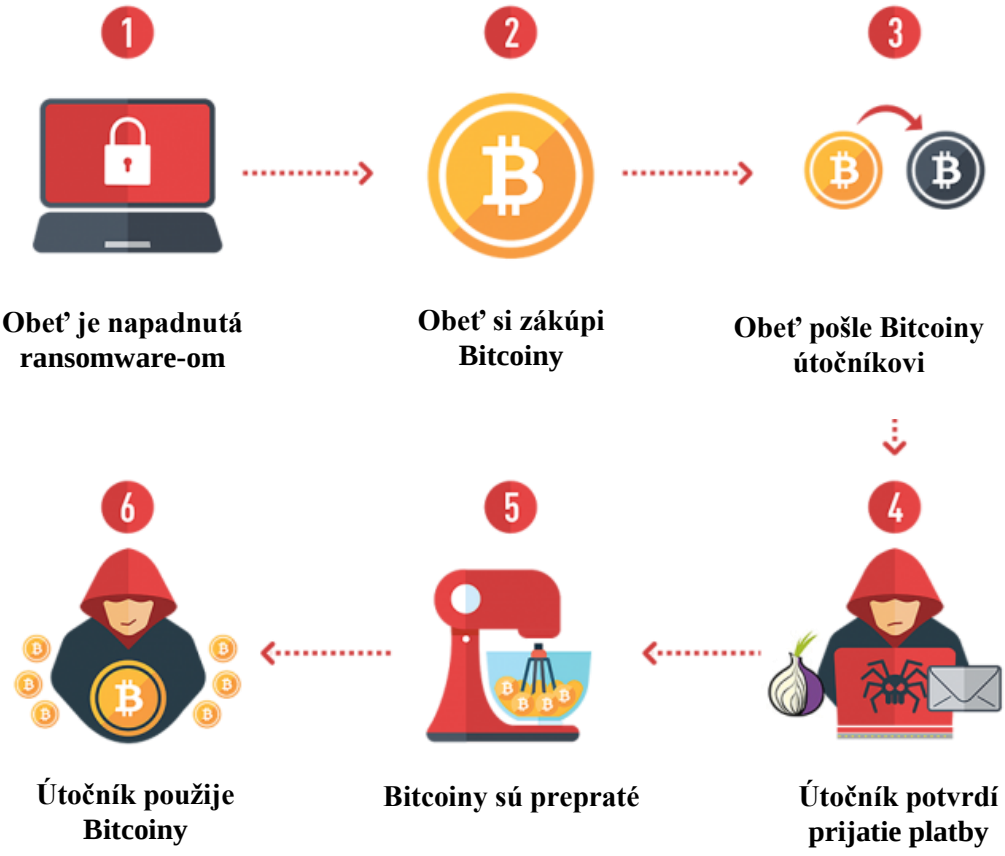
Verejné inštitúcie a organizácie – Ransomware útoky môžu zasiahnuť aj verejné inštitúcie ako sú rôzne úrady, univerzity, nemocnice a pod. Niektoré formy ransomware-u sú na uvedené organizácie špecificky a cielene zamerané. Nie sú vylúčené ani ransomware útoky na orgány verejnej správy a kritickú infraštruktúru, čo môže mať obrovské negatívne dopady na fungovanie samotného štátu. Útočníci veria, že nebudú odhalení a trestno-právne postihnutí, pretože väčšinou operujú z krajín s odlišnou legislatívou.[17]

Spôsoby zaplatenia výkupného

S dvoma hlavnými typmi ransomware-u sa spájajú aj dve hlavné metódy platby výkupného. V prípade locker ransomware-u ide spravidla o peňažné úhrady ako je napr. Ukash, Paysafecard, CashU alebo MoneXy. Následne sú takto získané finančné prostriedky často preprané cez webové stránky ponúkajúce online stávkovanie, z ktorých sú presunuté na predplatené karty. Šifrovací ransomware využíva kryptomeny a v súčasnosti je stále najviac používaná kryptomena Bitcoin. Kryptomenu je vo všeobecnosti vďaka jej podstate oveľa ťažšie vystopovať. Existujú služby, ktoré umožňujú pranie kryptomien, pri ktorom dochádza k miešaniu kryptomeny pochádzajúcej z legálneho obchodovania s kryptomenou získanou nelegálnou činnosťou.[18] Presný proces platby sa môže líšiť medzi rodinami ransomware-u, avšak typický proces platby výkupného zvyčajne vyzerá nasledovne:

[17] SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware. Security Response.* [online] [cit. 27.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[18] LEE, B. *Ransomware: Unlocking the lucrative criminal business model*. [online] [cit. 21.03.2018]. Dostupné na internete: https://www.paloaltonetworks.com/resources/research/ransomware-report



Obr. 2 Proces platby výkupného[19]

1. Obeti je zobrazená správa s požiadavkami útočníkov, ktorá môže obsahovať pokyny podrobne popisujúce proces zakúpenia Bitcoinov za účelom platby výkupného.
2. Obeť si zakúpi Bitcoiny, ktoré sú potrebné na zaplatenie výkupného.
3. Obeť pošle peniaze vo forme Bitcoinov na útočníkovu Bitcoin peňaženku.
4. Útočník potvrdí platbu prostredníctvom e-mailovej správy alebo stránky Tor a pokiaľ má obeť šťastie, poskytne prostriedky na dešifrovanie súborov obete.
5. Bitcoiny sa môžu prepať v službe na mixovanie kryptomien, ktorá vymení nelegálne získané Bitcoiny za iné Bitcoiny v rovnakej hodnote. Služba si za uvedenú funkciu odráta malú províziu.
6. Útočníci môžu používať Bitcoiny priamo na nákup tovaru, môžu s nimi obchodovať na obchodnej burze, alebo ich vymeniť za iné meny.

Ransomware ako služba

Služba Ransomware-as-a-Service (RaaS) je navrhnutá tak, aby ktokoľvek bez ohľadu na jeho technické znalosti a zručnosti, mohol uskutočniť ransomware útok. Prakticky ide o možnosť vytvoriť a zakúpiť si ransomware bez potreby disponovať nevyhnutnými odbornými schopnosťami pre jeho vytvorenie, šírenie alebo údržbu. Objednávateľ si môže v ponuke jednoducho vybrať výšku požadovaného výkupného, text a jazyk zobrazenej správy ako aj spôsob, akým sa bude ransomware šíriť.[20] Aj keď to nie je nový trend, uvedený model sa rýchlo

[19] EMISOFT. Spotlight on ransomware: Ransomware payment method. [online] [cit. 25.03.2018]. Dostupné na internete: https://blog.emsisoft.com/en/28256/ransomware-payment-methods/

[20] VIRY.CZ. Vyrob si svoji havěť! [online] [cit. 29.03.2018]. Dostupné na internete: https://www.viry.cz/satan-vyrob-si-svoji-havet/

rozvíja a čoraz väčší počet tvorcov ransomware-u ponúka svoje škodlivé produkty. Dochádza tým k vytvoreniu schémy, kedy tvorca ransomware-u ponúka podiel z profitu na každej ransomware infekcii výmenou za to, že objednávateľ bude tento ransomware šíriť. V porovnaní s inými typmi malvéru, ktoré si k úspešným útokom vyžadujú vyššiu úroveň programovania a technických znalostí, sa ransomware dá jednoducho objednať a následne šíriť. Predmetná schéma je výhodná najmä pre aktérov, ktorí už disponujú vlastnými botnetmi, alebo majú prístup k veľkému množstvu kompromitovaných počítačov.

Trend RaaS je pravdepodobne jedným z hlavných dôvodov, ktoré stoja za obrovským nárastom úspešných ransomware útokov v minulom roku. Pozoruhodné príklady uvedeného trendu, ktoré sa objavili v posledných dvoch rokoch sú Petya/Mischa, Philadelphia, Cerber, MacRansom alebo Shark ransomware, ktorý bol neskôr rebrandovaný pod názvom Atom, kde ponúkal vysoký 80% podiel na zaplatenom výkupnom. Ďalšie populárne nástroje ako Satan sa prezentujú tým, že umožňujú distribúciu ransomware-u v priebehu minúty.[21] Obchodný model služby RaaS je jednoduchý a namiesto naprogramovania a nasadenia vlastného ransomware softvéru si útočník tento útok objedná, pričom objednávateľ získa vopred dohodnutý podiel zo zaplateného výkupného. Jediné čo objednávateľ potrebuje v prípade, že sa trhovisko alebo fórum nachádza na webových stránkach darknetu je prehliadač, ktorý umožňuje prístup k týmto doménam a kryptomenu, prostredníctvom ktorej odvádza alebo získava podiel za nástroj alebo službu podľa stanovených podmienok.[22] V niektorých prípadoch si objednávateľ môže pozrieť odhad svojich potenciálnych zárobkov predtým, než si takýto útok objedná.

Úspech uvedenej služby a rastúci dopyt podnecuje autorov ransomware-u k tomu, aby ponúkali stále nové a sofistikovanejšie formy. Nárast ponúk RaaS v kombinácii s rozsiahlymi možnosťami prispôsobenia, ktoré tieto platformy prinášajú znamená, že potenciálne obete čelia náporu ransomware-u nielen z hľadiska kvantity ale aj kvality a rozmanitosti.

Záver

Ransomware má za sebou dlhú a zaujímavú históriu. Úspešne prešiel od svojich skromných začiatkov, kedy sa šíril na disketách, do modernej podoby, kde používa pokročilé šifrovacie techniky a zameriava sa nielen na počítače, ale aj na prenosné zariadenia a smart telefóny. Neobmedzuje sa len na konkrétnu zemepisnú oblasť alebo konkrétny operačný systém. Škodlivé akcie môže vykonávať v ktorejkoľvek časti sveta, na ľubovoľnom počte zariadení a ohrozené sú zariadenia so systémom Android, iOS, Windows aj Linux. Spôsob kompromitácie zariadenia sa môže líšiť v závislosti od cieľa a vykonané kroky sú obmedzené samotnými možnosťami napadnutého zariadenia.

Popularita ransomware-u sa zvýšila, pretože bol úspešný. Ransomware sa prispôsobil a zmenil, aby splnil rastúce požiadavky svojich tvorcov. Vyvíjal sa od klasických podvodov využívajúcich menej presvedčivé metódy až po súčasné agresívne šifrovacie formy. Dnes sa ransomware útoky presúvajú z domácich používateľov a zameriavajú sa na firmy a organizácie, ktorých dáta majú značne vyššiu hodnotu. Podniky sú v mnohých prípadoch pod mimoriadnym tlakom na dodržanie konkrétnych termínov a aj to je jeden z dôvodov, prečo sú ochotnejšie zaplatiť výkupné a zaplatiť aj vyššie sumy.

Vzhľadom na zvyšujúcu sa popularitu nositeľných zariadení a zariadení internetu vecí možno predpokladať stupňujúci sa záujem útočníkov aj o uvedené zariadenia. Okrem tradičných zariadení ako sú počítače, notebooky, tablety a smart telefóny, na ktoré je dnes primárne cielená väčšina ransomware útokov, zraniteľné sú aj také zariadenia, ako napríklad smart hodinky, smart televízory, chladničky, vozidlá pripojené k sieti internet a pod. Pred

[21] CARBON BLACK. The Ransomware Economy. [online] [cit. 21.03.2018]. Dostupné na internete: https://cdn.www.carbonblack.com/wp-content/uploads/2017/10/CB-Ransomware-Economy-Report.pdf

[22] LIFARS. *How to Combat Ransomware A Complete Guide*. [online] [cit. 21.03.2018]. Dostupné na internete: https://lifars.com/knowledge-center/how-to-combat-ransomware/

ransomware útokmi nie sú v bezpečí dokonca ani roboty.[23] Z uvedeného je zrejmé, že existuje široká škála zariadení, na ktoré sa môžu útočníci prostredníctvom ransomware útokov zamerať. Útočníci budú pokračovať v ransomware útokoch dovtedy, pokiaľ im takéto konanie bude produkovať zisk. To znamená, že najlepším spôsobom ako zmierniť alebo zastaviť ransomware útoky, je znížiť ich finančné výnosy pre útočníkov. K tomu je potrebné podniknúť kroky naprieč všetkým platformám, ktoré smerujú k zníženiu rizika infekcie alebo zmierneniu následkov. Sú to najmä vytváranie pravidelných off-line záloh, aktualizovanie operačných systémov a aplikačného softvéru, zvyšovanie bezpečnostného povedomia používateľov, používanie vhodného bezpečnostného riešenia a spamového filtra, zakázanie spustiteľných súborov v prílohách e-mailových správ, nastavenie operačného systému na zobrazenie prípon súborov a zakázanie makier v kancelárskom balíku Microsoft Office.

Útočníci neustále hľadajú nové spôsoby, ako nájsť a zneužiť zraniteľnosti a slabé miesta obetí. Avšak pre každú novú taktiku, ktorú útočníci použijú, existuje protiopatrenie ako sa chrániť.

Zoznam použitej literatúry a iných zdrojov:

CARBON BLACK. *The Ransomware Economy.* [online] [cit. 21.03.2018].
Dostupné na internete: https://cdn.www.carbonblack.com/wp-content/uploads/2017/10/CB-Ransomware-Economy-Report.pdf

CORRIGAN, C. *What all Android users need to know about ransomware.* [online] [cit. 29.03.2018].
Dostupné na internete: https://www.avg.com/en/signal/android-ransomware-guide

EMISOFT. *Spotlight on ransomware: Ransomware payment method.* [online] [cit. 25.03.2018].
Dostupné na internete: https://blog.emsisoft.com/en/28256/ransomware-payment-methods/

KREHEĽ, O. *Ransomware - a sneaky, dangerous cyber threa.t* [online] [cit. 26.03.2018].
Dostupné na internete: https://www.csoonline.com/article/3170196/security/ransomware-is-a-sneaky-dangerous-cyber-threat.html

LEE, B. *Ransomware: Unlocking the lucrative criminal business model*. Palo Alto Networks USA [online] [cit. 21.03.2018].
Dostupné na internete: https://www.paloaltonetworks.com/resources/research/ransomware-report

LEONG R. *Understanding ransomware & Startegies to defeat it*. Mcafee Labs. [online] [cit. 26.03.2018]. Dostupné na internete: https://portal.mcafee.com/documents/Show/4121

LIFARS. *How to Combat Ransomware A Complete Guide.* [online] [cit. 21.03.2018]. Dostupné na internete: https://lifars.com/knowledge-center/how-to-combat-ransomware/

LIFARS. *Robots are Now Vulnerable to Ransomware Attacks.* [online] [cit. 23.03.2018].
Dostupné na internete: https://lifars.com/2018/03/robots-now-vulnerable-ransomware-attacks/

LISKA, A., GALLO, T. *Ransomware: Defending Against Digital Extortion*. USA: O'Reilly Media, 2016, 182 p. ISBN 978-1-491-96788-1

O'BRIEN, D. *Ransomware 2017: An ISTR Special Report.* Symantec. [online] [cit. 21.03. 2018]. Dostupné na internete:
https://www.symantec.com/content/dam/symantec/docs/security-center/whitepapers/istr-ransomware-2017-en.pdf.

PALISSE, A. et al. *Ransomware and the Legacy Crypto API.* France: Revised Selected Papers. 239p. ISN:978-3-319-54875-3

[23] LIFARS. *Robots are Now Vulnerable to Ransomware Attacks* [online] [cit. 23.03.2018]. Dostupné na internete: https://lifars.com/2018/03/robots-now-vulnerable-ransomware-attacks//

PC REVUE. *Čo je ransomware a prečo by vás mal zaujímať?* [online] [cit. 25.03.2018]. Dostupné na internete: https://www.pcrevue.sk/a/Trend-Micro--Co-je-ransomware-a-preco-by-vas-mal-zaujimat
RUBBENS, P. *Understanding Ransomware Vectors Key to Preventing Attack.* [online] [cit. 29.03.2018]. Dostupné na internete: https://www.esecurityplanet.com/malware/prevent-ransomware-attack.html
SAVAGE, K., COOGAN, P., LAU, H. *The evolution of ransomware.* Security Response. California: Symantec, 2015, [online] [cit. 27.03.2018]. Dostupné na internete: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
URBAN, F. *Peniaze alebo dáta: hrozivý vzostup ransomware.* [online] [cit. 22.03.2018]. Dostupné na internete: https://touchit.sk/peniaze-alebo-data-hrozivy-vzostup-ransomware/58530
VESELÝ, P., GREGUŠ, M., BEŇOVÁ, E. *Current Approaches to Increased Protection against Trojan Horses in Cloud Server Solutions.* In: CBU International Conference Proceedings, vol. 5, Prague, Central Bohemia University, 2017, pp. 1092-1095. Print ISSN 1805-997X, Online ISSN 1805-9961
VIRY.CZ. *Vyrob si svoji havěť!* [online] [cit. 29.03.2018]. Dostupné na internete: https://www.viry.cz/satan-vyrob-si-svoji-havet/

Kontaktné údaje:
JUDr. Marek Petrik
Katedra informatiky a manažmentu – externý doktorand
Akadémia PZ v Bratislave
marek.petrik4@minv.sk

Možnosti stanovenia výšky škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov

Peter Polák, Tomáš Trúsik

Abstrakt:
Obsah príspevku je v súlade s jeho názvom zameraný na všeobecné vysvetlenie pojmu škoda a výška škody spôsobenej počítačovými trestnými činmi, na analýzu typov neoprávnených zásahov do počítačových systémov a programov, ktorými je spôsobená škoda, ako aj na predstavenie metód určenia škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov.
Kľúčové slová:
informačný systém, počítačový údaj, neoprávnené zásahy do počítačových systémov a údajov, počítačový trestný čin, škoda spôsobená počítačovými trestnými činmi, stanovenie výšky škody

Abstract:
This article is analyzing damage resulting of unauthorized interference with computer systems. The main focus is put to point out different types of impacts, present methods of determining the financial loss for use in criminal procedure and propose more precise market approach for calculating the damage. It comes together with analysis of current legal environment and laws that are to be used in cybercrime proceedings.
Key words:
information system, computer system, computer data, unauthorized interference with computer data and systems, cybercrime, damage caused by cybercrime, calculation of the financial losses

Úvod

Rozvoj ľudskej spoločnosti je v súčasnosti spojený predovšetkým so spracovávaním a využívaním informácií, pričom spôsoby spracovávania a využívania informácií ovplyvňujú všetky sféry spoločnosti. Informačné a komunikačné technológie, ako ich poznáme dnes, sa zrodili koncom 20. storočia spojením počítačov, masovokomunikačných prostriedkov a telekomunikačných sietí. S rozvojom a využívaním informačných a komunikačných technológií sú spojené aj negatívne javy, ktoré môže mať charakter neoprávneného nakladania s informačnými systémami, počítačovými programami a počítačovými údajmi, a teda aj charakter takzvaných počítačových trestných činov. Preto možno počítačovú (kybernetickú) kriminalitu označiť za jeden z negatívnych sprievodných fenoménov informatizácie spoločnosti. V čase, kedy sa počítače stali súčasťou nášho každodenného života a nájdeme ich v každom úradnom priestore, ba takmer v každej domácnosti, je aj páchanie trestnej činnosti súvisiacej s počítačmi oveľa jednoduchšie.

Počítačová (kybernetická) kriminalita spočíva teda v zneužívaní alebo vo využívaní informačných technológií, najmä počítačov, počítačových sietí a iných zariadení spôsobilých spracovať a prenášať informácie v digitálnej podobe (informačné systémy) na páchanie trestnej činnosti. Jej rozmach je priamo úmerný postupujúcej informatizácii spoločnosti. Rozvinuté krajiny sveta, a teda aj európske krajiny, považujú túto formu trestnej činnosti za jednu z globálnych hrozieb. Preto sa na národných úrovniach, ale aj na úrovniach nadnárodných, prijímajú okrem iného aj legislatívne opatrenia na jej potieranie. Aj napriek neustále sa rozvíjajúcej legislatíve, reflektujúcej na oblasť počítačových trestných činov a autorského práva, sa pri jej aplikácií v praxi stretávame s problémami. Jedným z dôvodov je nedostatok kvalifikovaných ľudí , ktorí by túto legislatívu , ktorá má objektívne špecifický charakter, vedeli efektívne využívať na jej účel. Medzi ďalšie dôvody problémov patrí nedostatočná súčinnosť právnikov a informatikov pri normotvornej činnosti, a potom aj pri využívaní výsledkov tejto činnosti. Z toho vznikajú situácie, kedy sa jednotlivé súvisiace ustanovenia Trestného zákona v procese dokazovania počítačových trestných činov uplatňujú s ťažkosťami. Medzi parciálne problémy dokazovania počítačovej trestnej činnosti patrí aj problém stanovenia výšky škody, spôsobenej takouto trestnou činnosťou.

Legislatívny rámec postihovania neoprávneného nakladania s informačnými systémami , počítačovými programami a počítačovými údajmi

Vzhľadom na globálny charakter neoprávneného nakladania s informačnými systémami, počítačovými programami a počítačovými údajmi vytvorili v podmienkach nášho kontingentu Rada Európy a Európska únia viaceré nástroje , účelom ktorých je prijatie legislatívnych opatrení v jednotlivých signatárskych štátoch alebo v jednotlivých členských štátoch, zameraných na efektívny postih takýchto negatívnych prejavov. Základným nástrojom Rady Európy v tejto oblasti je Dohovor o počítačovej kriminalite (ďalej len „Dohovor").[1] Pokiaľ ide o základný nástroj takéhoto charakteru v pôsobnosti Európskej únie, tak tým predovšetkým je Smernica 2013/40/EÚ o útokoch na informačné systémy (ďalej len „Smernica".[2] Výsledkom implementácie týchto spomínaných nástrojov je súčasná úprava takzvaných počítačových trestných činov v osobitnej časti Trestného zákona (zákon č. 300/2005 Z.z. , ďalej „Trestný zákon"). S účinnosťou od 1. januára 2016 sa na základe novely Trestného zákona pôvodný trestný čin Poškodenia a zneužitia záznamu na nosiči informácií podľa § 247 pretransformoval do piatich rozličných trestných činov, tvoriacich v osobitnej časti Trestného zákona skupinu takzvaných „počítačových trestných činov". Konkrétne ide o trestný čin Neoprávneného prístupu do počítačového systému podľa § 247, Neoprávneného zásahu do počítačového systému podľa § 247a, Neoprávneného zásahu do počítačového údaja podľa § 247b, Neoprávneného zachytávania počítačových údajov podľa § 247c a o trestný čin Výroby a držby zariadenia, hesla do počítačového systému alebo iných údajov podľa § 247d. Ide o trestné činy, ktoré spája skutočnosť, že postihujú konanie, ktoré má charakter protiprávneho útoku na počítač, počítačový systém, počítačový program alebo na počítačový údaj.

V osobitnej časti Trestného zákona sú upravené ďalšie trestné činy, ktoré majú blízko ku skupine počítačových trestných činov. V tomto prípade však ide o trestné činy, ktoré postihujú konanie spočívajúce v použití počítačov a počítačových systémov na páchanie trestnej činnosti. Patria sem také trestné činy ako Výroba detskej pornografie podľa § 368, Rozširovanie detskej pornografie podľa § 369, Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení podľa § 370 a Porušovanie autorského práva podľa § 283. Okrem toho do kategórie takýchto trestných činov treba vzhľadom na znaky skutkovej podstaty zarátať aj trestný čin Neoprávneného obohatenia podľa § 226 Trestného zákona.

Jedným z predpokladov zistenia škôd spôsobených neoprávneným nakladaním s informačnými systémami, počítačovými programami a počítačovými údajmi je aj poznanie znakov skutkových podstát spomínaných počítačových trestných činov.

Prvým z týchto trestných činov je **neoprávnený prístup do počítačového systému podľa § 247 Trestného zákona**. Primárnym objektom pri tomto trestnom čine je ochrana integrity počítačového systému. Pri sekundárnom objekte môžeme hovoriť o ochrane dôvernosti počítačových dát. Hmotným predmetom v tomto prípade bude počítačový systém, ktorý bude neoprávnene sprístupnený prelomením jeho bezpečnostného opatrenia. Pri objektívnej stránke musí byť preukázané, že páchateľ dokázal prekonať bezpečnostné opatrenia, vďaka čomu sa mu podarilo získať neoprávnený prístup do počítačového systému alebo jeho časti. Páchateľom môže byť jednak fyzická osoba, a to každá fyzická osoba, ktorá je staršia ako štrnásť rokov a je zároveň príčetná a jednak právnická osoba, ktorá spĺňa podmienky podľa zákona č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb (ďalej

[1] Dohovor o počítačovej kriminalite. Rada Európy (otvorený na podpis v Budapešti 23.11.2001), Oznámenie Ministerstva zahraničných vecí SR č. 137/2008 Z. z. (pre Slovesnkú republiku sa stal platným dňom 1.5.2008)

[2] Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV. Úradný vestník Európskej únie, L 218/8, 14. august 2013.

len „ zákon o TZPO“). Z hľadiska subjektívnej stránky pôjde o zavinenie, ktoré vyžaduje podobu priameho alebo nepriameho úmyslu. .

Kvalifikovanej skutkovej podstaty tohto trestného činu podľa odseku 2 sa páchateľ dopustí, ak čin, ktorý je uvedený v prvom odseku, spácha a spôsobí ním značnú škodu, čo predstavuje škodu vo výške najmenej 26 600 Eur. Kvalifikovanej skutkovej podstaty podľa odseku 3 sa dopustí páchateľ, ktorý spáchaním trestného činu podľa odseku 1 spôsobí škodu veľkého rozsahu, teda škodu vo výške najmenej 133 000 Eur, alebo ak páchateľ vykoná tento trestný čin ako člen nebezpečného zoskupenia.[3]

Ako už bolo uvedené podmienkou spáchania trestného činu neoprávneného prístupu do počítačového systému je prekonanie bezpečnostného opatrenia počítačového systému a následný neoprávnený prístup do tohto systému alebo jeho časti. Pojem „bezpečnostné opatrenie“ možno definovať ako „opatrenie, ktoré môže preniknutie do počítačového systému zabrániť alebo sťažiť a ktorého cieľom je, aby páchateľ mal zabránený voľný prístup do počítača, pričom na miere zabezpečenia nezáleží. Spôsoby zabezpečenia počítačového systému sú rôzne. Môže ísť o prostriedky, ktoré sa nachádzajú priamo v počítači (napr. zabezpečovací softvér, používanie rôznych bezpečnostných a vstupných hesiel do počítača, obmedzovanie užívateľského rozhrania) alebo to môžu byť zabezpečovacie prostriedky mimo počítača (napr. hardwarové zabezpečenie alebo zabezpečenie miestnosti, kde sa nachádza počítačový systém technickými bezpečnostnými dverami, opatrenými skenerom). Trestný zákon priamo neurčuje, či bezpečnostné opatrenie musí byť umiestnené priamo v počítači, aj keď sa z logickej stránky veci predpokladá, že by malo byť.

Ďalším tzv. počítačovým trestným činom je trestný čin **neoprávneného zásahu do počítačového systému podľa § 247a Trestného zákona.** Primárnym objektom tohto trestného činu je vlastnícke právo. Vlastníckym právom v tomto prípade rozumie vlastníctvo k počítačovému systému a k údajom na ňom uchovávaných a spracovávaných, s ktorými ma právo nakladať a disponovať len oprávnený vlastník. Sekundárnym objektom je ochrana počítačového systému pred obmedzením alebo porušením jeho fungovania. Ako hmotný predmet útoku možno pri tomto trestnom čine vnímať počítačový systém, ktorý bude pod útokom za účelom prerušenia, narušenia alebo obmedzenia jeho fungovania. Tento trestný čin obsahuje dve alternatívy objektívnej stránky. Prvou je konanie spočívajúce v obmedzení alebo v prerušení fungovania počítačového systému alebo jeho časti neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov priamo páchateľom. Druhou alternatívou je konanie spočívajúce v obmedzení alebo v prerušení fungovania počítačového systému alebo jeho časti tým, že páchateľ urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnené zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu. Kumulácia konaní podľa uvedených alternatív sa nevyžaduje, avšak možno predpokladať, že v mnohých prípadoch k nej dôjde. Subjekt je vyjadrený všeobecne, páchateľom môže byť každá fyzická osoba, ktorá je staršia ako štrnásť rokov a je zároveň príčetná. Páchateľom môže byť aj právnická osoba. Subjektívna stránka vyžaduje zavinenie vo forme priameho alebo nepriameho úmyslu.

Kvalifikovanej skutkovej podstaty tohto trestného činu sa podľa odseku 2 môže dopustiť páchateľ tak, že konaním podľa odseku 1 spôsobí značnú škodu , čo je škoda vo výške

[3] Členom nebezpečného zoskupenia sa podľa § 141 Trestného zákona rozumie člen zločineckej skupiny alebo teroristickej skupiny. Zločineckou skupinou sa podľa § 129 ods. 4 Trestného zákona rozumie "štruktúrovaná skupina najmenej troch osôb, ktorá existuje počas určitého časového obdobia a koná koordinovane s cieľom spáchať jeden alebo viacej zločinov, a to trestný čin legalizácie príjmu z trestnej činnosti podľa § 233 alebo niektorý z trestných činov korupcie podľa ôsmej hlavy tretieho dielu osobitnej časti Trestného zákona za účelom priameho alebo nepriameho získania finančnej alebo inej výhody" Teroristickou skupinou sa podľa § 129 ods. 5 Trestného zákona rozumie štruktúrovaná skupina najmenej troch osôb, ktorá existuje počas určitého časového obdobia na účely spáchania trestného činu teroru alebo trestného činu terorizmu.

najmenej 26 600 Eur, ďalej že takým konaním spôsobí vážnu poruchu v činnosti štátneho orgánu, orgánu územnej samosprávy, súdu alebo iného orgánu verejnej moci, alebo že takým konaním zneužije osobné údaje iného s cieľom získať dôveru tretej strany.[4] V tomto prípade pôjde o konania, kde sa na základe neoprávnene získaných osobných údajov. bude páchateľ vydávať za poškodeného, aby v jeho mene od tretej strany získal prospech (napr. finančný, majetkový) alebo aby získal utajované informácie od tretej strany. Kvalifikovanej skutkovej podstaty tohto trestného činu sa podľa odseku 3 môže dopustiť páchateľ tak, že konaním podľa odseku 1 spôsobí škodu veľkého rozsahu (ide o sumu najmenej vo výške 133 000 Eur) alebo spôsobí vážnu poruchy v kritickej infraštruktúre[5] alebo že sa konania dopustí ako člen nebezpečného zoskupenia.

Na rozdiel od trestného činu neoprávneného prístupu do počítačového systému sa pri neoprávnenom zásahu do počítačového systému nevyžaduje pre vznik trestnej zodpovednosti prekonanie bezpečnostných opatrení resp. získanie neoprávneného prístupu. Práve naopak, je irelevantné, či bol prístup oprávnený alebo nie, podstatou je spôsobenie obmedzenia alebo prerušenia fungovania počítačového systému alebo jeho časti a to rôznymi, zákonom taxatívne vymenovanými spôsobmi.

Medzi počítačové trestné činy patrí aj trestný čin **neoprávneného zásahu do počítačového údaja podľa § 247b Trestného zákona**. Primárnym objektom tohto trestného činu je ochrana integrity počítačových údajov, ktoré sú uschované v počítačovom systéme. Ako sekundárny objekt tu možno vnímať ochranu dôvernosti počítačových dát a integrity, poprípade aj ochranu obchodného, bankového, daňového a iného tajomstva uloženého vo forme dát, teda ochranu dát pred ich prípadným zničením, poškodením, vymazaním a pod. Objektívna stránka spočíva v tom, že páchateľ svojim konaním (napr. použitím škodlivého softvéru) úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti. Páchateľom môže byť jednak fyzická osoba, a to každá fyzická osoba staršia ako štrnásť rokov, ktorá je v čase spáchania činu príčetná. Páchateľom tohto trestného činu môže byť aj právnická osoba. Subjektívna stránka tohto trestného činu vyžaduje zavinenie vo forme priameho alebo nepriameho úmyslu. Kvalifikované skutkové podstaty tohto trestného činu, sú identické so skutkovou podstatou trestného činu neoprávneného zásahu do počítačového systému podľa § 247a Trestného zákona, nakoľko sú tieto trestné činy pomerne podobné. Odlišný je len následok, forma páchania je sčasti rovnaká.

Možno povedať, že trestný čin neoprávneného zásahu do počítačového systému podľa § 247a Trestného zákona je k trestnému činu neoprávneného zásahu do počítačového údaja

[4] Pojem osobné údaje je definovaný v zákone č. 122/2013 Z. z. zákon o ochrane osobných údajov v § 4 ods. 1, kde „osobnými údajmi sú údaje týkajúce sa určenej alebo neurčenej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, ekonomickú, kultúrnu alebo sociálnu identitu.“ Od 25.5. 2018 nadobúda účinnosť nový zákon o ochrane osobných údajov č. 18/2018 Z.z., pričom tento v § 2 definuje osobné údaje ako „údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu“.

[5] Pojem kritická infraštruktúra je definovaný v zákone č. 45/2011 Z. z. o kritickej infraštruktúre, kde v § 2, písm. a) je uvedené, že „prvkom kritickej infraštruktúry sa rozumie najmä inžinierska stavba, služba vo verejnom záujme a informačný systém v sektore kritickej infraštruktúry, ktorých narušenie alebo zničenie by malo podľa sektorových kritérií a prierezových kritérií závažné nepriaznivé dôsledky na uskutočňovanie hospodárskej a sociálnej funkcie štátu, a tým na kvalitu života obyvateľov z hľadiska ochrany ich života, zdravia, bezpečnosti, majetku, ako aj životného prostredia.“ Zákon týmto spôsobom chráni inštitúcie, akými sú Policajný zbor, Hasičský a záchranný zbor, sieť nemocničných zariadení a iné hospodárske alebo sociálne významné inštitúcie. Ich ohrozením by nehrozila len veľká majetková škoda, ale mohlo by dôjsť k značnému ohrozeniu ľudského zdravia a života – pozn. autorov.

podľa § 247b Trestného zákona vo vzťahu špeciality, pretože ak páchateľ napríklad poškodí údaje a obmedzí fungovanie počítačového systému, môže byť proti nemu vyvodená trestná zodpovednosť len za trestný čin neoprávneného zásahu do počítačového systému podľa § 247a Trestného zákona a nie za trestný čin neoprávneného zásahu do počítačového údaja podľa § 247b Trestného zákona. Ak by však došlo len k poškodeniu údajov bez toho, aby bola ovplyvnená funkčnosť počítačového systému, pôjde výhradne len o trestný čin neoprávneného zásahu do počítačového údaja podľa § 247b Trestného zákona. Spravidla sa najčastejšie páchateľ dopustí tohto trestného činu v jednočinnom súbehu s trestným činom neoprávneného prístupu do počítačového systému podľa § 247 Trestného zákona.

Ďalším v poradí počítačovým trestným činom, upraveným v osobitnej časti Trestného zákona, je trestný čin neoprávneného zachytávania počítačových údajov podľa § 247c Trestného zákona.

Objektom trestného činu neoprávneného zachytávania počítačových údajov je predovšetkým právo na súkromie a to v podobe korešpondencie, resp. ochrany tajomstva prepravovaných správ pomocou elektronickej komunikácie a ochrana počítačových dát prenášaných buď do vnútra počítačového systému alebo z vnútra počítačového systému. Pokiaľ ide o objektívnu stránku, tak tohto trestného činu sa môže páchateľ dopustiť alternatívnym konaním uvedeným v odseku 1 a v odseku 2 jeho skutkovej podstaty. Podľa odseku 1 sa tohto trestného činu dopustí ten, „kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje“. Prvým predpokladom vyvodenia trestnej zodpovednosti podľa tohto ustanovenia je teda neoprávnené zachytávanie počítačových údajov. Pojem neoprávnený sa v tomto ustanovení chápe ako konanie, na ktoré nemá subjekt oprávnenie vyplývajúce mu zo zákona, zmluvy alebo iného všeobecne záväzného právneho predpisu. Čo sa týka využitia technického prostriedku, ktorý má byť použitý priamo pri vykonávaní tohto zachytávania , tak prichádzajú do úvahy technické prostriedky hardvérového alebo softvérového charakteru. Ďalším znakom je zachytávanie takých prenosov počítačových údajov, ktoré sú neverejné. V tejto súvislosti treba upozorniť na na skutočnosť, že ide o neverejnosť prenosov počítačových údajov a nie o neverejnosť samotných údajov. To znamená, že dáta, ktoré sú predmetom prenosu, môžu byť verejne dostupné a nemusí ísť o utajované informácie (napr. obchodné tajomstvo, daňové tajomstvo a pod.). Ďalším znakom vyplývajúcim z ustanovenia odseku 1 tohto trestného činu je, že sa neoprávnene zachytávajú údaje, ktoré smerujú do počítačového systému, z neho, alebo v jeho rámci. Údaje smerujúce do počítača môžu byť buď údaje z iného počítačového systému, napríklad cez email, sociálnu sieť a pod., alebo údaje, ktoré sa dostávajú do počítača pomocou vstupných a vstupno-výstupných zariadení ako napríklad klávesnica, mikrofón, USB kľúč, modem a pod. Údaje smerujúce z počítačového systému môžu byť údaje, ktoré smerujú do iného počítačového systému alebo údaje z výstupných alebo vstupno-výstupných zariadení. Medzi tieto patria napríklad čítačka pamäťových kariet, monitor, tlačiareň a pod. Údaje smerujúce v jeho rámci bývajú najčastejšie tie, ktoré smerujú napríklad z operačnej pamäte do operačnej jednotky alebo údaje smerujúce z riadiacej jednotky do operačnej pamäte. Posledným znakom objektívnej stránky podľa ustanovenia odseku 1, ktorý je alternatívny, je zachytávanie počítačových údajov pomocou elektromagnetických emisií (vyžarovania) z počítačového systému. Samotné elektromagnetické emisie nie je možné považovať za počítačový údaj, avšak ich kolekciou je možné tento údaj rekonštruovať a tak získať relevantnú informáciu. Emisie sú vyžarované pri bežnom používaní z monitorov počítačových systémov a z tlačiarní, ktoré je možné zachytávať pomocou antén a následne ich rekonštruovať a prehrať v dátovej podobe. Emisie dokonca vyžaruje aj procesor počítača. Toto vyžarovanie nastáva vtedy, keď elektrický prúd zmení napätie a tým vytvorí elektromagnetické impulzy, ktoré vyžarujú ako neviditeľné rádiové vlny.

Obdobným spôsobom funguje vyžarovanie aj pri počítačových monitoroch. Monitory, ktoré obsahujú systém CRT (cathode ray tube), obsahujú elektrónovú pištoľ v zadnej časti obrazovej trubice, ktorá prenáša lúč elektrónov. Keď elektróny narazia na obrazovku, spôsobia, že sa obrazové body rozsvietia (fluoreskujú). Tento lúč prechádza obrazovku v rýchlych intervaloch zhora dole, vypínajúc sa a zapínajúc, čím spôsobuje zobrazovanie obrázka na monitore. Tieto zmeny následne vo vysokonapäťovom systéme monitora generujú signál, ktorý sú páchatelia schopní zachytiť a tým rekonštruovať vyžarované emisie vo výsledný dátový údaj. Káble od monitora, ktoré sú pripojené do počítača a sú nechránené, tento signál ešte na princípe antény zosilňujú, a tak umožňujú ľahšie zachytávanie emisií. Zachytávanie počítačových údajov pomocou elektromagnetických emisií (vyžarovania) z počítačového systému je technicky veľmi náročné a preto možno tento spôsob neoprávneného zachytávania počítačových údajov považovať za málo pravdepodobný.

Podľa odseku 2 sa tohto trestného činu dopustí ten, kto „ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby“. Pre naplnenie znakov objektívnej stránky podľa odseku 2 je teda nutné, aby bol páchateľ zamestnancom poskytovateľa elektronickej komunikačnej služby[6] a aby alternatívne konal podľa niektorého z troch alternatívnych konaní. Prvý spôsob konania spočíva v tom, že sa zamestnanec dopustí konania, ktoré je uvedené v odseku 1. Druhým spôsobom konania je, ak zamestnanec konanie uvedené v odseku 1 úmyselne umožní spáchať niekomu inému. Umožnenie môže nastať dvoma spôsobmi a to aktívnym alebo pasívnym spôsobom. Pasívnym spôsobom by bolo konanie uskutočnené ak by zamestnanec vedel o tom, že niekto neoprávnene zachytáva počítačové údaje a úmyselne to dovolí a neinformuje o tom zamestnávateľa, orgán činný v trestnom konaní alebo iný relevantný subjekt. Aktívnym spôsobom sa zamestnanec priamo podieľa napríklad na zjednodušení prístupu do tejto siete pre páchateľa a podobne. Tretí spôsobom konania spočíva v tom, že zamestnanec pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby. Pri pozmenení páchateľ v správe zmení jej obsah, vymaže jej časť alebo pridá nežiadaný obsah. Potlačením sa rozumie najmä zamedzenie toho, aby príjemca správu prijal, alebo aby ju po prijatí nebol schopný prečítať.

Subjektom tohto trestného činu v skutkovej podstate podľa odseku 1 môže byť akákoľvek fyzická alebo právnická osoba, ktorá spĺňa predpoklady vyvodenia trestnej zodpovednosti voči nej. V skutkovej podstate podľa odseku 2 ide o špeciálny subjekt a to zamestnanca poskytovateľa elektronickej komunikačnej služby. V tomto prípade môžu byť páchateľom len o fyzické osoby, nakoľko právnické osoby nemôžu byť zamestnancom poskytovateľa elektronickej komunikačnej služby. Subjektívna stránka rovnako ako pri ostatných počítačových trestných činoch vyžaduje zavinenie vo forme priameho alebo nepriameho úmyslu.

Kvalifikované skutkové podstaty tohto trestného činu, sú identické so skutkovými podstatami už uvedených počítačových trestných činov. Na viac je však v písmene a) odseku 3 upravená kvalifikovaná skutková podstata, ktorej sa páchateľ dopustí vtedy, ak sa dopustí konania podľa odsekov 1 a 2 z osobitného motívu.[7]

---

[6] Poskytovateľom elektronickej komunikačnej služby je podľa § 5 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách každá fyzická alebo právnická osoba, ktorá vykonáva podnikateľskú činnosti v oblasti poskytovania siete alebo služby v elektrotechnických komunikáciách pre tretiu osobu.

[7] Osobitným motívom sa podľa § 140 Trestného zákona rozumie spáchanie trestného činu a) na objednávku, b) z pomsty, c) v úmysle zakryť alebo uľahčiť iný trestný čin, d) v úmysle spáchať trestný čin terorizmu a niektorých foriem účasti na terorizme podľa § 419 Trestného zákona, e) z nenávisti voči skupine osôb alebo jednotlivcovi pre ich skutočnú alebo domnelú príslušnosť k niektorej rase, národu, národnosti, etnickej skupine, pre ich skutočný alebo domnelý pôvod, farbu pleti, pohlavie, sexuálnu orientáciu, politické presvedčenie alebo náboženské vyznanie, alebo f) so sexuálnym motívom.

Posledným počítačovým trestným činom, upraveným v osobitnej časti Trestného zákona, je trestný čin **výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov podľa § 247d Trestného zákona**. Primárnym objektom tohto trestného činu je ochrana tajomstva informácie prenášanej prostredníctvom elektronickej komunikačnej služby alebo tajomstva neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci. Sekundárne je tu chránená integrita počítačového systému a resp. všetkých objektov, ktorými sú chránené trestné činy od § 247 po § 247c TZ, nakoľko tento trestný čin obsahuje znaky každého z nich.[8] Objektívna stránka trestného činu výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov spočíva v tom, že „páchateľ v úmysle spáchať niektorý z trestných činov uvedených v § 247, § 247a, § 247b a § 247c Trestného zákona vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní zariadenie vrátane počítačového programu vytvoreného na neoprávnený prístup do počítačového systému alebo jeho časti, alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti“. K vyvodeniu trestnej zodpovednosti je teda potrebné, aby páchateľ naplnil aspoň jeden zo znakov objektívnej stránky trestného činu. Tieto znaky sú taxatívne vymenované a môžu byť naplnené kumulatívne alebo alternatívne.

Prvým znakom je vyrobenie. Vyrobením v tomto prípade rozumieme buď vytvorenie zariadenia, ktoré má slúžiť ako zariadenie na neoprávnený prístup do počítačového systému alebo vytvorenie resp. naprogramovanie počítačového programu, ktorého funkcia bude umožňovať prístup do počítačového systému, prístup k počítačovému heslu, prístupovému kódu alebo podobnému údaju, ktorý umožní prístup do počítačového systému. Dovozom môžeme v tomto prípade rozumieť činnosť, ktorej cieľom je prevoz takéhoto zariadenia alebo programu na územie Slovenskej republiky cez štátnu hranicu. Obstaraním môžeme rozumieť „akýkoľvek ďalší spôsob zadováženia si uvedených komponentov, ktorý nespadá pod niektorý z vymenovaných spôsobov nadobudnutia prístupového prostriedku, ktoré sú uvedené v predmetnom ustanovení.“ V tomto prípade teda môže ísť o obstaranie si takýchto zariadení alebo programov alebo hesiel a pod., krádežou, lúpežou, legalizáciou príjmu z trestnej činnosti, keď niekto prijme vec pochádzajúcu z trestnej činnosti v úmysle zatajiť existenciu takejto veci. Predajom a kúpou rozumieme predovšetkým získanie vlastníckych práv alebo odovzdanie vlastníckych práv zariadenia alebo počítačového programu kúpnou alebo predajnou zmluvou, alebo bez zmluvy, za finančnú odplatu. Na tieto účely boli vytvorené na dark webe internetové stránky, zapodievajúce sa nelegálnym obsahom, predajom, kúpou a podobne. Vymenením treba rozumieť prenesenie vlastníckych práv k tejto veci za protihodnotu v podobe inej veci resp. služby, nie však v podobne finančnej, nakoľko by sa jednalo už o kúpu resp. predaj, a nie o výmenu. Uvedením do obehu alebo akýmkoľvek sprístupnením sa rozumie ponúknutie zariadenia alebo programu verejnosti a to jeho sprístupnením napríklad na internetovej predanej stránke, alebo vo forme voľne stiahnuteľného obsahu. Musí ísť však o bezodplatné konanie, nakoľko v prípade odplaty alebo získaní protihodnoty by sa jednalo o predaj resp. kúpu alebo výmenu takéhoto zariadenia alebo programu. Uvedené konania, akými sú obstaranie, predaj, kúpa a iné, je nutné vykonať v súvislosti so zariadením vytvoreným na neoprávnený prístup do počítačového systému alebo jeho časti, alebo v súvislosti s obstaraním, predajom, kúpou počítačového hesla, prístupového kódu, alebo podobného údaja umožňujúceho prístup do počítačového systému. Zariadením, ktoré je vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, budeme rozumieť predovšetkým hardvér, ktorý nám umožní obísť bezpečnostné opatrenia počítačového systému alebo zariadenie, ktoré nám umožní bez vedomia majiteľa používať počítačový systém. Hlavným účelom takéhoto zariadenia spravidla je obídenie práve spomínaného bezpečnostného opatrenia na získanie neoprávneného prístupu

[8] KLIMEK, L., ZÁHORA, J., HOLCR, K. Počítačová kriminalita v európskych súvislostiach. 1. vyd. Bratislava: Wolters Kluwer s.r.o., 2016. s. 182

do počítačového systému, nakoľko z logiky veci vyplýva, že na neoprávnený prístup by potom žiadne zariadenie nebolo treba. Druhým prípadom je už spomínané ovládanie na diaľku, kde je z povahy vecí samozrejmé, že na ovládanie počítačového systému bez osobnej prítomnosti sa vyžaduje použitie zariadenia, ktoré nám tento neoprávnený prístup a následné používanie umožní. Počítačovým programom je súbor pokynov, ktoré vykonávajú špecifické úlohy pri fungovaní počítača. Počítačovým heslom môžeme rozumieť reťazec znakov, ktorý slúži na overenie totožnosti používateľa počas autorizačného procesu. Heslá bývajú zväčša používané v páre s používateľskými menami. Slúžia nám na prístup do počítačového systému, aplikácie alebo webovej stránky. Prístupovým kódom sa rozumie reťazec čísiel alebo písmen, ktoré umožňujú prístup do určitého systému. Hlavnou odlišnosťou od počítačového hesla je, že prístupový kód nie je spojený s používateľským menom a zväčša býva využívaný napríklad pri digitálnych trezoroch alebo SIM kartách, kde je v podobne PIN (personal identification number) kódu, setu štyroch náhodných číslic. Podobnými údajmi môžeme rozumieť „napríklad kryptografický kľúč, bezpečnostný certifikát.“[9]

Z formulácie znakov skutkovej podstaty trestného činu výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov podľa § 247d Trestného zákona vyplýva, že konanie popísané v skutkovej podstate má v zásade charakter prípravy. Vzhľadom na to, že príprava je trestná iba vo vzťahu k zločinu, zákonodarca toto ustanovenie koncipoval ako samostatný predčasne dokonaný trestný čin.“[10] Subjektom tohto trestného činu môže byť každá fyzická alebo právnická osoba. Subjektívna stránka je založená na zavinení vo forme priameho alebo nepriameho úmyslu. Obligatórnym znakom subjektívnej stránky je aj motív spočívajúci v tom, že páchateľ musí konať v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údaja podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c Trestného zákona

Kvalifikovaná skutková podstata tohto trestného činu je podľa odseku 2 založená na tom, že páchateľ konaním uvedeným v odseku 1 spácha značnú škodu. Kvalifikovaná skutková podstata podľa odseku 3 je založená na tom, že páchateľ konaním uvedeným v odseku 1 spôsobí škodu veľkého rozsahu alebo sa konania uvedeného v odseku 1 dopustí ako člen nebezpečného zoskupenia.

Škoda a zásady určenia výšky škody spôsobenej trestným činom podľa Trestného zákona

Trestný zákon definuje pojem škoda v ustanovení § 124. Podľa tohto ustanovenia sa „škodou rozumie ujma na majetku alebo reálny úbytok na majetku alebo na právach poškodeného alebo jeho iná ujma, ktorá je v príčinnej súvislosti s trestným činom, bez ohľadu na to, či ide o škodu na veci alebo na právach. Škodou sa rozumie aj získanie prospechu v príčinnej súvislosti s trestným činom“. Škodou sa rozumie aj ujma na zisku, na ktorý by poškodený inak vzhľadom na okolnosti a svoje pomery mal nárok alebo ktorý by mohol odôvodnene dosiahnuť.

Trestný zákon zároveň v ustanovení § 125 definuje jednotlivé druhy škôd z hľadiska rozsahu tak, že **škodou malou** sa rozumie škoda prevyšujúca sumu 266 eur. **Škodou väčšou** sa rozumie suma dosahujúca najmenej desaťnásobok takej sumy (najmenej 2 660 eur). **Značnou škodou** sa rozumie suma dosahujúca najmenej stonásobok takej sumy (najmenej 26 600 eur). Škodou veľkého rozsahu sa rozumie suma dosahujúca najmenej päťstonásobok takej sumy (najmenej 133 000 eur). Tieto hľadiská sa použijú rovnako na určenie výšky prospechu, hodnoty veci a rozsahu činu.

[9] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. 1. vyd. Bratislava: Wolters Kluwer s.r.o., 2016, s. 185

[10] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. 1. vyd. Bratislava: Wolters Kluwer s.r.o., 2016.s. 184

Základné skutkov podstaty takzvaných počítačových trestných činov, ktoré sú upravené v § 247 až 247d Trestného zákona nevyžadujú spôsobenie škody , ako majetkového následku trestného činu. Napriek tomu, však možno na túto situáciu aplikovať ustanovenie § 125 ods. 2 Trestného zákona podľa ktorého , ak Trestný zákon v osobitnej časti vyžaduje v základnej skutkovej podstate spôsobenie škody ako majetkový následok trestného činu a neuvádza jej výšku, má sa za to, že musí byť spôsobená aspoň škoda malá.

Trestný zákon upravuje v ustanovení § 126 aj niekoľko všeobecných zásad vzťahujúcich sa na určenie výšky škody spôsobnej trestným činom, ktoré znejú nasledovne.

- Pri určení výšky škody sa vychádza z ceny, za ktorú sa vec, ktorá bola predmetom útoku, v čase a v mieste činu obvykle predáva.
- Ak výšku škody nemožno takto zistiť, vychádza sa z účelne vynaložených nákladov na obstaranie rovnakej alebo obdobnej veci alebo na uvedenie veci do predošlého stavu.
- Ak nemožno určiť výšku škody alebo ujmy ani jedným z uvedených spôsobov , alebo ak sú vážne pochybnosti o správnosti výšky škody alebo takto určenej ujmy, určí sa jej výška na podklade odborného vyjadrenia alebo potvrdenia právnickej osoby, ktorej pôsobnosť alebo predmet činnosti poskytuje záruku objektívnosti určenia škody alebo ujmy. Inak sa výška škody určí na podklade znaleckého posudku.

Najmä z obsahu posledne uvedenej zásady pre určenie výšky škody vyplýva, že pri stanovení výšky škody spôsobenej neoprávnenými zásahmi do počítačových systémov možno využiť osobitnú metódu určenia výšky takto spôsobenej škody.

Typy neoprávnených zásahov do počítačových systémov

Vzhľadom na komplexnosť počítačových systémov, ako aj aktuálnu právnu kvalifikáciu počítačových trestných činov, teda trestných činov v oblasti počítačovej kriminality (kyberkriminality) je potrebná dekompozícia jednotlivých neoprávnených zásahov do počítačových systémov na v súčasnosti existujúce typy.

Pre účely tohto príspevku sa pod pojmom počítačový systém rozumie akékoľvek počítačové zariadenie alebo skupinu zariadení umožňujúce spracovanie určitého typu informácií s cieľom efektívneho spracovania dát alebo zjednodušenie práce. Môže pozostávať z hardware, software, počítačovej siete, ale aj samotnej elektronickej komunikácie s iným počítačovým systémom, či iného zariadenia k nemu pripojeného. Príkladom sú mobilné telefóny, sieťové routre, meteostanice, smart televízory alebo iné zariadenia, databázy, servery, či samotné elektronické súčiastky.

Konkrétne ide o tieto typy neoprávnených zásahov do počítačových systémov:

- Neoprávnené zásahy do programového vybavenia – software
- Neoprávnené použitie autorských diel, s ktorými je nakladané v rozpore s autorským právom.
- Neoprávnené šírenie autorských diel
- Vytváranie a šírenie prostriedkov na odstránenie ochranných prvkov slúžiacich na chránenie autorských diel.
- Neoprávnené generovanie a šírenie licenčných súborov, napríklad cez tzv. „keygeny“
- Narušenie funkčnosti informačného systému, tzv. „cracking“
- Zneužitie informácií získaných pri kolektívnej tvorbe informačných systémov
- Reverzné inžinierstvo.

Neoprávnené narušenie databáz a informácií uložených v počítačových systémoch:

- Zneužitie znalosti prístupu do databáz
- Úmyselné narušenie obsahu databáz
- Zverejnenie dátového obsahu informačného systému

- Neoprávnenie poskytnutie prístupu do databáz.

Neoprávnené narušenie komunikačných kanálov:

- Odchytávanie hesiel pre vstup do cudzích informačných systémov
- Neoprávnený vstup do počítačového systému
- Úmyselné narušenie funkčnosti
- Sprostredkovanie prístupu do počítačového systému cudzej osobe.

Neoprávnené zásahy do hardware počítačových systémov:

- Reverzná analýza a zmena hardvéru s cieľom získať prístup do analyzovaného zariadenia
- Narušenie toku informácií v tom ktorom zariadení na úrovni hardware.

Stanovenie škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov

Z hľadiska trestného konania je stanovenie škody spôsobenej neoprávnenými zásahmi do počítačových systémov jedným z kľúčových východísk pre kvalifikáciu trestnosti skutku. Vzhľadom na komplexnosť a predovšetkým veľké množstvo typov týchto zásahov sa v praxi ukazuje, že je zložité výšku nimi spôsobenej škody určiť.

Existujú prípady, keď sa škoda odvíja od hodnoty hardvérového vybavenia potrebného pre funkčnosť systému. Tieto škody sú väčšinou tie najnižšie. Naopak pri zásahoch do počítačových systémov vyvíjaných dlhý čas, proprietárne, napr. bankových systémoch alebo systémoch finančnej správy, vzniknutá škoda nepozostáva len z nákladov na identifikáciu narušiteľa, ale aj opravu systému – často krát spojenú s množstvom nákladov na preprogramovaní jeho častí.

Stanovenie výšky škody vyžaduje súdnoznaleckú analýzu a súčinnosť viacerých ďalších subjektov. Poškodeného, ďalej autora systému, vyšetrovateľa, svedkov a iných. Samotné konanie znalca tiež nie je jednoduché, nakoľko pri počítačových systémoch dochádza k prieniku veľkého množstva odborov a stanovenie už samotnej všeobecnej hodnoty systému vyžadujem znalcov z oblasti elektrotechniky, informatiky, ekonomiky a ďalších.

Stanovenie výšky škody spôsobenej zásahom do počítačových systémov vychádza predovšetkým **zo stanovania všeobecnej hodnoty dotknutého počítačového systému (VŠH)**. Bez jej znalosti by bolo náročné, ak nie priamo úplne nemožné, určiť škodu po neoprávnenom narušení. Následne, keď je známa VŠH, sa pristupuje k určeniu percentuálneho vplyvu zásahu do počítačového systému z hľadiska nárokov na jeho uvedenie do použiteľného stavu až po novú implementáciu celého systému. Až keď sú tieto dva parametre k dispozícii, je možné odhadnúť výšku škody. Pozrime sa preto na možnosti ich určenia detailne.

Pri stanovení VŠH počítačového systému je potrebné vychádzať z viacerých predpokladov, ktoré sú základom pre správny výber metódy:

- Informačný systém je/ nie je voľne predajný
- Informačný systém je/ nie je úzko odvetvovo orientovaný
- Informačný systém je/ nie je určený pre použitie obvyklým maloobchodným spotrebiteľom
- Informačný systém je jedinečný a jeho plnej funkcionalite nezodpovedá žiadny iný informačný systém
- Pre informačný systém nemôže jeho tvorca kvantifikovať budúce prínosy pre jeho užívateľa z ekonomických hľadísk
- A iných aktuálnych zistení pri tom ktorom prípade.

Inak je potrebné pristupovať k určeniu všeobecnej hodnoty počítačového systému, ktorý bol vyvíjaný na zákazku pre konkrétneho klienta a nie je v dodanom stave použiteľný nikde

inde. Ako príklad takého systému môžeme uviesť rôzne implementácie SAP na mieru, ktorých počiatočná hodnota je vysoká, ale v tom ktorom stave nie je možné takýto systém bez ďalšej modifikácie použiť u iného klienta.

Iný prístup je potrebné zvoliť pri odhade VŠH počítačového systému, ktorý vyvíja softvérová spoločnosť za účelom ďalšieho predaja. Napríklad drahé grafické aplikácie.

Rôzne je potrebné pristupovať k softvéru určenému na predaj relatívne malému množstvu zákazníkov (účtovnícke aplikácie) alebo veľkému množstvu klientov (antivírusy), pričom môžeme zvažovať trhový podiel systému z hľadiska existencie konkurenčných riešení a analýzy ich cien.

Na základe vstupných predpokladov sa následne zvolí metóda stanovenia všeobecnej hodnoty informačného systému[11].

Poznáme rôzne metódy stanovenia VŠH, pričom použitie tej ktorej závisí od situácie a typu počítačového systému. Ide o tieto metódy:

- Komparatívna metóda
- Metóda budúcich výnosov
- Nákladová metóda
- Metóda stanovenia trhovej hodnoty PS.

Základným princípom **komparatívnej metódy** je porovnanie dotknutého PS s iným produktom na trhu, podobným čo do ceny a funkcie. Porovnávajú sa podľa možností viaceré, predovšetkým so zameraním na ich trhovú cenu.

Ďalšou možnosťou je **metóda budúcich výnosov**, na základe ktorej sa projektuje ekonomický prínos informačného systému počas jeho odhadovanej životaschopnosti na trhu.

Treťou používanou metódou je **metóda nákladová**, keď sa stanovuje výška nákladov potrebných na vytvorenie informačného systému. A to formou preukázateľných nákladov alebo odhadovaných nákladov na naprogramovanie nového informačného systému s rovnakými funkciami aké poskytuje predmetný informačný systém.

Samotný výber metódy je na znalcoch v odbore oceňovania aktív firmy v súčinnosti so znalcami v oblasti elektrotechniky so zameraním na informačné systémy. Ako už bolo spomenuté skôr, počítačové systémy sú komplexné diela. Na ich tvorbe sa podieľa veľké množstvo subjektov z rôznych profesií a trh, pre ktorý sú určené, je citlivý na okamih uvedenia informačného systému ako aj na jeho kvalitu.

Komparatívna metóda, metóda budúcich výnosov a nákladová metóda sú v praxi veľmi často používané. Presnosť týchto metód však môže byť nízka, pokiaľ ide o informačný systém, ktorý má vysokú trhovú penetráciu alebo existujú ekvivalentné alternatívy, ktoré si môžu užívatelia zakúpiť. Nakoľko tento prípad žiadna zo spomínaných metód významnejšie nezohľadňuje a v súčasnosti existuje na trhu veľké množstvo počítačových programov používaných masovo, možno navrhnúť pre stanovenie výšky škody použiť metódu stanovenia trhovej hodnoty informačného systému.

Trhová metóda stanovenia všeobecnej hodnoty informačného systému vychádza z viacerých parametrov. Tými sú:

- východisková trhová hodnota informačného systému **(VTH)**
- dopad diskreditácie informačného systému na jeho užívateľov **(k_d)**
- trhová penetrácia informačného systému **(k_p)**
- množstvo konkurenčných informačných systémov a ich cenový model **(k_{kc})**
- miera dostupnosti informácií o princípoch fungovania informačného systému **(k_i)**

[11] Základným východiskom pre metodiku stanovenia všeobecnej hodnoty informačného systému je rovnako ako pri ostatných typoch majetku je vyhláška Ministerstva spravodlivosti Slovenskej repuky z 23. augusta 2004 o stanovení všeobecnej hodnoty majetku, v znení neskorších predpisov.

- miera aktuálizácie informačného systému **(k_a)**

Tieto parametre slúžia na opísanie situácie na trhu s podobnými počítačovými systémami a určujú sa znalcom ku konkrétnemu dátumu. Obor hodnôt ktoré môžu samotné koeficienty k_d až k_a nadobúdať, je v intervale od 0 do 1. Ich vzájomným vynásobením dostaneme číslo opäť z intervalu 0 až 1, ktorým môžeme primerane znížiť východiskovú trhovú hodnotu PS, čím sa vypočítame všeobecnú hodnotu PS trhovou metódou.

Pod východiskovou trhovou hodnotou informačného systému (VTH) sa rozumie indikatívna hodnota všetkých predaných licencií informačného systému jeho autorom od doby jeho uvedenia na trh. Autor počítačového systému by mal byť schopný dodať potrebné podklady na jej stanovenie. Môže to byť napríklad formou účtovaných faktúr o predaji licencií alebo počty jednotlivých druhov licencií aj s ich cenníkmi platnými v jednotlivých obdobiach.

Napríklad ak autor počítačového programu, ktorý slúži na prehrávanie filmov v kinách, od jeho uvedenia na trh predal 1500 licencii s jednotkovou cenou 500 EUR, potom východisková trhová hodnota informačného je VTH = 1500 x 500 EUR = 750000 EUR.

Pri výpočte je potrebné skúmať štruktúru predajného modelu informačného systému, čiže rozlišovať typy licencií, skúmať ceny v jednotlivých krajinách, atď..

Východisková trhová hodnota tvorí základ odhadu všeobecnej hodnoty informačného systému, pričom ďalšie vstupné parametre majú korektívny charakter smerom k jeho skutočnej hodnote na trhu.

Ako už bolo uvedené pri stanovení trhovej hodnoty informačného systému,, treba okrem východiskovej trhovej hodnoty informačného systému vychádzať z nasledovných parametrov:

- *dopad diskreditácie informačného systému na jeho užívateľov (k_d)*

Každý informačný systém je napadnuteľný. Jednotlivé zásahy do informačných systémov sme si popísali v predchádzajúcich kapitolách. Diskreditácia informačného systému formou neoprávneného zásahu priamo súvisí s náladou užívateľov takto napadnutý softvér kupovať a používať, čo má priamy efekt na jeho trhovú hodnotu. Preto je potrebné tento fakt zohľadniť pri výpočte jeho všeobecnej hodnoty.

- *trhová penetrácia informačného systému (kp)*

Každý trh má svoj limit v maximálnom počte predaných produktov. Napríklad mobilné telefóny je možné predať s istou toleranciou napríklad maximálne 115% obyvateľstva. Niektorí ľudia si kúpia viac kusov, iní nemajú žiadne. Rovnaká situácia je i na trhu s informačnými systémami. Pod trhovou penetráciou informačného systému rozumieme mieru podielu daného informačného systému na trhu. Ak napríklad znalec odhadne celkový možný počet predaných licencií na trhu na 1000 kusov a autor zdokladuje predaj 350 kusov, potom je trhová penetrácia 35%. S trhovou penetráciou IS úzko súvisí atraktivita informačného systému a teda jeho ďalšia predajnosť. Ak by bola trhová penetrácia na úrovni 100%, znamenalo by to, že každý užívateľ, ktorý by mohol mať záujem o konkrétny informačný systém takýto alebo jemu podobný už má a pravdepodobnosť nákupu ďalšej licencie by sa znižovala.

- *množstvo konkurenčných informačných systémov a ceny (kkc)*

Tento vstupný parameter musí zohľadňovať predovšetkým funkčne podobné aplikácie, ktoré môžu substituovať úžitkovú hodnotu hodnoteného informačného systému, a tiež ich ceny. Na odhad trhovej hodnoty má totiž zásadný vplyv fakt, ak je na trhu v ponuke porovnateľný iný IS pri ktorom autor nepožaduje odmenu za používanie – freeware.

- *miera dostupnosti informácií o princípoch fungovania informačného systému (ki)*

Ak sú princípy fungovania hodnoteného informačného systému všeobecne známe, zvyšuje sa pravdepodobnosť poklesu ceny z dôvodu možného vzniku novej konkurencie. Tento vstupný parameter by mal mať nízky vplyv na výslednú odhadnutú trhovú hodnotu IS. Považujem však za potrebné ho uviesť nakoľko v informatike dochádza k neustálemu

zjednodušovaniu tvorby počítačových programov a tým sa zvyšuje šanca rýchleho vytvorenia podobného informačného systému iným autorom, ak sú mu známe princípy fungovania.

- *miera aktualizácie informačného systému (ka)*

Každý informačný systém vyžaduje zo strany autora neustálu prácu na jeho aktualizáciách. Ak by napríklad tvorca účtovníckeho softvéru svoj produkt neaktualizoval, tak by ho nebolo možné použiť už pri prvej zmene napríklad zákona o DPH. Ak by v inom prípade tvorca počítačového programu prestal svoj produkt vyvíjať, konkurencia by ho s funkciami dostihla, predbehla a záujem o jeho softvér by poklesol. Je preto potrebné pri stanovovaní všeobecnej hodnoty informačného systému navrhovanou trhovou metódou zohľadniť mieru aktualizácií.

Vstupné parametre navrhovanej metódy musia byť odborne stanovené formou koeficientov, ktoré sa medzi sebou budú násobiť do jedného finálneho koeficientu „k“. Ako už bolo spomenuté vyššie, koeficienty k_d až k_a nadobúdajú hodnoty v intervale od 0 do 1, a teda aj ich súčin **k** bude v intervale 0 až 1. Týmto koeficientom **k** sa následne vynásobí odhadnutá východisková hodnota informačného systému. Výsledok, ktorý vznikne bude všeobecná hodnota informačného systému stanovená trhovou metódou.

$$\mathbf{k = k_d \times k_p \times k_{kc} \times k_i \times k_a}$$

$$\mathbf{VŠH = VTH \times k}$$

Samotné koeficienty (k_d, k_p, k_{kc}, k_{ki} a k_a) určí znalec podľa konkrétnej situácie na trhu. Nakoľko však ide o návrh metódy, presnejšie stanovenie rozsahov a hodnôt týchto koeficientov je potrebné vypracovať po dôkladnej odbornej analýze a diskusii.

Trhová metóda stanovenia všeobecnej hodnoty informačného systému je výhodná v tom, že nevyžaduje veľkú mieru súčinnosti ďalších subjektov, ani štúdium rozsiahlych podkladov, ktoré pri vývoji softvéru vznikajú. Jej použitie je vhodné pre informačné systémy s vysokou mierou rozšírenia na trhu a zároveň trh ponúka iné konkurenčné riešenia. Metóda formou vymedzenia vstupných parametrov zohľadňuje súčasné trendy vývoja a distribúcie informačných systémov.

Navrhovaná metóda umožní širokej spektre profesionálov odhadovať hodnotu počítačových programov a tú následne použiť pre ďalšie potreby. Využitie nájde v znaleckom posudzovaní pri presnejšom stanovení škody spôsobenej páchateľom. V súkromnom sektore môže byť táto metóda použitá napríklad pri stanovení hodnoty obchodnej spoločnosti, ktorá vyvíja a predáva informačné systémy.

Dostávame sa k cieľu tohto príspevku, ktorým je stanovenie výšky škody spôsobenej neoprávneným zásahom do počítačového systému.

Vstupným parametrom pre stanovenie výšky škody spôsobenej neoprávneným zásahom do počítačového systému je vždy všeobecná hodnota (VŠH). Metódy jej určenia sme si rozobrali v predchádzajúcich odsekoch.

Pri určení výšky škody sa odborne analyzuje vplyv zásahu na funkčnosť a ďalšiu použiteľnosť dotknutého počítačového systému a kvalifikovane odhaduje percentuálna miera vplyvu zásahu (%). Konkrétna analýza prebieha v tíme odborníkov, znalcov a pre právne účely by mala zahŕňať vytvorenie znaleckého posudku, v ktorom bude dôkladne popísaná.

Percentuálna miera vplyvu zásahu do počítačového systému následne vstupuje do je výpočtu škody vychádzajúceho zo všeobecnej hodnoty PS a to nasledovne: **Š = VŠH * %,** pričom **Š** je odhad výšky spôsobenej škody, **VŠH** je všeobecná hodnota systému a **%** miera vplyvu zásahu do PS.

Záver

Na základe obsahu príspevku možno urobiť záver, že počítačová (kybernetická) kriminalita, podstatu ktorej tvoria neoprávnené zásahy do počítačových systémov, počítačových programov a počítačových údajov je veľmi zložitá a náročná a problematika. Zložitosť je daná predovšetkým samotnou povahou kybernetického priestoru, v ktorom ku skúmanej trestnej činnosti dochádza a tým , čo tento priestor vytvára. S touto skutočnosťou sa spája aj náročnosť zistenia neoprávnených zásahov do počítačových systémov , ako aj náročnosť zaistenia a skúmania touto činnosťou vytvorených kriminalistických stôp. K týmto problémom na viac pristupuje aj problém stanovenia výšky škody spôsobenej trestnými činmi, ktoré majú charakter počítačových trestných činov. Pritom z hľadiska trestného konania je práve stanovenie škody spôsobenej neoprávnenými zásahmi do počítačových systémov jedným z kľúčových východísk pre kvalifikáciu trestnosti skutku. Príspevok preto ponúka typológiu neoprávnených zásahov do počítačových systémov, počítačových programov a počítačových údajov, ako aj východiská pre trestnoprávnu kvalifikáciu takýchto zásahov, vrátane východísk pre stanovenie výšky škody spôsobnej takouto trestnou činnosťou.

Zoznam použitej literatúry:

GŘIVNA, T., POLČÁK R. *Kyberkriminalita a právo,* Praha : Auditorium, 2008, 220 s., ISBN: 978-80-903786-7- 4

HOLJENČÍK, J., NANIŠTA, R., SMOLA, A. *Metodika na stanovenie všeobecnej hodnoty elektrotechnických zariadení*, Bratislava : Slovenská technická univerzita, 2004, 51 s.

IVOR, J. , POLÁK, P., ZÁHORA, J. *Trestné právo hmotné. Osobitná časť*. Bratislava : Wolters Kluwer. 2017, 646 s., ISBN: 978-80-8168-585-9.

IVOR, J. , POLÁK, P., ZÁHORA, J. *Trestné právo hmotné. Všeobecná časť*. Bratislava : Wolters Kluwer. 2016, 555 s., ISBN: 978-80-8168-509-5.

KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* 1. vyd. Bratislava: Wolters Kluwer s.r.o., 2016. 445 s. ISBN 978-80-8168-538-5

NANIŠTA, R. a kolektív. *Metodika znaleckého posudzovania. Učebné texty*. Bratislava : Slovenská technická univerzita, 2003

SMEJKAL, V. a kolektív. *Právo informačních a telekomunikačních systémů*, Praha : C. H. Beck, 2004, 770 s., ISBN: 80-7179-765-0

Kontaktné údaje:

doc. JUDr. Peter Polák, PhD.
Fakulta práva Paneurópskej vysokej školy n.o.
Bratislava
peter.polak@paneurouni.com

Mgr. Bc. Tomáš Trúsik
ProtoWay s.r.o.
Bratislava
tomas.trusik@protoway.eu

Počítačová kriminalita a jej dynamika vývoja v rokoch 2014 - 2017

Liliana Réveszová

Abstrakt:
Počítačová kriminalita patrí k najobľúbenejším konverzačným témam na Slovensku, ktorá je často skloňovaná v médiách. O počítačovej kriminalite počul asi každý z nás, niektorí s ňou majú aj osobnú skúsenosť. Najstaršie činy spadajúce pod počítačovú kriminalitu majú najmenej 25rokov. Uvedená spomínaná trestná činnosť predstavuje obrovské finančné straty, veľmi často presahuje hranice jedného štátu a stáva sa medzinárodným trestným činom. V uvedenom príspevku sa v jej prvej časti venujeme definícii počítačovej kriminality a v druhej časti sa zameriavame na reálnu dynamiku vývoja počítačovej kriminality v Slovenskej republike v rokoch 2014 – 2017. Aj na jej základe môžeme konštatovať, že počítačová kriminalita je v súčasnosti najrýchlejšie rozvíjajúca sa forma kriminality, počet jej obetí denne stúpa.
Kľúčové slová:
počítačová kriminalita, trestný čin, absencia definície, dynamika vývoja, formy, páchateľ, obete

Abstract:
Computer crime is one of the most popular conversational topics in Slovakia, which is often mentioned in the media. Each of us has heard about computer crime, some have their personal experience. The oldest cybercrime cases occurred at least 25 years ago. The above-mentioned criminal activity causes enormous financial loss. Very often it crosses the borders of one country and becomes an international criminal offence. In the first part of the paper, we are focusing on the definition of cybercrime, and in the second part we are dealing with the real dynamics of cybercrime development in the Slovak Republic in 2014-2017. We can also state that cybercrime is currently the fastest growing form of crime, and the number of its victims is rising daily.
Keywords:
computer crime, offence, absence of a definition, dynamics of development, forms, perpetrator, victims

Úvod

V dnešnom svete s neustálym rozvojom výpočtových technológií, získava problematika počítačovej kriminality na intenzite. Zakaždým sa vyskytujú nové spôsoby počítačovej kriminality a zároveň sú zdokonaľované tak, aby boli čo najmenej odhaliteľné a postihnuteľné. Neinformovanosť ľudí a zabezpečenie počítačov v tejto problematike sú veľkým problémom, pretože 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 počítačovú kriminalitu hodnotíme ako jednu z najnebezpečnejších fenoménov. Vzhľadom k tomu môžeme konštatovať, že je potrebné tejto problematike venovať osobitne zvýšenú pozornosť.

Cieľom tohto článku je čitateľom priniesť základné informácie o počítačovej kriminalite, jej definícii, o jej páchateľoch, ich motívoch páchania počítačovej kriminality, o spôsoboch páchania počítačovej kriminality, jej foriem v slovenskej právnej úprave a následným grafickým zobrazením a porovnaním dynamiky konkrétnych foriem počítačovej kriminality v slovenskej právnej úprave za roky 2015 – 2017.

Vymedzenie počítačovej kriminality

Počítačová kriminalita a jej počiatky možno datovať do obdobia 60. a 70. rokov 20.storočia, samozrejme, že v tých časoch bola odlišná od dnešnej.

V literatúre sa stretávame s argumentmi autorov Smejkala a Poradu, že počítačová kriminalita vznikla v okamihu, keď sa počítače začali meniť na mnohoúčelovo použiteľné zariadenia z matematických strojov v pôvodnom zmysle slova a ktoré boli schopné prevziať najrôznejšiu agendu a keď niekto postupne prišiel na myšlienku, že modifikáciou programov alebo údajov spracovávaných počítačom môže dosiahnuť účinok, ktorý spôsobí niekomu škodu

či inému neoprávnený prospech. Súčasne sa počítač objavil ako zločinný nástroj, keďže niekto úplne iný zistil, ako jednoducho je možné spáchať niektoré trestné činy s takým skvelým pomocníkom.[1]

Pri vymedzení pojmu počítačová kriminalita nie je vo všeobecnosti žiadna uznávaná definícia, pretože odborná verejnosť v chápaní tohto pojmu nie je jednotná a definovanie tohto pojmu je veľmi neurčité aj napriek tomu, že dnešná doba je počítačmi úplne pohltená. Uvedený druh kriminality sa zvykne najčastejšie označovať ako počítačová kriminalita, kybernetická kriminalita či kyberkriminalita. V princípe možno všetky tri uvedené termíny považovať za synonymá. Ako ho na svoje účely vymedzí záleží len na autoroch, oficiálnom dokumente či právnom predpise. Anglické ekvivalenty týchto pojmov objavujúce sa v zahraničnej literatúre, či článkoch predstavujú pojmy „cybercrime", „high-tech crime", „IT crime", „virtual crime“, či „computer crime", ktorý je časovo najstarším pojmom.. Jednotná a záväzná definícia tohto pojmu sa zatiaľ nenachádza v žiadnom zákone, či zmluve, ktorú je SR viazaná dodržiavať.[2] Z lingvistického hľadiska pojem počítačová kriminalita v právnom kontexte pramení v Zmluve o fungovaní Európskej únie ako jeden z európskych trestných činov. „Navyše, v podmienkach Slovenskej Republiky pojem počítačová kriminalita je udomácnený aj na Akadémii policajného zboru Slovenskej republiky, ako aj na Právnickej fakulte Univerzity Pavla Jozefa Šafárika v Košiciach.“[3]

„Za súčasného stavu poznania je definovanie pojmu počítačová kriminalita mimoriadne náročná úloha, priam nemožná.“[4] 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.“[5] Z definície nám ale vyplýva otázka, čo sa rozumie počítačovým trestným činom? Skupiny trestných činov počítačovej kriminality možno teda vnímať ako vhodnú alternatívu vymedzenia pojmu počítačová kriminalita.

Jednanie spadajúce pod pojem počítačová kriminalita je možné chápať v troch skupinách, ktoré sa udomácnili v odbornej literatúre a to ako:
- trestné činy vo vzťahu k počítaču vrátane jeho príslušenstva – tu je počítač cieľom útoku,
- trestné činy vo vzťahu k počítačovému softvéru, dátum, respektíve informáciám, synonymom tohto druhu počítačovej kriminality môže byť informačná kriminalita,
- trestné činy, kedy je počítač prostriedkom k páchaniu trestnej činnosti.[6]

Delenie nie je absolútne a rozhodne nevylučuje súbeh konaní uvedenými pod rôznymi rovinami, toto je dôležité si uvedomiť.

---

[1] SMEJKAL, V., et 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, s. 64.

[2] Najpravo. *Základné formy počítačovej kriminality*. [online]. [cit. 15. 06. 2018]. Dostupné na internete:<http://www.najpravo.sk/clanky/zakladne-formy-pocitacovej-kriminality.html>

[3] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s. 53.

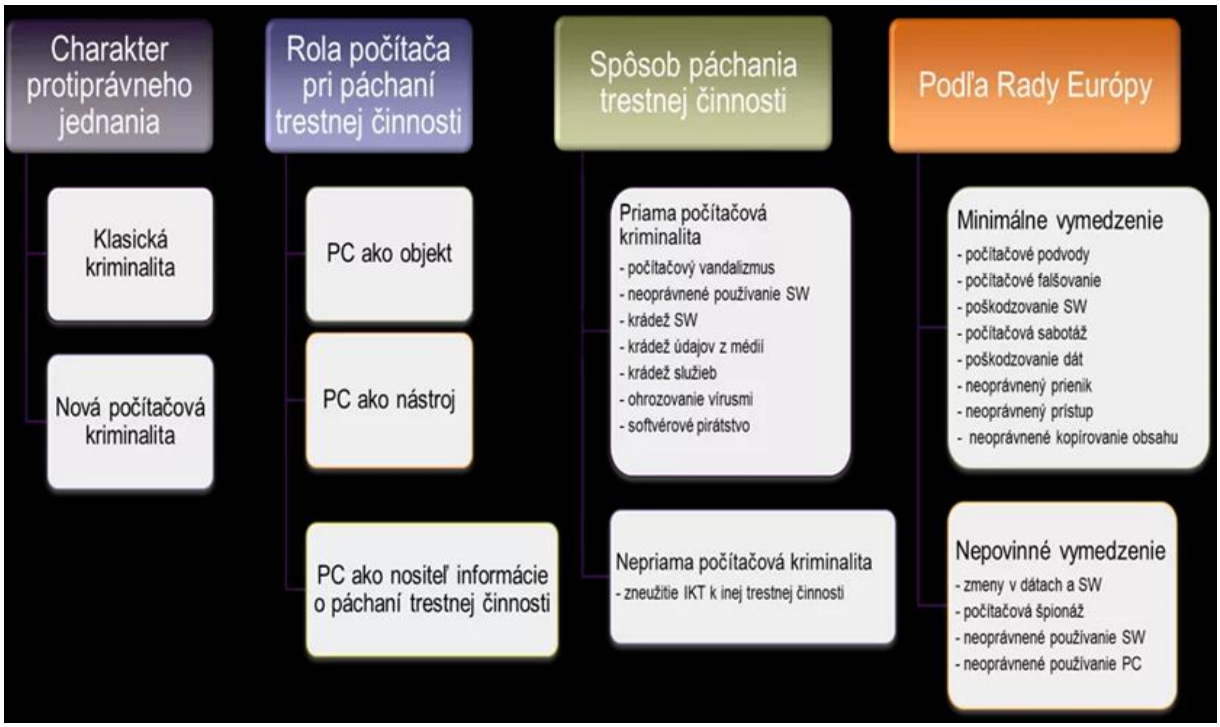
[4] KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s.25.

[5] KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s.25.

[6] SMEJKAL, V. Internet @ §§§, s. 153.

Pojem počítačová 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.“[7]

„Dohovor o počítačovej kriminalite je prvou medzinárodnou dohodou o boji proti zločinom páchaným prostredníctvom internetu a ďalších počítačových sietí uzavretý 23.novembra 2001. Hlavným cieľom dohovoru je presadzovanie spoločnej politiky zameranej na delikty súvisiace s porušovaním autorských práv, podvodmi cez počítače, šírením detskej pornografie či narúšaním bezpečnosti sietí ako aj ochranu spoločnosti proti počítačovým zločinom.“[8] Uvádzaný dohovor priniesol konkrétnu štandardizáciu v pohľade na kategorizáciu počítačovej kriminality – kategorizácia je možná z niekoľkých možných uhlov pohľadu, viď. obrázok č.1.



Obrázok 1 Štandardizáciu v pohľade na kategorizáciu počítačovej kriminality podľa Dohovoru o počítačovej kriminalite.
Zdroj: < http://preventista.sk/info/pocitacova-internetova-kriminalita-a-jej-prevencia-v-skolskom-prostredi/>

Spôsoby páchania počítačovej kriminality

V kapitole si uvedieme niekoľko spôsobov páchania počítačovej kriminality, ktorých sa dopúšťajú jej páchatelia, ktorí sú veľmi pokroková a vynaliezaví. Isté z týchto spôsobov sú páchané už niekoľko rokov, ale neustále sú vylepšované, zjednodušené ich použitia, sú sofistikované až v takej miere, že v niektorých konkrétnych prípadoch sú priam až

[7] Preventista. *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/>

[8] Preventista. *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/>

neobjasniteľné. Vymenujeme si tie najbežnejšie a najškodlivejšie spôsoby páchania počítačovej kriminality, pretože podrobnejšia analýza by bola nad rámec tohto príspevku.

K najbežnejším a najškodlivejším spôsobom počítačovej kriminality zaraďujeme hacking, cracking, warez (linking), porušovanie autorských práv prostredníctvom „torrent-ov", malware, phishing, sniffing, skimming.

Páchatelia počítačovej kriminality

V tejto kapitole si priblížime profil páchateľov počítačovej kriminality. Zvyčajne sú to muži vo veku 17 až 30 rokov, ale nevylučuje sa ani vyšší vek.[9] „Pôvod páchateľov tohto druhu trestnej činnosti nie je ničím podmienený. Pochádzajú zo všetkých sociálnych vrstiev a z krajín celého sveta."[10] Vzdelanie nie je rozhodujúcim faktorom pri trestnej činnosti, aj keď páchanie počítačovej kriminality si vyžaduje vedomosti z oblasti informačných technológií. Mnohí páchajú trestnú činnosť úspešne aj napriek tomu , že nedosiahli žiadne vzdelanie v oblasti informačných technológií. Naproti tomu, mnohí sú zase vysoko kvalifikovaní absolventi vysokých škôl a univerzít v odboroch zameraných na informačné technológie. Väčšinu kurzov/ predmetov však považovali za stratu času, keďže ich nezaujímalo to, čo im škola ponúka. Títo páchatelia oboch skupín majú spoločnú črtu a to, že sú spravidla nadpriemerne, ba až vysoko inteligentní. Obvykle sa aj sami cítia byť veľmi inteligentní, ak nie aj najinteligentnejšími na svete.[11] Laickou verejnosťou je páchateľ počítačovej kriminality chápaný a pomenovaný ako hacker – odvodené od slova hacking.

Smejkal uvádza delenie páchateľov do piatich kategórií:
- zamestnanci poškodenej organizácie,
- príslušníci organizovaného zločinu,
- prienikári, hackeri, ktorí majú anarchistické ciele,
- osoby príliš nepremýšľajúce o svojom konaní a jeho následkoch – deti, mladiství, osoby neznalé práva,
- profesionáli pracujúci za peniaze, živiaci sa činnosťou ako prieniky, odhaľovanie utajovaných informácií, špionáž a podobne.[12]

Uvedená klasifikácia však jednoznačná nie je. Jednotlivé kategórie sa môžu vzájomne prelínať, a to hlavne s ohľadom na motív jednotlivých páchateľov.[13]

Motívy páchateľov počítačovej kriminality je možné všeobecne zhrnúť nasledujúcim spôsobom:
- motívy zištné – pohnútkou je nedostatočné finančné zabezpečenie páchateľov, vidina ľahkého a relatívne bezpečného zisku,
- túžba dokázať svoju intelektuálnu prevahu – napríklad nad tvorcami ochranných programov, nad zamestnávateľmi,
- túžba po výsadnom postavení – v podnikateľskom prostredí ide o snahu zlikvidovať konkurenciu podobne,
- krycie motívy k utajeniu inej trestnej činnosti – obavy z odhalenie iného trestného činu, ktorý ani nemusí mať povahu počítačovej kriminality,

[9] HOLCR, K. et al. *Kriminológia*. Bratislava : Iura Edition, 2008, ISBN 978-80-8078-206-1, s. 361.
[10] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach.* Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s. 53.
[11] IVOR, J., KLIMEK, L. et ZÁHORA, J. *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky*. Žilina : Eurokódex, 2013, ISBNE 978-80-8155-017-1, str. 310.
[12] SMEJKAL, V. *Kybernetická kriminalita*. 2015, s. 135.
[13] PORADA, V., STRAUS, J. *Kriminalistika*. 2013, s. 510.

- túžba prekonať pocit nedocenenia svojich schopností – neúspech v reálnom živote, neschopnosť nadviazať sociálne kontakty, pocit odlúčenia od svojich vrstovníkov a podobne, vedie k nutkaniu kompenzácie týchto nedostatkov,
- politické alebo iné ideologické motívy.[14]

Obete počítačovej kriminality

Je veľmi dôležité vedieť koho si páchateľ vyberie ako svoj cieľ. Preventívne opatrenia možno uplatniť nielen v prípade, ak vieme kto môže byť páchateľom, ale predvídame i osobnostné predpoklady ľudí, ktorí sa môžu stať jeho potenciálnou obeťou. Všetci páchatelia, najmä tí inteligentní, si za svoju obeť vyberú osoby, ktoré predstavujú isté známky zraniteľnosti a bezbrannosti. Tak ako zlodej si zväčša za svoju obeť nevyberie niekoho kto je napríklad ozbrojený, tak aj páchatelia počítačovej kriminality si opatrne vyberajú osoby, voči ktorým sa pokúsia zasiahnuť. Môžeme hovoriť o štyroch druhoch obetí počítačovej kriminality: Naivné obete počítačovej kriminality, Zúfalé a chamtivé obete počítačovej kriminality, Neskúsené obete počítačovej kriminality a Náhodné obete počítačovej kriminality.[15]

Dynamika foriem počítačovej kriminality v slovenskej právnej úprave roky 2014 - 2017

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.[16] 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

Tohto trestného činu sa dopustí trestne zodpovedná osoba, ktorá svojím úmyselným konaním:

- 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.[17]

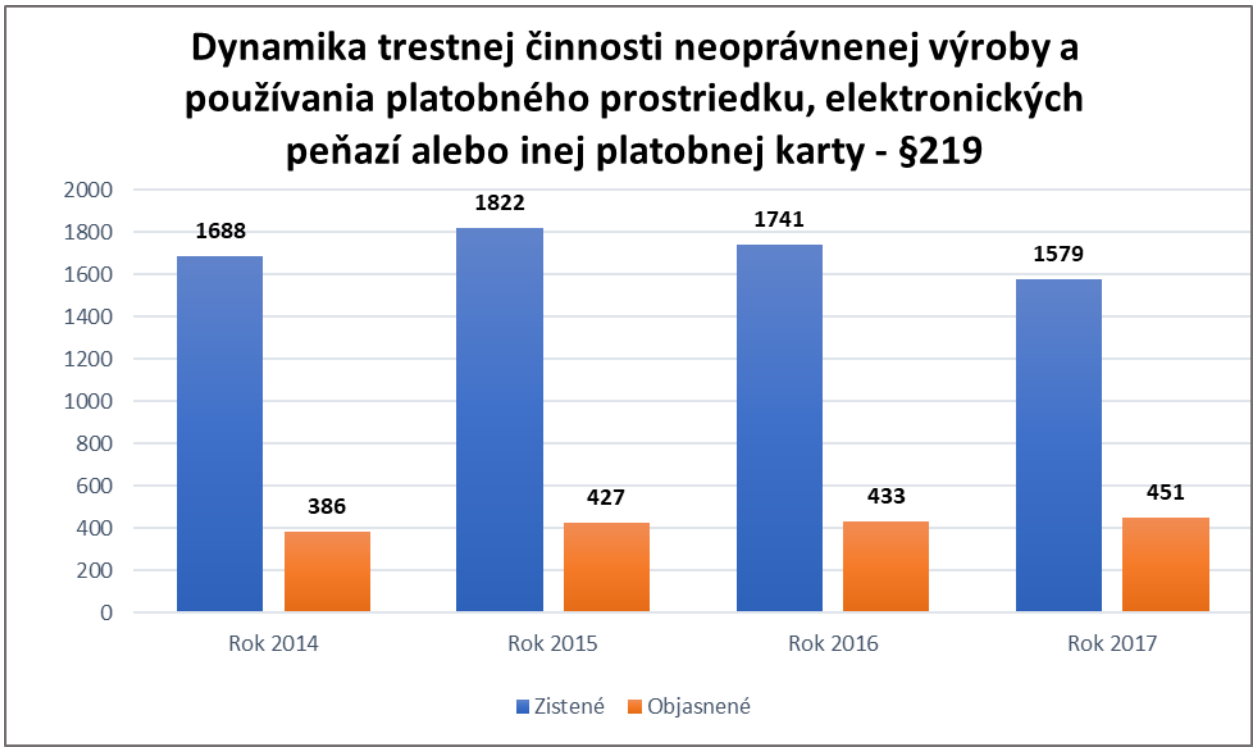
Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 1).

[14] PORADA, V., STRAUS, J. *Kriminalistika*. 2013, s. 512.

[15] 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>

[16] HOLCR, K., KLIMEK, L. Počítačová kriminalita v európskych súvislostiach. 2016, s. 87.

[17] IVOR, J. Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky. 2013, s. 299.



Graf č. 1 Dynamika konkrétnej trestnej činnosti
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.

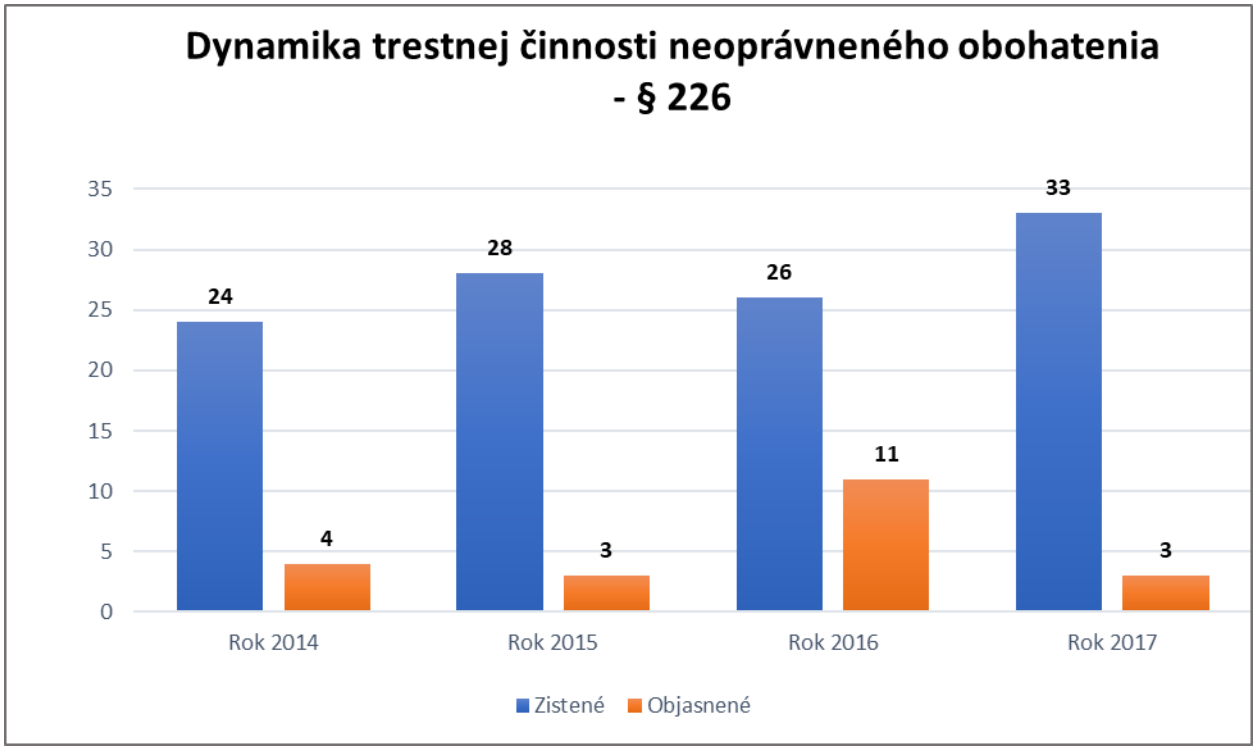
Pokiaľ ide o trestné činy v Slovenskej republike, ktoré sú zhodné s problematikou útokov na počítačové systémy , môžeme poukázať na trestný čin neoprávneného obohatenia (§ 226 TZ), trestný čin neoprávneného prístupu do počítačového systému (§ 247 TZ), trestný čin neoprávneného zásahu do počítačového 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.“[18] Najčastejším vykonaním tohto trestného činu sú neoprávnené zásahy do výherných automatov.

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 2).



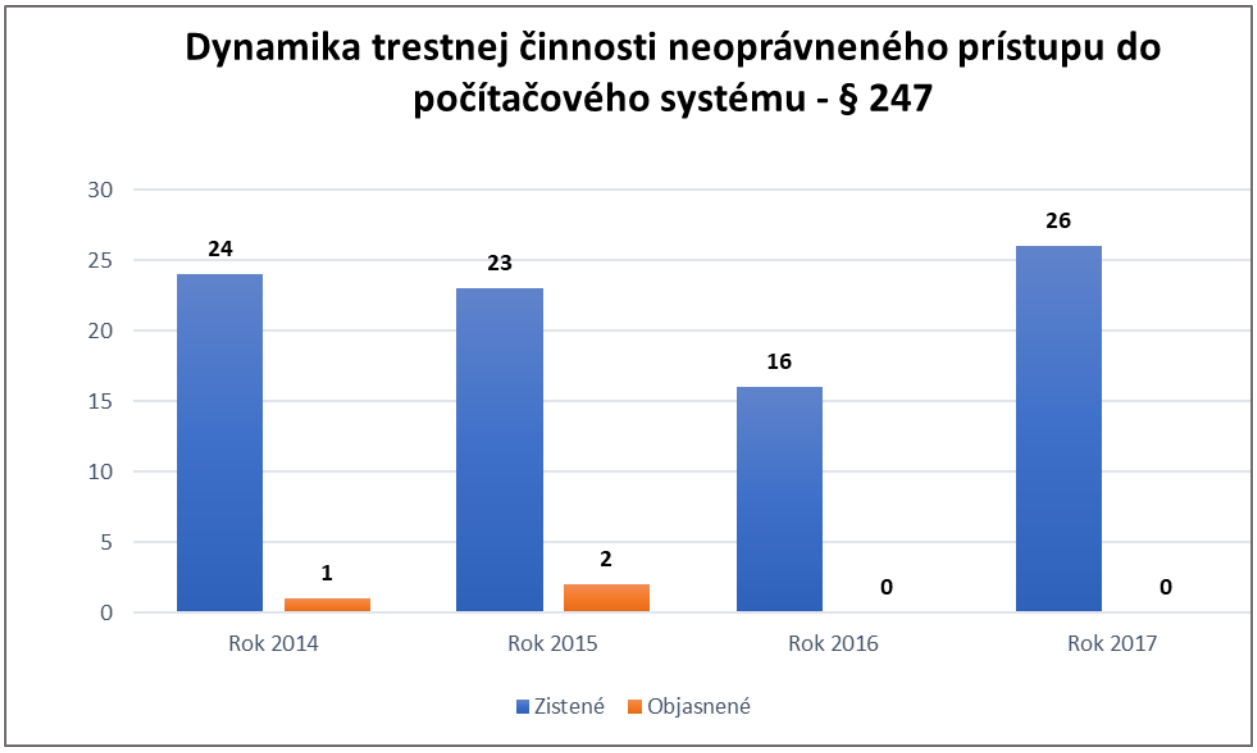
Graf č. 2 Dynamika konkrétnej trestnej činnosti
Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: www.minv.sk

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.[19]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 3).

[18] § 226 ods. 1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.
[19] § 247 ods.1. *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.



Graf č. 3 Dynamika konkrétnej trestnej činnosti
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.[20] S rozvojom internetu detská pornografia dostala ďalší rozmer, keďže je priamo prístupná na internete.

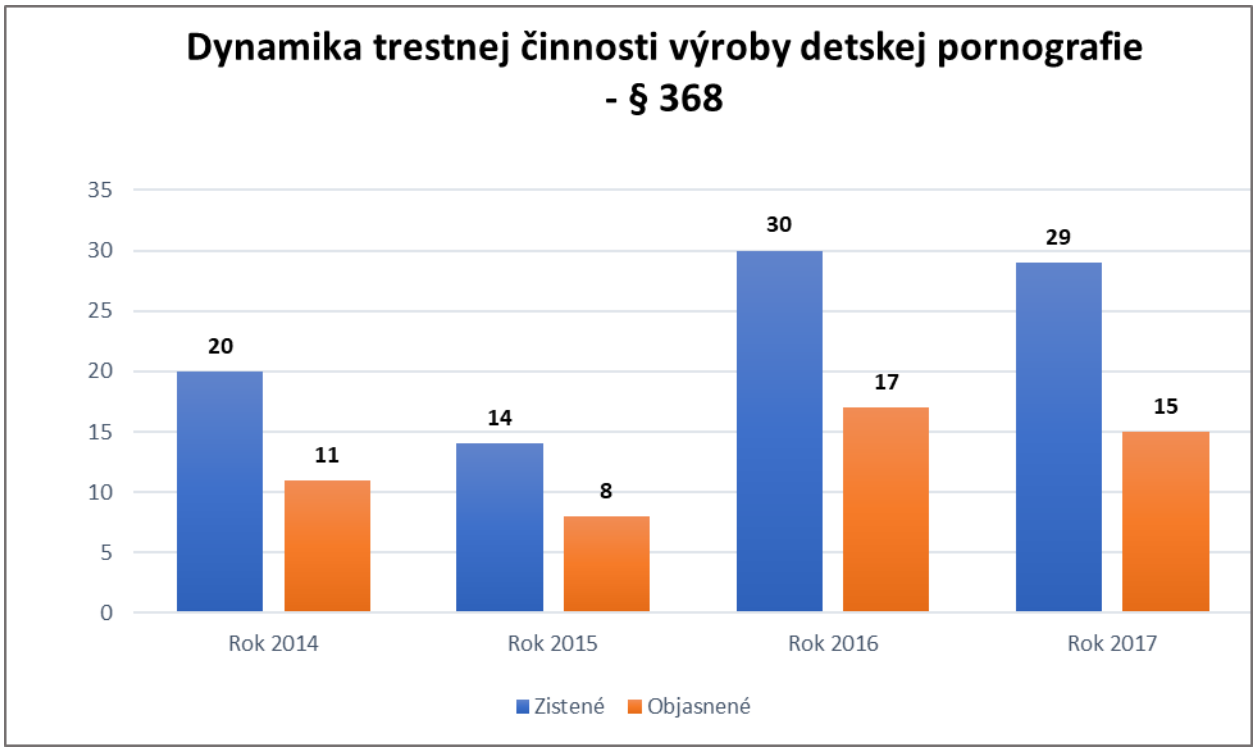
Pokiaľ ide o trestné činy v Slovenskej republike, ktoré sú zhodné s problematikou detskej pornografie na internete a kontaktovanie detí na účely ich sexuálneho zneužitia, môžeme poukázať na trestný čin výroby detskej pornografie (§ 368), trestný čin rozširovanie detskej pornografie (§ 369), trestný čin 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.“[21] 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 (graf 4).

[20] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s. 188.
[21] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s. 228.



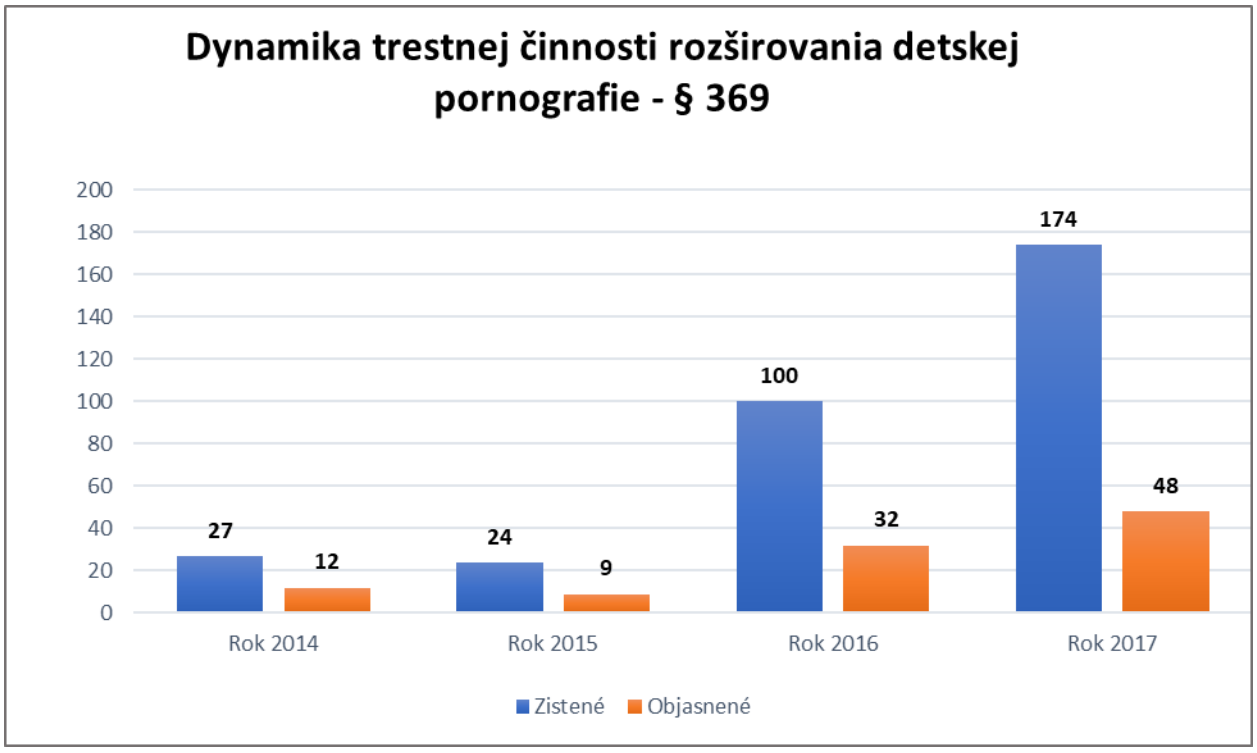
Graf č. 4 Dynamika konkrétnej trestnej činnosti
Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: www.minv.sk

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.“[22]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 5).

[22] § 369 ods.1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.



Graf č. 5 Dynamika konkrétnej trestnej činnosti
Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: www.minv.sk

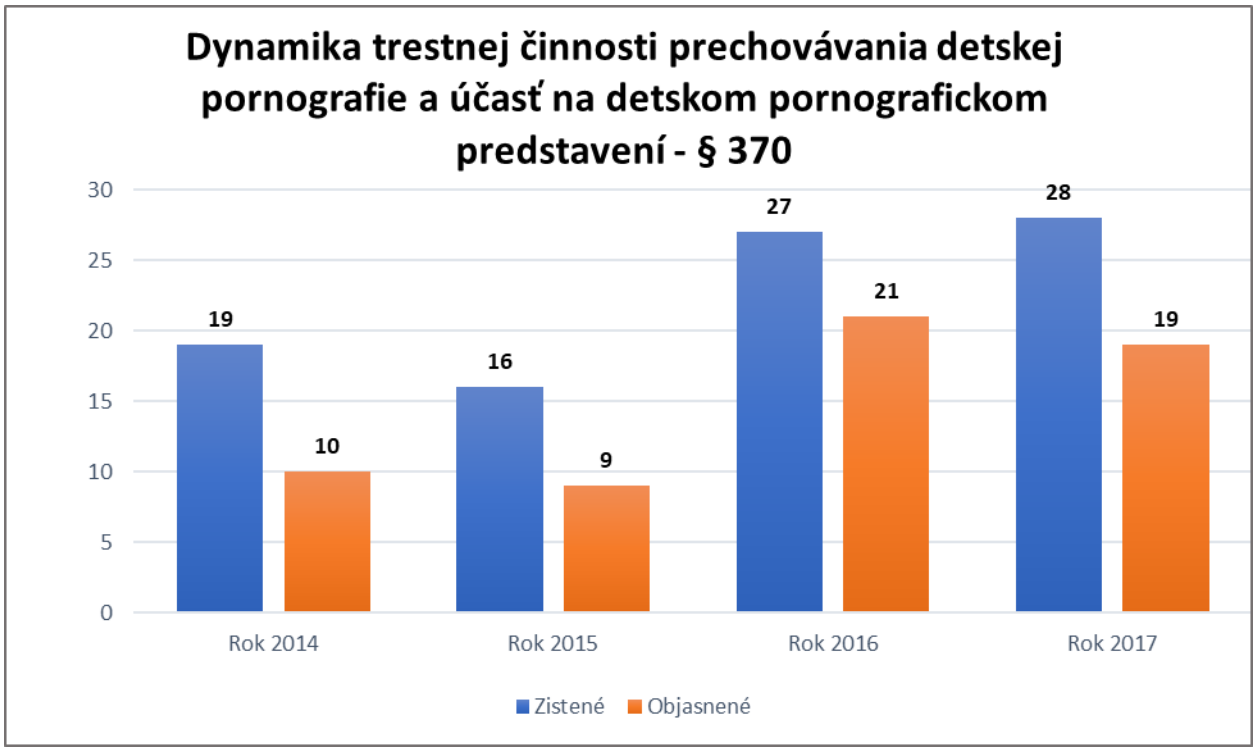
Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení

§ 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.“[23]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 6).

[23] KLIMEK, L., ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o., 2016, ISBN 978-80-8168-538-5, s. 265.



Graf č. 6 Dynamika konkrétnej trestnej činnosti
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.[24]

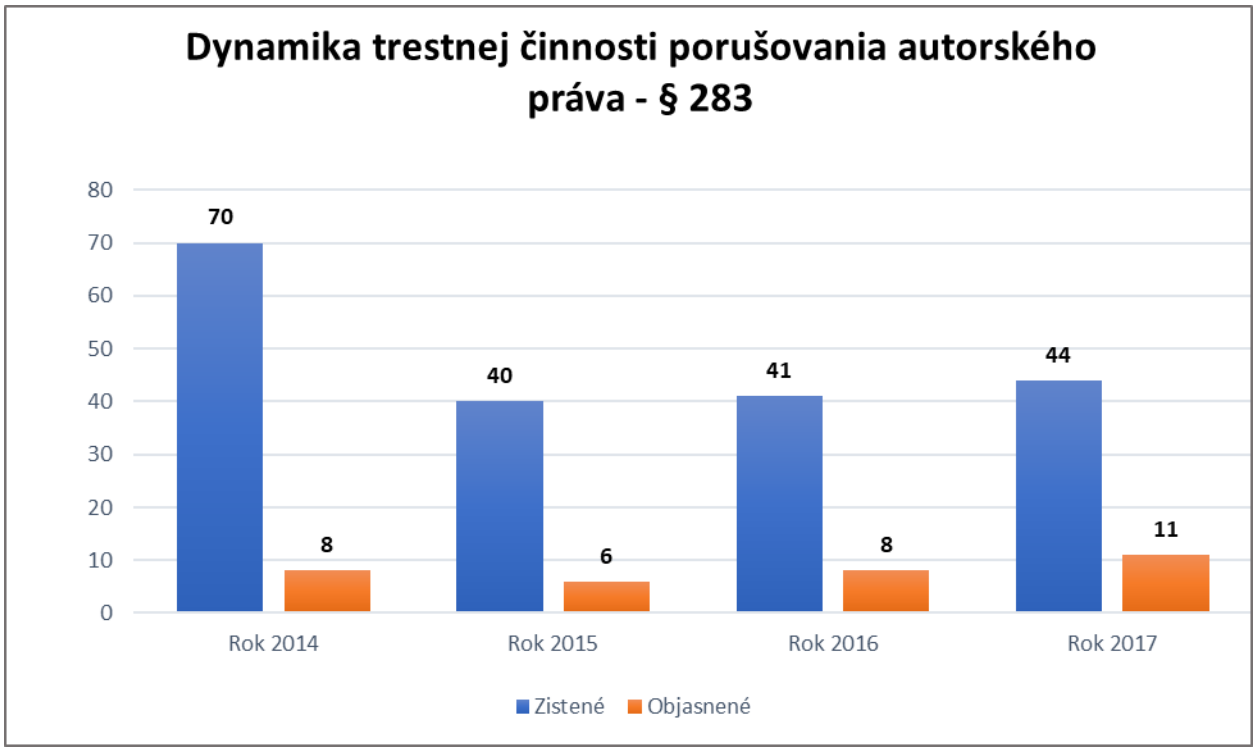
V Slovenskej republike ochranu autorského práva primárne poskytuje Trestný zákon v § 283 a Autorský zákon č. 185/2015 Z.z.

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.“[25]

Následne uvádzame dynamiku trestnej činnosti pri tomto trestnom čine vyjadrenú vo forme grafu (graf 7).

[24] SMEJKAL, V., PORADA, V. Současné problémy spojené s digitalizací, dokazováním, identifikací a autentizací při vyšetřovaní. In: *Bezpečnosť, extrémizmus, terorizmus: Zborník príspevkov*, s. 139.
[25] § 283 ods.1 *zákona č. 300/ 2005 Z.z. Trestný zákon* v znení neskorších predpisov.



Graf č. 7 Dynamika konkrétnej trestnej činnosti
Zdroj údajov: Ministerstvo vnútra SR. Dostupné na: www.minv.sk

Záver

Cieľom článku bolo zhrnutie základných východísk o počítačovej kriminalite ako celku. Ďalším účelom bolo poukázanie na jednotlivé spôsoby a formy, ktoré sú uvedené v osobitnej časti Trestného zákona, ktorými páchatelia počítačovej kriminality spôsobujú škody bežným užívateľom výpočtovej techniky. Zároveň sme v článku popísali páchateľov počítačovej kriminality, ich motívy páchania tejto kriminality a obete počítačovej kriminality. Jednou z najpodstatnejších častí tohto článku bolo uvedenie foriem počítačovej kriminality v slovenskej právnej úprave a ich následné grafické zobrazenie a porovnanie dynamiky za roky 2014 – 2017.

Zoznam použitej literatúry:

Monografie / knihy

IVOR, J., KLIMEK, L. *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky*. Žilina: EUROKÓDEX. ISBN 978-80-8155-017.

KLIMEK, L. ZÁHORA, J., HOLCR, K. *Počítačová kriminalita v európskych súvislostiach*. Bratislava : Wolters Kluwer s.r.o. ISBN 978-80-8168-538-5.

PORADA, V. a STRAUS, J. *Kriminalistika*: (výzkum, pokroky, perspektivy). Plzeň: Vydavatelství a nakladatelství Aleš Čenek. ISBN 978-0-521-864582-9.

SMEJKAL, V. *Internet @ §§§*. Praha: Garda. ISBN 80-247-0058-1.

SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-201-2.

ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, a.s.
ISBN 978-80-7552-758-5.

Článok zo zborníka

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 2014, ISBN 978-80-8054-601-4.
SMEJKAL, V. et 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.
Internetové zdroje
Epravo. *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>
Najpravo. *Základné formy počítačovej kriminality.* [online]. [cit. 15. 06. 2018]. Dostupné na internete:<http://www.najpravo.sk/clanky/zakladne-formy-pocitacovej-kriminality.html>
Ministerstvo vnútra SR. *Štatistika kriminality v Slovenskej republike 2014 – 2017* [online]. [cit. 15. 06. 2018]. Dostupné na internete: <www.minv.sk>
Preventista. 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/>
Zákony
Zákon č. 300/2005 Z.z. *Trestný zákon* v znení neskorších predpisov

Kontaktné údaje:
Mgr. Bc. Liliana Réveszová
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
liliana.reveszova@minv.sk

Sociálne inžinierstvo a páchanie trestného činu podvodu v kontexte počítačovej kriminality

Monika Širilová

Abstrakt:
Príspevok sa zaoberá fenoménom sociálneho inžinierstva a jeho vybraných foriem, konrétne pharmingm a phishingom, ktoré nepochybne súvisia s problematikou počítačovej kriminality. V úvode príspevku je pozornosť upriamená na neustály trend rastu počítačovej kriminality, pričom v nasledujúcich častiach je pozornosť venovaná najmä charakteristike a podstate pharmingu a phishingu. Následne v záverečnej časti poukazujem na prepojenie medzi pharmingom a phishingom, a trestným činom podvodu.
Kľúčové slová*:*
počítačová kriminalita, sociálne inžinierstvo, pharming, phishing, podvod

Abstract:
This article deals with phenomenon of social engineering and its particular forms, concretely pharming and phishing, which are undoubtedly linked with issue of computer criminality. In the introduction the attention is paid to steady growth of computer criminality, which in next parts the attention is paid mainly to characteristics and essence of pharming and phishing. Subsequently in final part I am pointing to connection between pharming and phishing and the crime of fraud.
Key words:
computer criminality, social engineering, pharming, phishing, fraud

Úvod

Počítačová kriminalita v súčasnosti celkom nepochybne predstavuje aktuálnu problematiku, ktorej význam a potenciál rastú priamo úmerne s tým, ako rýchlo sa rozvíjajú informačné technológie. Zjednodušene to znamená vzostup počítačovej kriminality.

Vývoj počítačov a počítačových systémov sa signifikantne zlepšuje a neustále zrýchľuje, pričom tieto sú stále výkonnejšie, menšie, lacnejšie a v neposlednom rade viac „user-friendly“[1]. V súvislosti s ich vývojom a dostupnosťou sa logicky rozšírili do celej spoločnosti, obchodného styku ako aj do osobného života takmer každého jednotlivca. Moderné obchodné spoločnosti a rovnako celé krajiny sú závislé na počítačových systémoch, ktoré podporujú ich činnosť, počínajúc personálnym manažmentom a končiac správou financií.

Počítače sa stali neoddeliteľnou súčasťou obchodných a štátnych procesov, pričom bez nich by v súčasnosti nebolo možné zabezpečiť riadne fungovanie obchodu či štátu. Pre ilustráciu sa skúsme na chvíľu zamyslieť a predstaviť si, ako by bez počítačových systémov fungovali daňové systémy, účtovníctvo, vykonávali sa audity, vyrábali automobily či zbrane, alebo ako by napríklad efektívne fungovali ozborojné zložky.

Rozmach lacných, výkonných a „user-friendly“ počítačov umožňuje čoraz väčsiemu množstvu ľudí ich používanie, a čo viac, má za následok, že sa ľudia čoraz viac spoliehajú na počítače v každodennom živote. Rovnako, ako sa na počítače spoliehajú ľudia v ich každodennom živote, obchodné spoločnosti aj jednotlivé štáty, spoliehajú sa na ne aj osoby, ktoré majú v úmysle páchať trestnú činnosť. Počítačová kriminalita, najmä v súvislosti s pácháním trestných činov podvodu, rovnako narastá, a je nepochybné, že je nárast sa bude zvyšovať, čím viac budú jednotlivé počítačové siete prepojené, a to najmä na medzinárodnej úrovni.

Nakoľko v súčasnosti neexistuje spôsob, ako presne určiť koľko fyzických ako aj právnických osôb sa stali obeťami počítačovej kriminality, je potrebné v danej súvislosti uviesť do pozornosti prieskumy niektorých spoločností, ktoré predstavujú základný stavebný kameň pochopenia vážnosti predmetnej problematiky.

[1] Pozn. autora: „user-friendly“ znamená priblíženie a prispôsobenie ovládania spôsobom, ktorý je bližší užívateľovi.

Do pozornosti uvádzam najmä „Globálny prieskum hospodárskej kriminality 2016. Správa za Slovensko.“ od spoločnosti PricewaterhouseCoopers (ďalej len „PWC“), v ktorom sa uvádza:

- 13% respondentov, ktorí sa na Slovensku stretli s hospodárskou kriminalitou uviedlo, že išlo počítačovú kriminalitu
- slovenskí respondenti považujú počítačovú kriminalitu za druhú najväčšiu hrozbu (17% respondentov) po sprenevere majetku a jej výskyt v priebehu najbližších 24 mesiacov považujú za pravdepodobný. Toto riziko je nižšie v porovnaní so Strednou a Východnou Európou (25%) aj so svetom (34%). Na druhej strane si 58% spoločností myslí, že riziko vzrástlo.[2]

Pojem počítačová kriminalita

Pojem počítačová kriminalita má v slovenskom jayzku niekoľko alternatív – napríklad kybernetická kriminalita alebo kyberkriminalita. V anglickom jazyku nachádzame oveľa viac alternatív, napríklad computer crime, ktorý je časovo najstarším pojmom, alebo novšie alternatívy cyber crime, resp. cybercrime alebo cyber-crime, zriedkavo taktiež pojmy high-tech crime, virtual crime alebo výnimočne e-crime.

Za súčasného stavu poznania je definovanie počítačovej kriminality mimoriadne náročná, ba priam nemožná úloha. Z praktického hľadiska je vhodnejšie poukázať na skupiny počítačových trestných činov:

1. trestné činy, ktorých cieľom je počítač,
2. trestné činy, pri ktorých je počítač používaný ako nástroj na ich spáchanie,
3. trestné činy, pri ktorých má počítač len vedľajšiu príležitostnú úlohu pri ich páchaní.

Ad 1. V prvom prípade je počítač cieľom či terčom útoku, pričom konanie spočíva napríklad v prieniku do počítača za účelom „krádeže“ dát, súborov či dokumentov, v neoprávnenom zásahu do informačných systémov alebo aj vo vydieraní založenom na hrozbách zo zverejnenia odcudzeného obsahu. V tomto prípade dochádza k neoprávnenému prístupu k počítaču, t.j. hackerstvu.

Ad 2. V prípade trestných činov, pri ktorých je počítač používaný ako nástroj, počítač slúži na uľahčenie páchania trestnej činnosti. Ide napríklad o falšovanie peňazí, falšovanie úradných listín, výrobu a distribúciu detskej pornografie na internete, porušovanie autorských práv, alebo v neposlednom rade ide o výrobu nelegálnych kópií počítačových programov.

Ad 3. V poslednom prípade, keď počítač má len vedľajšiu príležitostnú úlohu pri páchaní trestných činov, počítač zohráva malú úlohu a nie je potrebný na spáchanie trestného činu. Príkladom je napísanie vydieračského alebo výhražného listu, ktorý je napísaný na počítači, ale mohol byť napísaný aj na písacom stroji alebo rukou, taktiež ohováranie prostredníctvom internetu, ekonomická kriminalita či ilegálny predaj drog prostredníctvom internetu. Táto skupina počítačových trestných činov nepredstavuje počítačovú kriminalitu v pravom zmysle slova.[3]

Organizácia spojených národov vo svojom *Manuáli pre prevenciu a kontrolu počítačového zločinu* z roku 1994 na margo počítačovej kriminality hovorí, že sa jedná o tradičné zločinné aktivity ako krádež, podvod alebo falšovanie, teda o činy, ktoré sú trestné vo väčšine krajín sveta, pričom sa k ním pridružujú nové spôsoby zneužitia počítačov, ktoré sú, alebo by mali byť trestné.[4] Zjednodušene možno konštatovať, že ide o kriminalitu, ktorá súvisí

[2] Pricewaterhouse Coopers: Globálny prieskum hospodárskej kriminality 2016. Správa za Slovensko. Dostupné na: <https://www.pwc.com/sk/sk/forenzne-sluzby/assets/gecs-slovensko-2016.pdf>

[3] KLIMEK, L. Základy trestného práva Európskej únie. Bratislava : Wolters Kluwer, 2017, s. 102

[4] Manuál OSN pre prevenciu a kontrolu počítačového zločinu, OSN 1994. Dostupné na: <http://www.uncjin.org/Documents/EighthCongress.html

s počítačom ako predmetom trestnej činnosti, samozrejme vynímajúc ho ako hmotný predmet, alebo s počítačom ako nástrojom trestnej činnosti.

Z vyššie uvedených definícií je zrejmé, že pojem počítačová kriminalita je veľmi široký, z čoho vyplýva, že vzhľadom na limitovaný rozsah príspevku nie je možné venovať sa danej problematike komplexne a obsiahnuť všetky aspekty s ňou súvisiace. Z tohto dôvodu som sa rozhodla svoju pozornosť sústrediť na problematiku „sociálneho inžinierstva", ktorá podľa môjho názoru v súčasnosti predstavuje čoraz frekventnejšie sa vyskytujúci fenomén, resp. praktiku používanu na páchanie počítačovej kriminality, a to najmä trestných činov podvodu.

Sociálne inžinierstvo

Samotný pojem sociálne inžinierstvo je možné definovať ako ovplyvňovanie a presviedčanie ľudí s cieľom oklamať ich tak, aby uverili, že sociotechnik je skutočne osoba s totožnosťou, ktorú predstiera a ktorú si vytvoril pre potreby manipulácie. Vďaka tomu je sociotechnik schopný využiť ľudí, s ktorými hovorí, a rovnako aj technologické prostriedky.[5]

Existuje množstvo ďalších definícií, avšak zo všetkých vyplýva, že pokiaľ ide o bezpečnosť počítačových systémov, najslabším článkom v reťazci vždy bol a bude človek.

Základnú ideu sociálneho inžnierstva predstavuje otázka „prečo by sa na prelamovanie hesiel mala používať brutálna sila, keď je oveľa jednoduchšie prinútiť niekoho, kto heslo pozná, aby nám ho prezradil."[6] Pri vhodne vedenom útoku si navyše obeť v prevažnej väčšine prípadov vôbec neuvedomí, že bola „okradnutá" o cenné informácie. Práve túto skutočnosť môžeme považovať za najnebezpečnejšiu črtu sociálneho inžinierstva. Keď nám niekto odcudzí peňaženku s kreditnou kartou, je nám okamžite jasné, že túto skutočnosť musíme oznámiť príslušnej banke a naša kreditná karta bude okamžite zablokovaná. Avšak v prípade, ak útočník použije sociálne inžinierstvo, sa ako obeť vôbec nemusíme dozvedieť, že nás niekto pripravil o tieto informácie. Tretie tisícročie je taktiež nazvané informačným vekom, kde je úspešný ten, kto ovláda spôsob ako hľadať, získavať a správne vyhodnocovať informácie. Bohužiaľ musím konštatovať, že ľudia si stále neuvedomujú cenu informácií ako aj skutočnosť, že informácie je potrebné náležitým spôsobom zabezpečiť.

Druhou príčinou toho, že je možné vykonávať sociotechnické útoky na pomerne dôležitých miestach vyplýva z virtuality odboru informačných technológií. V danom prípade absentuje schopnosť prenesenia týchto pojmov do reality. Zjednodušene môžeme konštatovať, že ľudia nepovažujú za dôležité to, na čo nemôžu siahnuť. Ako príklad uvádzam nasledovnú situáciu. Ak kolegovi bude odcudzený bicykel, je všetkým jasné, že došlo k spáchaniu trestného činu krádeže. Ak by si však niekto od kolegu skopíroval jeho program alebo výsledky jeho celoročnej práce elektronickou cestou, tak sa v podstate nič nestalo. Kolegovi nič nezmizlo a neutrpel žiadnu hmotnú ujmu.

Väčšina ľudí považuje prieniky do počítačových systémov za čisto technickú záležitosť, kedy „páchateľ" využil medzery systému vo svoj prospech. Podstata však spočíva v tom, že úloha pomocníka zohráva pri prekonávaní bezpečnostnej bariéry sociotechnikom významnú úlohu. Nedostatočná informovanosť používateľov často poskytuje výnimočnú príležitosť využiť ich ako „vstupnú bránu" do počítačového systému v prípadoch, kedy k nemu útočník nemá žiadny autorizovaný prístup.

Použitie sociálneho inžinierstva predstavuje v prevažnej väčšine prípadov „najlacnejší" a zároveň najdnoduchší spôsob, ako narušiť bezpečnosť inak veľmi robustných systémov. Vo

[5] ŠIMEK, R. Kolokviální práce [online], Historie a vývojové trendy ve výpočetní technice, Fakulta informatiky, Masarykova univerzita Brno, 2003. Dostupný na:
< http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>.

[6] MITNICK, K., SIMON, W. *The Art of Intrusion*; 1. vydanie, Wiley; 2005. s. 34

všobecnosti sa o sociálnom inžinierstve dá povedať, že útoky majú vysoké percento úspešnosti a sú veľmi zákerné. Pri dobrom skrývaní útočníka je navyše takmer nemožné ho vystopovať.[7]

V rámci sociálneho inžinierstva využívajú útočníci množstvo metód, ktoré vedú k získaniu požadovaných informácií. Nie všetky metódy však nevyhnutne súvisia s počítačovou kriminalitou ako takou. Z tohoto dôvodu sa v nasledujúcej časti môjho príspevku nebudem venovať metódam, kde utočník komunikuje s osobami priamo „tvárou v tvár", prípadne prostredníctvom telefónu. Svoju pozornosť upriamim na dve metódy, ktorými su „phishing" a „pharming".

Phishing

Phishing môžeme charakterizovať ako podvodnú techniku používanú prostredníctvom internetu, ktorej cieľom je získavanie citlivých údajov (napr. hesiel, čísel kreditných kariet a pod.) od obetí útoku. Podstatou phishingu je rozosielanie e-mailových správ, ktoré vyzerajú ako oficiálne žiadosti banky, prípadne inej inštitúcie, a ktoré vyzývajú adresáta na zadanie jeho údajov do odkazovanej stránky. Táto stránka môže napríklad napodobňovať prihlasovacie okno internetového bankovníctva, prípadne stránku inej spoločnosti. Užívateľ zadá svoje prihlasovacie meno a heslo, prípadne iné údaje, ktoré nasledne umožnia útočníkom páchať trestnú činnosť.

Phishing v e-mailoch a na internete využíva možnosť zverejniť odkaz, ktorý v skutočnosti vedie inam, než to predstiera. V minulosti sa útočníci v odkazoch snažili zachovať aspoň časť adresy skutočnej internetovej stránky, avšak aktuálne vlny phishingu sa touto skutočnosťou vôbec nezaťažujú, a to z dôvodu, že bežní užívatelia častokrát vôbec nemajú vedomosť o tom, ako by mala vyzerať originálna internetová adresa.[8]

Hlavnou podstatou phishingu je zber informácií, ktoré následne útočník použije na svoje finančné, prípadne iné obohatenie, čím sa dopúšťa trestného činu podvodu, prípadne aj iného trestného činu v zmysle Trestného zákona.

Autori phishingových správ vo veľkej miere zneužívajú dôverčivosť používateľov internetu. Americké prieskumy dokazujú, že v jednotlivých kampaniach býva postihnutých až 5% používateľov, pričom v mohých prípadoch býva ich počet dokonca väčší.[9] Pre väčšinu používateľov internetu predstavuje neznalosť problematiky zásadný handicap. V súčasnosti nie len dotknuté inštitúcie, ale rovnako aj médiá prispievajú k zvyšovaniu informovanosti verejnosti prostredníctvom zverejňovania rôznych interných ako aj externých správ.

V súvislosti s phishingom považujem za potrebné rovnako uviesť do pozornosti tzv. „spear phishing", ktorý sa do centra diania dostal pár rokov dozadu. Spear phishing predstavuje cielený útok na obchodné spoločnosti, ktorého cieľom je presvedčiť obeť o tom, že predmetný email pochádza priamo zvnútra, od výkonného riaditeľa predmetnej spoločnosti, prípadne od vedenia jej obchodného partnera. Obsah predmetného emailu tvoria inštrukcie resp. príkazy priamo zamestnancovi, aby vykonal bankový prevod určite finančnej čiastky za účelom zabezpečenia kontinuity podnikania. V mnohých prípadoch, následne po zaslaní emailu, sa útočník telefonicky spojí priamo so zamestnancom, ktorému bol predmetný email adresovaný a vydáva sa priamo za odosielateľa, prípadne za právneho zástupcu odosielateľa.

[7] SECURITY WORLD 4/2008, Interní zaměstnanci, IDG CZECH, a.s, s. 25

[8] HOBZA, O. EMAG : technologický magazín [online]. 1998. Dostupný na: <http://www.emag.cz/vishing-phishing-pres-telefon/>.

[9] BITTO, O. LUPA : server o českém internetu [online]. 1998. Dostupný na: <http://www.lupa.cz/clanky/jak-se-nechytit-na-phishingovounavnadu/>

Na zdôraznenie vážnosti a miery nebezpečnosti predmetných útokov uvádzam do pozornosti Bulletin FBI, v zmysle ktorého bola hodnota škody vzniknutej na základe spear phishingu v USA od októbra 2013 do februára 2016 2,3 miliardy dolárov.[10]

Pharming

Pharming je možné charakterizovať ako činnosť, pri ktorej útočníci presmerúvajú internetovú komunikáciu z jedného webu na iný, ktorý vyzerá rovnako, s cieľom zmiasť užívateľa tak, aby zadal svoje údaje ako užívateľské meno a heslo do databázy na ich falošnom webe.

Samotný pharming má dve podoby, z ktorých jedna je omnoho efektívnejšia, ale pre útočníka zároveň obtiažnejšia, čo značne obmedzuje jej použitie. Použitie druhej metódy je značne jednoduchšie, avšak zároveň je možné sa proti nej efektívnejšie brániť. Obom metódam sa budem venovať ďalej v mojom príspevku.

V predmetnej súvislosti považujem za potrebné uviesť do pozornosti rozdiel medzi pharmingom a phishingom, ktorý spočíva v tom, že pri phishingu sa od užívateľa vyžaduje, aby „klikol" na internetový odkaz uvedený v emaile od útočníka. Pri použití pharmingu je užívateľ priamo odkázaný na internetový odkaz útočníka bez toho, aby o tom vedel a musel osobitne „kliknúť" na nejaký internetový odkaz.

V nasledujúcej časti sa budem venovať obom metódam pharmingu zmienených vyššie. Vo všeobecnosti sa tieto metódy môžu rozdeliť na globálnu a lokálnu.

Podstata globálneho pharmingu spočíva v tom, že útočník neoslovuje konkrétneho úžívateľa, ale napadne vybraný DNS server.[11] Pokiaľ sa útočníkovi podarí zmeniť záznam v zabezpečenom DNS serveri, tak všetci užívatelia, ktorí sú pripojení na tento DNS server a zadajú do adresového riadku internetového prehliadača správnu adresu (napríklad adresu internetového bankovníctva), budú automaticky odkázaní na falošnú stránku. V prípade, ak je táto falošná stránka značne prepracovaná, je takmer nemožné zistiť, že sa jedná o podvod. Jediným spôsobom, ako je v danom prípade možné zistiť, že sa nejedná o originálnu stránku, je kontrola certifikátu, ktorým je táto stránka podpísaná, nakoľko útočník nie je schopný vykonať zmeny v predmetnom certifikáte.

Na druhej strane, podstatu lokálneho pharmingu predstavuje útok na jednotlivé počítače. Osobné počítače, ktoré pracujú na operačnom systéme Windows obsahujú tzv. hosts súbor, ktorý funguje obdobne ako DNS server – obsahuje IP adresy a korešpondujúce domény. Ak sa útočníkovi podarí do predmetného súboru zapísať adresu podvodnej stránky, vo vzťahu k užívateľovi dochádza k rovnakému efektu ako v predchádzajúcom prípade. Teda aj po zadaní správnej internetovej stránky bude zobrazená podvodná stránka a všetky údaje automaticky získa útočník.

Z uvedeného jasne vyplýva, že prvá metóda je nezávislá na osobných počítačoch jednotlivých užívateľov, avšak útočník najskôr musí prelomiť ochranu DNS servera, ktorý sa vyznačuje najvyšším stupňom ochrany. Nakoľko táto metóda je značne komplikovaná a prináša so sebou riziko detekovania správcom servera, je z pohľadu počítačovej kriminality nepochybne ľahšie zvoliť si druhú alternatívu.[12]

Sociálne inžinierstvo a trestný čin podvodu

[10] FBI: „FBI Warns of Dramatick Increase in Business E-Mail Scams. Dostupné na: <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams>

[11] Pozn. autora: DNS (Domain Name System) je hierarchický systém doménových mien, ktorý je realizovaný prostredníctvom serverov DNS a protokolom s totožným menom, medzi ktorými dochádza k výmene informácií. Jeho hlavnou úlohou sú vzájomné prevody doménových mien a IP adries. Dostupné na: <www.wikipedia.sk>

[12] BEDNÁŘ, V. Lupa : server o českém internetu [online]. Dostupný na: <http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/>

V nadväznosti na vyššie uvedené možno za pomoci analógie vyvodiť záver, že sociálne inžinierstvo v kontexte počítačovej kriminality nepochybne súvisí s trestnou činnosťou páchanou na počítači, keďže jednoznačným cieľom páchateľa je získanie citlivých informácií súvisiacich s prihlasovacími údajmi, heslami, prípadne osobnými údajmi užívateľov.

V predmetnej súvislosti sa do popredia dostáva otázka následného využitia takto získaných informácií. Z aplikačnej praxe nepochybne vyplýva, že páchatelia takto získané informácie využívajú na získanie istého obohatenia, pričom nemusí ísť nutne len o peňažné obohatenie. Zákon č. 300/2005 Z.z. Trestný zákon v § 221 ustanovuje, že podvodom sa rozumie obohatenie seba alebo iného tým, že páchateľ uvedie niekoho do omylu alebo využije niečí omyl. Z predmetnej definície skutkovej podstaty vyplýva, že pharming a phishing môžeme zaradiť k novým spôsobom páchania podvodov prostredníctvom internetu.

Od takpovediac klasických druhov podvodov sa pharming a phishing odlišujú tým, že ich samotné odhalenie, ale najmä vyšetrenie je veľmi obtiažne. Pre orgány činné v trestnom konaní je značne komplikované a v mnohých prípadoch dokonca nemožné vystopovať páchateľov, nakoľko títo využívajú rôzne spôsoby internetového pripojenia. Rovnako uvádzam do pozornosti skutočnosť, že páchatelia rovnako vo väčšine prípadov páchajú trestnú činnosť zo zahraničia, čo opätovne komplikuje celý priebeh vyšetrovania, nakoľko slovenské orgány činné v trestnom konaní nedisponujú žiadnou právomocou na území iného štátu. V uvedených prípadoch je potrebné žiadať o spoluprácu prostredníctvom inštitútu právnej pomoci, čo je však problematické z časového hľadiska.

Z vyššie uvedeného vyplýva, že prevencia a obozretnosť internetových užívateľov je najlepšia cesta, ako čeliť týmto hrozbám. Zásadne platí, že prostredníctvom internetu by sa nemali zdieľať údaje o platobných kartách, ich PIN kódoch, ani iné údaje, ktorých zneužitie by mohlo viesť k majetkovej ujme.

Záver

Cieľom môjho príspevku bolo priblíženie sociálneho inžinierstva ako takého a zároveň niektorých jeho foriem, konkrétne pharmingu a phishingu, ktoré sa priamo dotýkajú problematiky počítačovej kriminality ako takej. Ako to vyplýva zo samotného príspevku sociálne inžinierstvo predstavuje novodobý fenomén, ktorý sa neustále rozmáha a postihuje čoraz väčšie množstvo jednotlivcov ako aj obchodných spoločností. Je nepochybné, že najväčšie riziko v oblasti bezpečnosti a ochrany pred sociálnym inžinierstvom predstavuje človek ako taký. V závere si dovolím konštatovať, že v súčasnosti nie je možné úplne predísť útokom sociálnych inžinierov. Z hľadiska prevencie je preto najdôležitejšie informovať širokú verejnosť, klientov, ako aj vlastných zamestnancov o týchto hrozbách. Zvyšovaním povedomia a sociálnom inžinierstve nezabránime len tomu, aby sa osobné a citlivé informácie dostali do rúk utočníkov, ale zároveň prispejeme aj k znižovaniu kriminality, a to najmä trestných činov podvodov.

Zoznam použitej literatúry:

BEDNÁŘ, V. *Lupa : server o českém internet*.
Dostupný na: http://www.lupa.cz/clanky/pharming-je-zpet-a-silnejsi/
BITTO, O. *LUPA : server o českém internetu.* 1998. Dostupný na: http://www.lupa.cz/clanky/jak-se-nechytit-na-phishingovounavnadu/
FBI. *„FBI Warns of Dramatick Increase in Business E-Mail Scams.* Dostupné na: https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams
HOBZA, O. *EMAG: technologický magazín, 1998.*
Dostupný na: http://www.emag.cz/vishing-phishing-pres-telefon/

KLIMEK, L. *Základy trestného práva Európskej únie.* Bratislava : Wolters Kluwer, 2017, ISBN 978-80-8168-601-6, 264 s.
Manuál OSN pre prevenciu a kontrolu počítačového zločinu, OSN 1994. Dostupné na: http://www.uncjin.org/Documents/EighthCongress.html
MITNICK, K., SIMON, W. *The Art of Intrusion*; 1. vydanie, Wiley; 2005. ISBN 978-0764569593, 290 s.
Pricewaterhouse Coopers. *Globálny prieskum hospodárskej kriminality 2016*. Správa za Slovensko. Dostupné na: https://www.pwc.com/sk/sk/forenzne-sluzby/assets/gecs-slovensko-2016.pdf
SECURITY WORLD 4/2008, *Interní zaměstnanci*, IDG CZECH, a.s,
ŠIMEK, R. *Kolokviální práce. Historie a vývojové trendy ve výpočetní technice*, Fakulta informatiky, Masarykova univerzita Brno, 2003. Dostupný na: <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>

Kontaktné údaje:
Mgr. Monika Širilová, MLA
Fakulta práva
Paneurópska vysoká škola v Bratislave
monika.sirilova@centrum.sk

Možnosti oznamovania kriminality páchanej v kybernetickom priestore bezpečnostným zložkám

Viktor Šoltés, Ladislav Mariš

Abstrakt:
Bezpečnostné zložky musia byť schopné v čo najkratšom čase kriminalitu páchanú v kybernetickom priestore odhaliť, zamedziť jej šíreniu a odhaliť jej páchateľov. Na tento účel sa v jednotlivých krajinách Európskej únie využívajú rôzne online platformy pre nahlasovanie takýchto bezpečnostných incidentov. Príspevok sa zaoberá analýzou online platforiem využívaných v rôznych krajinách Európskej únie pre nahlasovanie kriminality páchanej predovšetkým v kybernetickom priestore. Závery príspevku môžu byť využité pri návrhu a implementácii podobného systému aj v podmienkach Slovenskej republiky.
Kľúčové slová:
Kybernetická bezpečnosť, kriminalita, bezpečnostné zložky, online, legislatíva

Abstract:
Security components must be able to detect, prevent, and detect offenders within the shortest possible period of cyber crime. For this purpose, different online platforms are used to report such security incidents across the European Union. This paper deals with the analysis of online platforms used in various countries of the European Union to report crimes committed primarily in cyberspace. Conclusions of the contribution can be used to design and implement a similar system in the Slovak Republic as well.
Key words:
Cyber security, crime, security forces, online, legislation

Úvod

Rozvoj technológií v súčasnom svete so sebou okrem množstva pozitív prináša aj isté druhy negatív. Jednou z možností, ako zabezpečiť rozvoj spoločnosti je rozširovanie informačnej spoločnosti u obyvateľov. Informačná spoločnosť však so sebou prináša aj nové formy hrozieb. Úlohou štátu je prijímať opatrenia, ktoré budú jeho občanov chrániť pred kybernetickými bezpečnostnými hrozbami a kybernetickou kriminalitou. Jednou z možností boja proti kybernetickým bezpečnostným incidentom je aj vytváranie prijateľného užívateľského prostredia pre nahlasovanie takýchto incidentov.

Zákonná úprava kybernetickej bezpečnosti

Prvá legislatívna norma **Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z.** (ďalej „zákon“), ktorá upravuje problematiku kybernetickej bezpečnosti na Slovensku, bola dňa 09. marca 2018 publikovaná v Zbierke zákonov Slovenskej republiky a má účinnosť od apríla 2018.

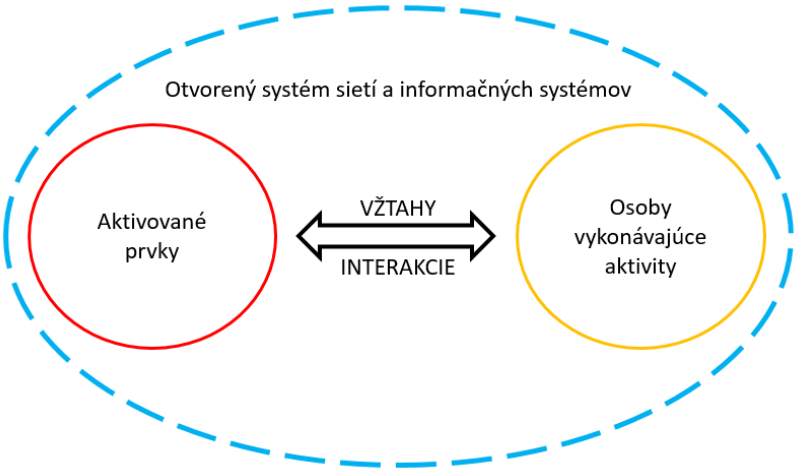
Zákon systematicky a v plnom rozsahu upravuje problematiku kybernetickej bezpečnosti, vrátane transpozície Smernice Európskeho parlamentu a Rady (EÚ) č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii[1]. Zákon o kybernetickej bezpečnosti ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti a upravuje[2]:

- organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- národnú stratégiu kybernetickej bezpečnosti,
- jednotný informačný systém kybernetickej bezpečnosti,
- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (jednotky CSIRT) a ich akreditáciu,

[1] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
[2] Zákon č 69/2018 Z. z. o kybernetickej bezpečnosti

- postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,
- bezpečnostné opatrenia,
- systém zabezpečenia kybernetickej bezpečnosti,
- kontrolu nad dodržiavaním tohto zákona, audit a sankcie.

Zákon vymedzuje základné pojmy, pričom definuje o. i. aj **kybernetický priestor** ako **globálny dynamický otvorený systém sietí a informačných systémov**, ktorý tvoria aktivované prvky kybernetického priestoru, **osoby** vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi (Obrázok 1).



Obrázok 1 Kybernetický priestor podľa zákona o kybernetickej bezpečnosti

Kybernetickou bezpečnosťou rozumieme podľa zákona 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 sa rozumie 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 ktorej následkom je:

- **strata dôvernosti** údajov, **zničenie** alebo **narušenie integrity** systému,
- **obmedzenie** alebo **odmietnutie dostupnosti** základnej služby alebo digitálnej služby,
- **vysoká pravdepodobnosť kompromitácie** činnosti základnej služby alebo digitálnej služby alebo
- **ohrozenie bezpečnosti** informácií.

Riešením kybernetického bezpečnostného incidentu rozumieme podľa zákona **všetky postupy** súvisiace s **oznamovaním**, **odhaľovaním**, **analýzou** a **reakciou** na kybernetický bezpečnostný incident a s **obmedzením** jeho **následkov**[3].

Koncepcia kybernetickej bezpečnosti Slovenskej republiky

17. júna 2015 vláda Slovenskej republiky schválila uznesením č. 328/2015 Koncepciu kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, ktorej cieľom je navrhnúť nový inštitucionálny rámec riadenia kybernetickej bezpečnosti v Slovenskej republike[4].

[3] Zákon č 69/2018 Z. z. o kybernetickej bezpečnosti

[4] ŠOLTÉS, V., MIŠÍK, J., KUBÁS, J., ŠTOFKOVÁ, Z. Education in information security. In INTED 2016 : proceedings. Valencia, Spain: IATED Academy, 2016. s. 4418-4424.

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[5].

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020

Návrh akčného plánu vláda Slovenskej republiky schválila dňa 2. marca 2016 uznesením č. 93/2016. Akčný plán obsahuje návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru štátu pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť Slovenskej republike nenahraditeľné škody, a tak by mohla byť narušená dôveryhodnosť štátu, či organizácie. Akčný plán ku Koncepcii je jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík, medzinárodnej spolupráce, zvyšovania povedomia a spôsobilostí, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru. Jednotlivé úlohy sú zoskupené v ôsmich prioritných oblastiach, s určením zodpovedného riešiteľa a spolupracujúcich subjektov, vrátane časového rámca ich realizácie.[6]

Národná jednotka pre riešenie kybernetických incidentov SK-CERT

V súvislosti s určením Národného bezpečnostného úradu (NBU) za ústredný orgán štátnej správy pre kybernetickú bezpečnosť od 1. januára 2016 NBU prevádzkuje útvar Slovak Computer Emergency Response Team (SK-CERT). Útvar zabezpečuje služby spojené s riadením bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov. SK-CERT ako národná jednotka CSIRT poskytuje svojim partnerom tieto služby[7]:

- proaktívne služby na zabezpečenie včasnej detekcie a prevencie kybernetických incidentov,
- reaktívne služby na vzniknuté hrozby a incidenty (napr. reakcia a riešenie kybernetických bezpečnostných incidentov),
- manažment kvality a zabezpečenia spojený s hodnotením a následným kontinuálnym zlepšovaním bezpečnosti organizácií,
- monitoring bezpečnosti za účelom zberu informácií o kybernetických bezpečnostných incidentoch z rôznych zdrojov prostredníctvom špecializovaných technických nástrojov,
- vydávanie bezpečnostných bulletinov a varovaní a tým včasne oznamovať a vhodne distribuovať informácie ohľadom kybernetickej bezpečnosti na národnej aj medzinárodnej úrovni.

Národná jednotka pre riešenie počítačových incidentov CSIRT.SK

CSIRT.SK (Computer Security Incident Response Team) je špecializovaná jednotka pre riešenie počítačových incidentov v Slovenskej republike. Bola zriadená uznesením vlády SR č. 479/2009 z 1. júla 2009 v súlade s Národnou stratégiou pre informačnú bezpečnosť v Slovenskej republike (uznesenie vlády SR č. 570/2008) Ministerstvom financií SR s cieľom zabezpečiť primeranú úroveň ochrany národnej informačnej a komunikačnej infraštruktúry (NIKI) a kritickej informačnej infraštruktúry. Webové sídlo Národnej jednotky CSIRT.SK (Obrázok 2) je www.csirt.gov.sk, ktoré zriadilo DataCentrum (rozpočtová organizácia Ministerstva financií SR.

[5] Národný bezpečnostný úrad, Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020.
[6] Národný bezpečnostný úrad, Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.
[7] Národný bezpečnostný úrad, Služby SK-CERT.

Obrázok 2 Webové sídlo Národnej jednotky CSIRT.SK

Tím zabezpečuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi, telekomunikačnými operátormi, poskytovateľmi internetových služieb a inými štátnymi orgánmi (napr. polícia, vyšetrovatelia, súdy), podieľa sa na budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti, aktívne kooperuje so zahraničnými organizáciami a reprezentuje SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni[8].

Európske CSIRT tímy

Sieť jednotiek CSIRT (CSIRTs Network, ďalej len „sieť“) pozostáva z jednotiek CSIRT členských štátov a jednotky CERT-EU, ktorá je CSIRT tímom európskych inštitúcií. Cieľom tejto siete je výmena informácií na dobrovoľnej báze o službách, činnostiach, spôsobilostiach a incidentoch na základe vybudovanej dôvery medzi jednotlivými tímami. V prípade incidentu môže táto sieť vymieňať, sprístupňovať a prerokúvať informácie a prediskutovať a vykonať koordinovanú reakciu na incident či poskytnúť podporu pri jeho riešení[9].

Jednotný informačný systém kybernetickej bezpečnosti

Jednotný informačný systém kybernetickej bezpečnosti (JISKB) je informačný systém, ktorého správcom a prevádzkovateľom je úrad a ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT. JISKB je určený aj na spracovanie a vyhodnocovanie údajov a informácií o stave kybernetickej bezpečnosti. JISKB obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. JISKB pozostáva z verejnej časti a neverejnej časti a prístup k nemu je bezodplatný. Verejná časť jednotného JISKB obsahuje[10]:

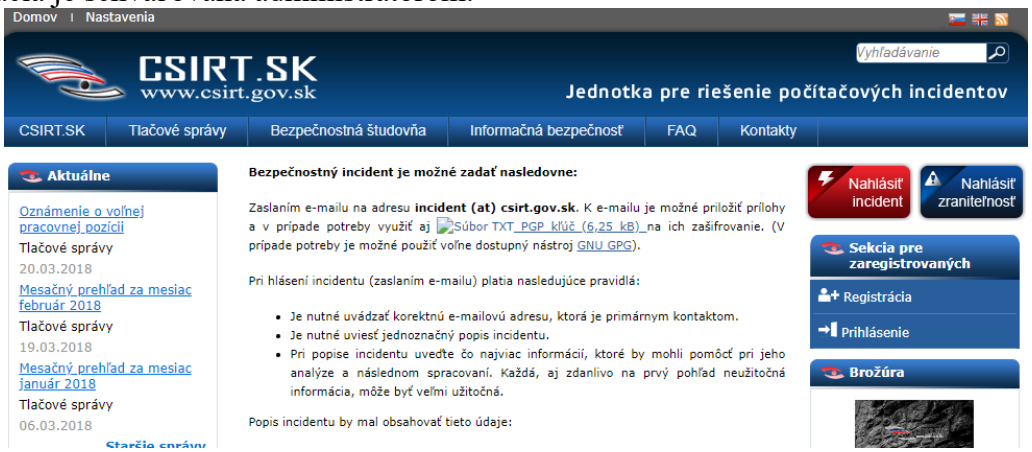
- register ústredných orgánov,
- zoznam základných služieb,

[8] Zákon č 69/2018 Z. z. o kybernetickej bezpečnosti
[9] CSIRT.SK REPORT 2016.
[10] Zákon č 69/2018 Z. z. o kybernetickej bezpečnosti

- register prevádzkovateľov základných služieb,
- zoznam digitálnych služieb,
- register poskytovateľov digitálnych služieb,
- register kybernetických bezpečnostných incidentov,
- zoznam akreditovaných jednotiek CSIRT,
- metodiky, usmernenia, štandardy, politiky a oznamy,
- informácie a údaje potrebné na používanie JISKB,
- výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu.

Nahlasovanie bezpečnostných incidentov na Slovensku

Nahlasovanie bezpečnostných incidentov a zraniteľností je možné realizovať zaslaním emailu, pričom inštrukcie na nahlásenie incidentu a zraniteľnosti sú zverejnené na stránke CSIRT.SK (Obrázok 3). Sekcia pre registrovaných používateľov je určená **zamestnancom verejnej správy SR a organizáciám patriacim do kritickej infraštruktúry**, pričom registrácia je schvaľovaná administrátorom.



Obrázok 3 Webové sídlo Národnej jednotky CSIRT.SK
s možnosťou nahlásenia incidentu alebo zraniteľnosti

Na stránke CSIRT.SK je sekcia Informačná bezpečnosť, časť Oznámenia a varovania, v ktorej sú chronologicky uverejňované bezpečnostné oznámenia a varovania, napr. zraniteľnosti, útoky, rôzne phishingové vlny, zneužívania a podobné informácie súvisiace s kybernetickými hrozbami.

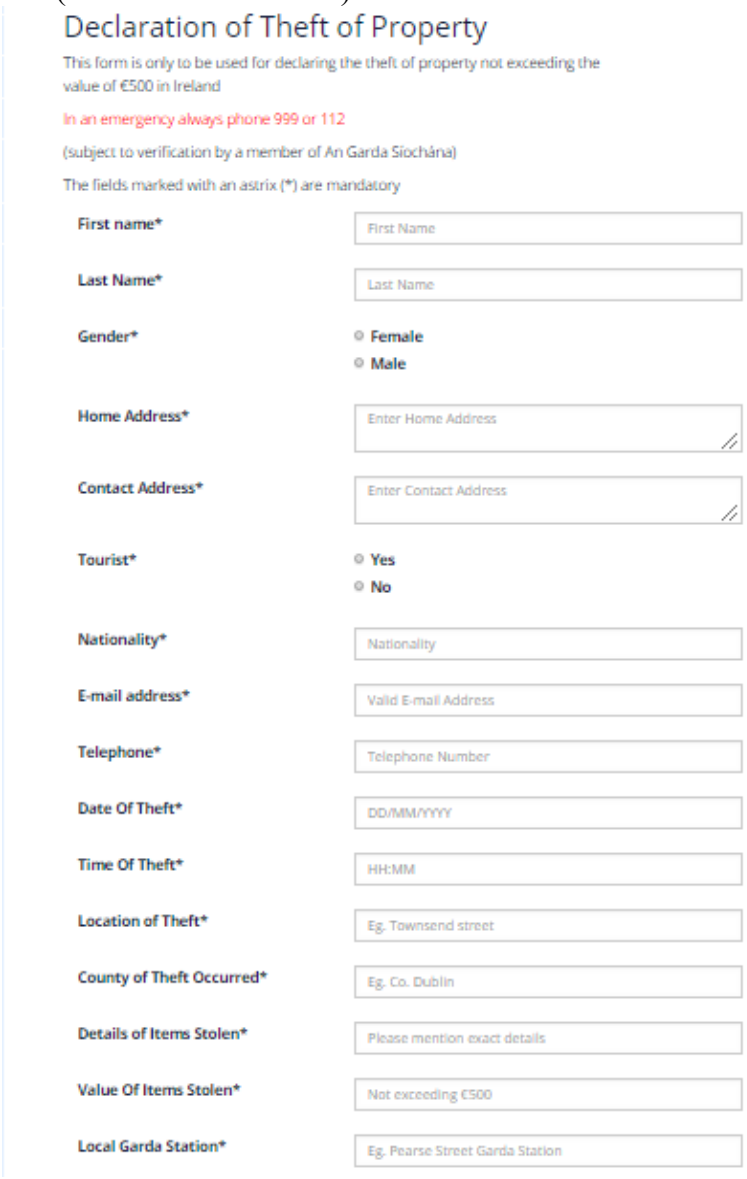
Nahlasovanie incidentov a zraniteľností vo vybraných krajinách Európskej Únie

V **Írsku** môžu obete krádeží majetku do 500 € nahlásiť tieto trestné činy Írskej národnej polícii a bezpečnostnej službe An Garda Síochána formou online formulára (Obrázok 4). Formulár je potrebné vyplniť len v prípade, ak daný trestný čin už nebol predtým nahlásený osobne, a ak nejde o[11]:

- vlámanie alebo pokus o vlámanie do domu alebo podnikateľského subjektu,
- krádež alebo pokus o krádež Vášho motorového vozidla,
- krádež majetku s použitím sily alebo hrozby použitia sily,
- akýkoľvek typ násilnej kriminality,
- krádež strelnej zbrane.

[11] Declaration of Theft of Property. Írsko: An Garda Síochána, 2018.

Pre správne vyplnenie online formulára je nevyhnutné správne uviesť kontaktné telefónne číslo a čas dostupnosti na tomto čísle. Následne je osoba, ktorá nahlásila trestný čin online kontaktovaná národnou políciou. Pri vypĺňaní formulára je nevyhnutné poskytnúť kompletné informácie o skutku. Poskytnutie nedostatočných informácií totiž môže predĺžiť čas vyšetrovania a objasnenia krádeže majetku. Po vyplnení formulára je možné tento formulár vytlačiť a následne odoslať. Pomocou tohto formulára je možné nahlásiť len krádeže majetku, ktoré sa stali v Írsku (nie v Severnom Írsku).



Declaration of Theft of Property

This form is only to be used for declaring the theft of property not exceeding the value of €500 in Ireland

In an emergency always phone 999 or 112

(subject to verification by a member of An Garda Síochána)

The fields marked with an astrix (*) are mandatory

First name* — First Name

Last Name* — Last Name

Gender* — Female / Male

Home Address* — Enter Home Address

Contact Address* — Enter Contact Address

Tourist* — Yes / No

Nationality* — Nationality

E-mail address* — Valid E-mail Address

Telephone* — Telephone Number

Date Of Theft* — DD/MM/YYYY

Time Of Theft* — HH:MM

Location of Theft* — Eg. Townsend street

County of Theft Occurred* — Eg. Co. Dublin

Details of Items Stolen* — Please mention exact details

Value Of Items Stolen* — Not exceeding €500

Local Garda Station* — Eg. Pearse Street Garda Station

Obrázok 4 Online formulár pre nahlásenie krádeže majetku v Írsku

Vo **Francúzsku** využívajú podobný systém nahlasovania kriminality ako v Írsku. Online platforma je však špecializované pre nahlasovanie kriminality páchanej cez internet (obrázok 5). Prostredníctvom online formulára je možné nahlasovať nasledujúce kybernetické bezpečnostné incidenty[12]:

- Pedofília alebo malá korupcia na internete,

[12] Portail officiel de signalement des contenus illicites de l'Internet. Francúzsko: Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, 2018.

- Podnecovanie k rasovej nenávisti alebo podnecovanie k diskriminácii osôb z dôvodu ich pôvodu, pohlavia, sexuálnej orientácie alebo zdravotného postihnutia,
- hrozby násilia alebo podnecovanie k násiliu,
- ilegálna preprava vecí (narkotiká, zbrane atď.),
- ohrozenie ľudí,
- podnecovanie k spáchaniu trestných činov,
- spam,
- ohováranie,
- podvod.

Online formulár nie je vhodné používať, ak je občan svedkom alebo obeťou udalostí, vyžadujúcich okamžité policajné alebo záchranné služby ako sú napríklad agresia, nehoda, požiar a pod. V tomto prípade je nevyhnutné okamžite kontaktovať policajné alebo záchranné služby telefonátom na ich známe telefónne číslo 112.

Obrázok 5 Online formulár pre nahlásenie kybernetickej kriminality vo Francúzsku

Jeden z najprepracovanejších systémov nahlasovania kriminality online používa **Spojené kráľovstvo Veľkej Británie a Severného Írska.** Ak došlo k spáchaniu podvodu, obeť môže zavolať „Action Fraud" – britské národné centrum pre ohlasovanie podvov. Podvod je možné centru nahlásiť, ak bol spáchaný na území Veľkej Británie alebo v prípade, že je spojený s Veľkou Britániou a bol uskutočnený on-line. Online platforma umožňuje ohlasovateľovi vybrať si z dvoch druhov hrozieb – nahlásenie podvodu a kybernetickej kriminality a nahlásenie phishingového útoku.

V prípade ak dochádza k priamemu počítačovému útoku v reálnom čase, je nevyhnutné okamžite nahlásiť tento útok na telefónne číslo 0300 123 2040. Táto služba je k dispozícii 24

hodín denne, 7 dní v týždni. V prípade ak útok neprebieha v reálnom čase, je možné skutok, ktorý sa stal nahlásiť pomocou online formulára v závislosti od typu hrozby[13]:

- Krádež vozidla,
- Podozrivé online správanie s dieťaťom alebo smerom k dieťaťu,
- Online zločiny z nenávisti alebo šikanovania,
- Falšované lieky alebo zdravotnícke pomôcky, ktoré sú k dispozícii na nákup online,
- Daňový podvod,
- Výhody z podvodu,
- Imigračný podvod,
- Falšovaná mena.

Online formulár na podávanie informácií o podvodoch (Obrázok 6) obsahuje sériu otázok týkajúcich sa incidentu, ktorý je oznamovaný, vrátane otázok týkajúcich sa podozrivého. Vyplnenie formulára trvá približne 20 až 30 minút. Po spustení vypĺňania musí ohlasovateľ incidentu vyplniť formulár naraz. Z toho dôvodu je nevyhnutné pred začatím vypĺňania sa uistiť, že ohlasovateľ má k dispozícii všetky relevantné informácie (napr. mená, dátumy, informácie o podozrivých a pod.). Zatiaľ čo nahlasovanie bezpečnostných incidentov prostredníctvom telefónneho čísla je anonymné, pri nahlasovaní týchto incidentov online nie je možné pre ohlasovateľa zaistiť anonymitu.

Obrázok 6 Online formulár pre nahlásenie kybernetickej kriminality v Spojenom kráľovstve Veľkej Británie a Severného Írska

Nahlasovanie phishingových pokusov o útok prebieha taktiež vo forme vypĺňania online formulára. Ten je potrebné vyplniť len v prípade ak ešte nedošlo k strate finančných prostriedkov alebo osobných údajov. V prípade, že k takýmto stratám už došlo, je nevyhnutné tento bezpečnostný incident nahlásiť ako trestný čin.

Nemecké federálne polície, ale aj štátna polícia vypracovali príručku pre podniky pre nahlasovanie ekonomickej kybernetickej kriminality. Súčasné zistenia polície a prieskumy

[13] ActionFraud. Spojené kráľovstvo: National Fraud & Cyber Crime Reporting Centre, 2018.

ukazujú, že nemecká ekonomika - malá, stredná a dokonca veľká - vo všetkých podnikateľských sektoroch je značne postihnutá kybernetickou kriminalitou v najrôznejších formách. Situácia sa v posledných rokoch zhoršila, pretože charakter útokov sa stal zložitejším a rôznorodejším. Firemné a zákaznícke údaje sa v mnohých prípadoch nezákonne používajú na spáchanie rôznych iných trestných činov. Činnosť podnikov môže byť ovplyvnená útokmi na systémy ich informačných technológií bez toho, aby ich podnik bol schopný rozpoznať. Včasné a správne vyhodnotenie týchto indikácií napadnutia systému je nevyhnutné na iniciovanie cielených obranných opatrení[14].

Útoky môžu byť spáchané interne alebo externe a často si vyžadujú širokú škálu rozhodnutí manažérov podnikov vo veľmi krátkom čase. Preto je dôležité pre bezpečnostných pracovníkov firiem oboznámiť sa s možnými scenármi hrozieb v ranom štádiu, poznať potrebné možnosti ochrany a prijať opatrenia. Technické bezpečnostné prostriedky sú len jednou zo súčastí komplexného bezpečnostného konceptu. Správcovia systému zohrávajú dôležitú úlohu v tomto bezpečnostnom procese.

Záver

Internet má byť miestom slobody, a preto na ňom musia byť rešpektované práva a povinnosti. Internet sa nesmie stať nebezpečným miestom, v ktorom sú užívatelia vystavení hrozbám. Keďže rozvoj technológií umožňuje aj vznik nových typov hrozieb, je nevyhnutné aby jednotlivé krajiny prijímali také opatrenia, aby sa internet stal bezpečnejším miestom. Z tohto dôvodu sa krajiny zameriavajú na vytváranie rôznych platforiem, umožňujúcim online nahlasovanie kriminality so dôrazom na kybernetickú kriminalitu.

S cieľom predchádzania kybernetickej kriminality a na ochranu kybernetického priestoru bol na Slovenku len nedávno prijatý nový Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Ten ustanovuje základné východiská prevencie kybernetických incidentov a vytvára základ právneho rámca pre požiadavky na informačné systémy. Za ústredný orgán štátnej správy pre kybernetickú bezpečnosť je na Slovensku možné považovať Národný bezpečnostný úrad, ktorý prevádzkuje útvar Slovak Computer Emergency Response Team (SK-CERT). Na Slovensku je možné nahlásiť bezpečnostné incidenty prostredníctvom zaslania emailu. Inštrukcie na nahlásenie incidentu sú zverejnené na stránke CSIRT.SK.

V zahraničí sú využívané predovšetkým online platformy pre nahlasovanie kriminality páchanej v kybernetickom priestore. Za najprepracovanejší systém je možné považovať systém Spojeného kráľovstva, ktorý umožňuje prostredníctvom online formulára nahlásiť rôzne druhy kybernetickej kriminality. V prípade, že obeť podvodu chce zostať v anonymite, je možné využiť aj telefónne číslo, ktorá je k dispozícii 24 hodín denne 7 dní v týždni.

Internet je miesto, ktoré na rozdiel od jednotlivých krajín nepozná hranice. Z hľadiska budúceho vývoja spoločnosti je možné očakávať vznik nových sofistikovanejších hrozieb vyplývajúcich z technologického pokroku. Z toho dôvodu je nevyhnutné aby štáty svoje jednotlivé národné systémy pre nahlasovanie kybernetických bezpečnostných incidentov prepájali a vytvárali ucelenú sieť. Jedným z riešení môže byť aj vytvorenie jednotky Európskej únie pre boj s kybernetickou kriminalitou, ktorá by okrem iného riešila kybernetickú kriminalitu na medzinárodnej úrovni.

Zoznam použitej literatúry:

ActionFraud. Spojené kráľovstvo: *National Fraud & Cyber Crime Reporting Centre,* 2018. Dostupné na: https://www.actionfraud.police.uk/

Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020. Bratislava: Národný bezpečnostný úrad, 2016. Dostupné na: http://www.nbusr.sk/wp-

[14] Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft. Nemecko: Offizielles Portal der deutschen Polizei, 2018.

content/uploads/kyberneticka-bezpecnost/Akcny-plan-realizacie-Koncepcie-kybernetickej-bezpecnosti-SR-na-roky-2015-2020.pdf
CSIRT.SK REPORT 2016. Bratislava: CSIRT.SK, 2017. Dostupné na: https://www.csirt.gov.sk/doc/CSIRT-SK-Report-2016.pdf
Declaration of Theft of Property. Írsko: An Garda Síochána, 2018. Dostupné na: https://www.garda.ie/en/About-Us/Online-Services/Theft-Declaration/
Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020. Bratislava: Národný bezpečnostný úrad, 2015. Dostupné na: http://www.nbusr.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf
Portail officiel de signalement des contenus illicites de l'Internet. Francúzsko: Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, 2018. Dostupné na:
https://www.internetsignalement.gouv.fr/PortailWeb/planets/Accueil!input.action
Služby SK-CERT. Bratislava: Národný bezpečnostný úrad, 2018. Dostupné na: https://www.sk-cert.sk/sk/sluzby/index.html
Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
ŠOLTÉS, V., MIŠÍK, J., KUBÁS, J., ŠTOFKOVÁ, Z. Education in information security. In *INTED 2016 :* proceedings. Valencia, Spain: IATED Academy, 2016. s. 4418-4424. ISBN 978-84-608-5617-7.
Zákon č 69/2018 Z. z. o kybernetickej bezpečnosti
Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft. Nemecko: Offizielles Portal der deutschen Polizei, 2018. Dostupné na: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Kontaktné údaje:
Ing. Viktor Šoltés, PhD.
Katedra bezpečnostného manažmentu
Fakulta bezpečnostného inžinierstva
Žilinská univerzita v Žiline
Viktor.Soltes@fbi.uniza.sk

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

Informační bezpečnost a její aplikace v praxi

Vladimír Šulc

Abstrakt:
Ve společnosti jsou změny související s „digitalizací společnosti“. Narůstá vliv virtuálního světa na chod společnosti. Dříve se tvrdilo, že narůstá vliv sociálních sítí na uvažování a jednání lidí, to dnes neplatí, dnes lidé na sociálních sítích přímo žijí. Většina bankovních transakcí je prováděna přes aplikace internetového bankovnictví, do kamenné banky není třeba téměř chodit. Vážně se uvažuje o zrušení hotovostních peněz, vždyť převody peněz lze přece levněji a rychleji realizovat bezhotovostně a tisk a správa hotovostních peněz je drahá.
Klíčová slova:
Bezpečnost, digitalizace, skutková podstata trestného činu, sociální sítě, trestné činy.

Abstract:
There are sharp changes in society related to "digitization of the company". The influence of the virtual world is on the rise of the company. Previously, for example, it was argued that the impact of social networks on young people's thinking and behavior is no longer the case nowadays young people live on social networks today. Most banking transactions are done through Internet banking applications, and there is no need to go to the bank anywhere.
Key words:
Security, digitization, crime, social networks, crimes.

Úvod

Vážně se uvažuje o zrušení hotovostních peněz, vždyť převody peněz lze přece levněji a rychleji realizovat bezhotovostně a tisk a správa hotovostních peněz je drahá. Rozvíjí se propojení úřadů s občany, jednou z vizí je i to, aby občané na úřad nemuseli chodit a veškerou komunikaci s úřady si mohli zařídit na internetu. Uvažuje se dokonce i o volebním hlasování přes internet. Jsou však počítačové systémy obyvatel dostatečně chráněny a zabezpečeny proti kybernetickým útokům zvenčí natolik, aby skrze ně mohli lidé bezpečně virtuálně žít? Mají tito uživatelé alespoň základní povědomí o kybernetické ochraně svých dat, svých osobních údajů a hesel? Vědí, jak se bezpečně chovat při používání internetového bankovnictví? I to jsou některé otázky, na nichž se budu snažit ve svém příspěvku nalézt odpověď. Vzhledem k omezenému rozsahu tohoto příspěvku jsem se rozhodl popsat pouze dva nejdůležitější a nejčastější trestné činy v oblasti kybernetické kriminality. Tyto dva trestné činy jsem považoval za vhodné uvést, protože velmi souvisí se základními druhy kybernetické kriminality. Popis všech trestných činů, které by mohly spadat do oblasti kybernetické kriminality, by zabral minimálně jednu samostatnou kapitolu.

Druhy trestných činů

A) Trestný čin neoprávněný přístup k počítačovému systému a nosiči informací jako základní trestný čin v oblasti kybernetické kriminality.

Trestný čin neoprávněný přístup k počítačovému systému a nosiči informací patří v oblasti kybernetické kriminality mezi opravdu nejdůležitější trestné činy.

Individuálním objektem je u tohoto trestného činu ochrana počítačového systému, nosiče informací a zabránění jeho zneužití, dále ochrana dat uložených v počítačovém systému nebo na nosiči informací. Pojem počítačový systém je tvořen nejen hardware, (jeho jednotlivými komponenty, na nichž jsou uložena data, informace a software), ale i systémy propojující software, hardware a zajišťujícími komunikaci mezi počítačovým systémem a uživatelem. Počítačový systém se obvykle sestává z různých zařízení označovaných jako základní zpracovávací jednotka a periferní zařízení. Periferní zařízení plní určité specifické funkce v interakci se základní jednotkou. Takovými periferními zařízeními jsou např. tiskárna,

monitor, CD nebo DVD čtecí/zapisovací zařízení nebo jiná paměťová zařízení.[1] Nosičem informací se „*rozumí jakýkoli nosič dat v informační technice, tedy materiál, do kterého nebo na který lze zaznamenávat („zapsat“) data a z kterého lze data zpět získat („přečíst“)*“[2] Zákonodárce zde má na mysli jakýkoliv interní i externí magnetický pevný disk, jakoukoliv diskovou případně disketovou mechaniku, elektrickou paměť počítače, USB disk, případně jiné nosiče schopné plnit funkce shora definované (mobilní telefon s pamětí, chytré hodinky, diáře).

Objektivní stránka trestného činu, tedy zejména po stránce jednání je pak popsána v samotných skutkových podstatách trestného činu. V první základní skutkové podstatě trestného činu[3] pachatel překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo jeho části. Bezpečnostním opatřením „*je třeba rozumět každé opatření, jehož cílem je zabránit volnému přístupu k počítačovému systému nebo nosiči informací (např. heslo nebo použití firewallu). Na stupni, míře zabezpečení nezáleží. Úroveň zabezpečení nelze považovat za rozhodující, postačí, že pachatel musí překonat nějakou překážku. Existence jakéhokoli zabezpečení totiž na jedné straně jasně signalizuje, že si uživatel nepřeje, aby někdo nepovolaný do systému vstupoval, na druhé straně musí pachatel vyvinout zvýšené úsilí, aby do systému vstoupil*.“[4]

V druhé základní SPTČ pachatel získá přístup k počítačovému systému nebo k nosiči informací a data neoprávněně užije, zničí, poškodí, pozmění, padělá nebo data do počítačového systému či na nosič informací neoprávněně vloží či učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického vybavení. U kvalifikovaných skutkových podstat uvedených v odstavcích tři, čtyři a pět nastupují ještě další jiné skutečnosti a těžší následky, vždy však musí být jednáním pachatele zasažen některý individuální objekt popsaný výše.

Subjekt je zde obecný, zákonodárce nevyžaduje od subjektu tohoto trestného činu nějaké speciální vlastnosti nebo dovednosti. Z hlediska subjektivní stránky zákonodárce u základní skutkové podstaty uvedené v prvním a druhém odstavci striktně vyžaduje úmyslné zavinění.

K naplnění ustanovení odstavce 1 je třeba překonání bezpečnostního opatření, je tedy třeba se do počítače například za pomocí prolamovače hesel nejprve dostat. Překonání bezpečnostního opatření však může být i obecnější povahy, například využitím znalostí vylákaných přístupových údajů.

Ustanovení odstavce 2 je oproti odstavci 1 neobsahuje povinnost překonání bezpečnostní překážky. Ustanovení pokrývá neoprávněné jednání toho, kdo přístup k počítačovému systému ať již oprávněně, nebo neoprávněně má a není mu tedy třeba jakékoliv bezpečnostní opatření překonávat. Ustanovení ošetřuje například neoprávněné jednání zaměstnanců bank s osobními a obchodními údaji o klientech banky uložených v počítačovém systému banky, jednání mstivého zaměstnance mazajícího informace o klientech společnosti, jednání zaměstnance kopírujícího si data z počítačového systému společnosti pro své další podnikání a tak dále.

Ustanovení odstavců 3, 4 a 5 jsou kvalifikovanými skutkovými podstatami k odstavcům 1 a 2. Ošetřují větší výši způsobené škody, nebo získání pachatelova většího prospěchu. Ošetřují

[1] ŠÁMAL, P. a kol. *Trestní zákoník*. 1. Vydání. Praha: C.H.Beck, 2009. ISBN 978-80-7400-109-3, str. 2088.
[2] ŠÁMAL, P. a kol. *Trestní zákoník*. 1. Vydání. Praha: C.H.Beck, 2009. ISBN 978-80-7400-109-3, str. 2088.
[3] Dále jen SPTČ.
[4] ŠÁMAL, P. a kol. *Trestní zákoník*. 1. Vydání. Praha: C.H.Beck, 2009. ISBN 978-80-7400-109-3, str. 2088.

pachatelův úmysl ohrozit funkčnost celého počítačového systému, dále úmysl způsobit poruchu činnosti státní správy a tak dále.

B) Trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 trestního zákoníku.

Trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi patří k nejdůležitějším a nejčetnějším trestných činů z hlediska kybernetické kriminality. Kriminalizuje zejména počítačové pirátství. Z hlediska závažnosti je minimálně stejně závažný jako trestný čin neoprávněný přístup k počítačovému systému. Počítačové sítě umožňují prakticky neomezené neoprávněné zveřejňování, stahování, sdílení a nabízení autorsky chráněných děl, tedy hudby, filmů a počítačových programů. Na internet jsou tak mnohdy i běžnými uživateli umísťována díla ke stažení jiným uživatelům, běžní uživatelé si díla prostřednictvím P2P sítí a k tomu vytvořených programů sami stahují a zároveň je mnohdy nevědomky nabízejí jiným ke stažení.

Individuálním objektem u základní SPTČ uvedené v prvním odstavci je ochrana zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukově nebo zvukově obrazovému záznamu a rozhlasového nebo televizního vysílání. Objektivní stránka zahrnuje pachatelův neoprávněný zásah do výše popsaných statků. Tento zásah však musí být vyšší než nepatrný, proto zde při právní kvalifikaci skutku musí policejní orgán zejména přihlédnout k rozsahu pachatelova zásahu, době jeho trvání a jeho intenzitě.[5]

Subjekt je zde obecný, zákonodárce od pachatele nevyžaduje žádné speciální dovednosti či postavení. Z hlediska subjektivní stránky zákonodárce v prvním odstavci striktně vyžaduje úmyslné zavinění. U kvalifikovaných skutkových podstat pak dostačuje, je-li těžší následek, i pouhé nedbalostní zavinění.

Odstavec 1 je jedinou základní skutkovou podstatou tohoto trestného činu, odstavce 2 a 3 tvoří skutkové podstaty kvalifikované, které mají vesměs doplňující a upřesňující charakter. „*Ustanovení § 270 trestního zákoníku je normou s blanketní dispozicí, která obsahuje na předpisy o právu autorském.“*[6] Definice pojmů jako autorské dílo, umělecký výkon, atd. je tedy třeba hledat zejména v ustanovení § 2 autorského zákona.[7] V autorském zákoně jsou také v § 2 až 66 definovány veškeré základní pojmy jako rozmnožování, půjčování, autor, zveřejnění a vydání díla, právo dílo užít, pronájem, půjčování a jiné základní pojmy.

Autorský zákon dále v hlavě šesté obsahuje popis přestupků a správních deliktů právnických a podnikajících fyzických osob. Je na orgánech činných v trestním řízení posoudit, zdali intenzita porušení zájmu chráněného trestním zákonem byla jednáním pachatele natolik dostatečná, že se již jedná o trestný čin a nikoliv pouze o přestupek nebo správní delikt. Odevzdání věci příslušnému orgánu k projednání přestupku nebo jiného správního deliktu dle ustanovení § 159a odst. 1 písm. a) trestního řádu bývá policejním orgánem často užíváno u nejednoznačných a malicherných případů.

---

[5] NOVOTNÝ, F. a kol. *Trestní zákoník 2010*. Komentář. 1. vydání. Praha: Eurounion, 2010. ISBN 978-80-7317-084-4. str. 522.

[6] NOVOTNÝ, F. a kol. *Trestní zákoník 2010*. Komentář. 1. vydání. Praha: Eurounion, 2010. ISBN 978-80-7317-084-4. str. 522.

[7] Zákon 121/2000 Sb. ze dne 7. dubna 2000, o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Základy zabezpečení domácího počítače před kybernetickými útoky

Stejně jako si chráníme své domovy pomocí dveří a zámků, je nutné chránit i svůj počítač a data v něm uložená. Podcenit zabezpečení počítače může vést ke ztrátě citlivých dat, rodinných fotografií, ztrátě přihlašovacích jmen a hesel a jejich následné nožné zneužití útočníkem k nedovolenému obohacení nebo k páchání trestné činnosti vaším jménem.

Je třeba si povšimnou i toho, k čemu všemu může být rodinný počítač využíván. Většinou to totiž není jenom prohlížeč internetu. Na rodinném počítači používáme internetové bankovnictví, máme na něm oskenované zdravotní zprávy od lékaře, smlouvy s citlivými údaji, pojistky, sbírku rodinných fotografií, mnohdy i program s firemním účetnictvím a s dálkovým přístupem do firmy a jiné. Kolik však rodinných financí investujeme do vlastního zabezpečení stroje s takto důvěrnými informacemi o našem životě? Mnohdy naprosté minimum nebo vůbec nic.

Věřím, že každý uživatel počítače svá data nějakým způsobem zabezpečuje. Prakticky však svůj počítač a data na něm uložená ochráníme dvojím způsobem. První způsob zahrnuje bezpečné nastavení počítače (pravidelné aktualizace, antivirový program, firewall,…). Druhý způsob zahrnuje bezpečné uživatelovo chování při práci s počítačem. V následujících dvou podkapitolách si o tom povíme více.

Bezpečné nastavení počítače

Bezpečné nastavení počítače zahrnuje více důležitých prvků. V první řadě je doporučováno používat nejnovější a plně aktualizovanou verzi operačního systému počítače. V současné době je nejnovějším operačním systémem společnosti Microsoft operační systém Windows 10. Prakticky se doporučuje **mít neustále zapnuté automatické aktualizace systému** a tyto aktualizace automaticky stahovat a následně automaticky instalovat. Laikům se nedoporučuje si vybírat aktualizace a některé neinstalovat. Raději nainstalovat veškeré. Operační systém dle námi nainstalovaných programů na počítači vybírá vhodné aktualizace, čím tedy méně zbytečných programů máme na počítači nainstalovaných, tím budou aktualizace rychlejší. Aktualizace operačního systému totiž řeší mimo jiné bezpečnostní chyby (trhliny) v systému a „záplatuje je“. Útočník do neaktualizovaného počítače tedy poměrně snadno pronikne, pokud danou bezpečnostní chybu zná.

Na co se již poněkud zapomíná, je **pravidelné aktualizování ostatních programů** nainstalovaných na počítači. Zejména je nutno se zaměřit na internetový prohlížeč a jeho doplňky. Obecně se i doporučuje míti ve svém internetovém prohlížeči nainstalováno co nejméně těchto doplňků, a to právě pro jejich zranitelnost. Na neaktuálnost nainstalovaných programů Vás přitom upozorní některé placené programy, které já osobně považuji za zbytečné, nebo kvalitní antivirový program, který například při probíhajících testech počítače kontroluje i aktuálnost a zranitelnost nainstalovaných programů.

Nainstalovaný, aktuální a automaticky **aktualizovaný antivirový program** považuji téměř za nezbytnost. Bez „antiviru“ je totiž počítač opravdu zranitelný proti útokům zvenčí. Kvalitní antivirový program nás dále například upozorní například i při navštívení rizikové stránky na internetu, kontroluje tedy i například naše procházení internetu, kontroluje, kam jsme prohlížečem přesměrováváni a tak dále. Antivirový systém je dnes již součástí operačního systému Windows 10. Tento základní antivirový program od společnosti Microsoft však není považován za nejlepší a v testech antivirových programů se neumísťuje na prvních příčkách. Zákazník dále může volit, zdali si nainstaluje jiný antivirový program zdarma, nebo jeho placenou verzi. Placená verze přitom zpravidla nabízí prvky pokročilejší ochrany, a to například při používání internetového bankovnictví. Jako jeden z nejlepších antivirových programů je

doporučován antivirový program společnosti ESET software spol. s r. o., program ESET NOD32 Antivirus. Tento program v rámci zakoupené licence využívá i PČR. Naopak se nedoporučuje mít nainstalováno více antivirových programů současně, docházelo by totiž k výraznému zpomalení počítače.

Firewall je program, který kontroluje všechny síťové komunikace a brání útočníkům v přístupu na počítač. Základní firewall je již součástí operačního systému Windows 10, podobně jako u antivirového programu je však doporučováno mít na počítači nainstalován lepší. Kvalitnější firewally bývají součástí většinou placených verzí antivirových programů. Firewall musí být v nastavení operačního systému počítače vždy zapnut.

Správné nastavení uživatelských účtů a hesel je běžnými uživateli často opomíjeno. Každý uživatel počítače by měl mít vytvořen vlastní účet, v němž má své osobní nastavení, nainstalované programy a svá data. Při nastavení uživatelských účtů a hesel je pak dobré dodržovat tyto zásady:

- každý uživatel počítače má svůj vlastní účet zabezpečený dostatečně silným heslem,
- heslo k danému uživatelskému účtu není jednoduše dostupné, např. nalepené na počítači nebo nástěnce,
- heslo k uživatelskému účtu jednotliví uživatelé, nemají-li k tomu důvod, nesdílejí,
- pro běžnou práci s počítačem je dobré pracovat jako standardní uživatel, nikoli jako administrátor.

Mnoho počítačů se k síti internet připojuje pomocí bezdrátové sítě. Domácí bezdrátová síť přináší mnoho výhod, lze ji snadno zřídit a lze k ní připojit i například chytré domácí spotřebiče (televize, ovládání vytápění,…). **Je však důležité bezdrátovou síť správně zabezpečit**, jinak kdokoli může přistupovat ke všem síťovým prostředkům a přenášeným datům, a to včetně citlivých dat. Nedovolte cizím lidem využívat vaši bezdrátovou síť. Připojení k bezdrátové síti by mělo být samozřejmě chráněno kvalitním (složitým) heslem.

Bezpečné chování uživatele

V oblasti IT odborníků probíhají diskuse, jak by se měl uživatel na internetu bezpečně chovat, aby si nenakazil počítač nebo aby nepřišel o svá soukromá data. Základní normy bezpečného chování na internetu jsou přitom docela logické a jednoduché. Často souvisí i s tím, co chceme s počítačem na internetu dělat, k čemu nám počítač slouží.

Za **rizikové chování na internetu** lze považovat například navštěvování různých zahraničních porno stránek, které uživatele neustále někam přesměrovávají, využívání zahraničních erotických a flirt seznamek, stahování a instalování „kreknutých“ programů, stahování souborů s přidaným obsahem (s filmem si stáhneme i vir) a tak dále. I toto chování by snad nebylo problematické, pokud bychom na toto rizikové chování měli zvláště určený počítač, který by nesloužil k ničemu jinému. Ne, já opravdu nejsem moralista a kdo se nikdy na internetu nepodíval na nějaké pornografické dílo, tak se zřejmě dívá doteď. Provádět však výše popsanou rizikovou činnost na počítači, na kterém zároveň používám internetové bankovnictví a spravuji firemní účetnictví, považuji za poněkud sebevražedné.

Ochrana hesel a přihlašovacích údajů spočívá zejména v tom, že tato hesla a přihlašovací údaje zadávám jenom tam, kde si jsem jistý, že patří. Pokud například tyto přihlašovací údaje zadám do nějakého „vyskakovacího okna“, mohu si být jist, že je něco špatně. Hesla by měla být dostatečně silná a měla by být měněna v pravidelných intervalech.

Neměl bych používat stejná hesla k různým účtům. Obecně se nedoporučuje mít na svém počítači nastaveno automatické vyplňování hesel.

K **důležitým účtům a k internetovému bankovnictví** je lepší se připojovat pouze ze zabezpečeného počítače, který není zároveň využíván rizikově. Chytré mobilní telefony s operačním systémem Android jsou velice rizikové. Pokud chci přesto ovládat internetové bankovnictví pomocí mobilního telefonu, stáhnu si a nainstaluji si pro toto speciální mobilní aplikaci dané banky, tato je více zabezpečená.

Je dobré počítač pravidelně **kontrolovat pomocí antivirového programu**. Jako nejlepší a zdarma doporučuji ESET online scanner. Tento program je volně dostupný z: https://www.eset.com/cz/online-scanner/. Jedná se o nejkvalitnější jednorázové zkontrolování počítače. Při této kontrole doporučuji mít vypnutý stávající antivirový program. Kontrolu doporučuji provádět minimálně každé 3 měsíce, nebo po každém rizikovém chování a restartu počítače.

Bezpečné placení na internetu by vydalo na samostatnou kapitolu. Je ovšem otázkou, zdali bezpečné placení na internetu může vůbec být, zdali je možné. Čísla platebních karet pro placení je třeba zadávat pouze na serverech, kterým důvěřuji. Pokud jsem někam přesměrován, nikdy čísla karet nezadávám. Pro placení na internetu je lepší použít kreditní kartu (jedná se o peníze banky), nikoliv kartu debetní (moje peníze na mém účtu). Pro placení na internetu je dobré mít v bance nastaven bezpečný měsíční limit. Otázkou zůstává zvážení pojištění platebních karet pro jejich neoprávněné použití třetí stranou (útočníkem).

Zálohování citlivých dat, rodinných fotografií, naskenovaných dokumentů, smluv, je taktéž doporučováno. Dnešní doba nabízí možnost využití cloudových úložišť, tedy že data budou ukládána na server na internetu (Dropbox, Microsoft One drive, Google disk,…). Nastavení ukládání dat (zálohování) lze i automaticky. Osobně využívám dvojí zálohování dat, jedno automaticky na cloudové úložiště a druhé na externí pevný USB disk. Při využití zálohování nám po napadení počítače hackerem a jeho provedeným zašifrování dat, nehrozí ztráta důležitých dat na něm uložených, přinejhorším přijdeme pouze o data neuložená v posledním období.

Otevírání příloh doručené emailové pošty, kde neznáme odesílatele, nebo která se nám zdá jinak podivná, se nedoporučuje. Právě touto cestou se mohou na náš počítač dostat nechtěné programy (viry). Toto je ještě důležitější, pokud si poštu například pomocí emailového klienta do počítače rovnou stahujeme. Zde se doporučuje podezřelé zprávy ihned mazat a jejich přílohy vůbec neotevírat (nespouštět).

Bezpečné užívání virtuálních měn, virtuálních peněženek, klíčů k virtuálním peněženkám by také vydalo na samostatnou kapitolu. Tato problematika by se však měla týkat pouze pokročilých uživatelů, začátečník by se do tohoto vůbec neměl pouštět. Zde by měl uživatel uplatňovat prvky pokročilejší ochrany, kterými se však tato práce nezabývá (pokročilé šifrování dat, USB klíče, VPN připojení k internetu).

Závěr

Lze tedy konstatovat, že ať se bude vývoj informačních technologií ubírat jakýmkoliv směrem, je boj s počítačovou kriminalitou marný, pokud nedojde ke sjednocení právních řádů jednotlivých zemí. Internet nemá hranice a tudíž jeho omezování jen v některých státech se tak míjí účinkem. Na základě výše popsaných způsobů průniků/kybernetických útoků do informačních systémů je nutné věnovat tomuto problému velkou pozornost. Bezpečnostní

opatření v dané věci musí být naším prioritním cílem, kdy se jedná zejména o zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.

Seznam použité literatury:

CHALOUPKA, A. *Aplikace informační a kybernetické bezpečnosti.* Praha : Policejní akademie ČR v Praze, katedra bezpečnostního managementu. 2018.
NOVOTNÝ, F. a kol. *Trestní zákoník* 2010. Komentář. 1. vydání. Praha: Eurounion, 2010. ISBN 978-80-7317-084-4. str. 522.
ŠÁMAL, P. a kol. *Trestní zákoník*. 1. Vydání. Praha: C.H.Beck, 2009. ISBN 978-80-7400-109-3, str. 2088.
Zákon 121/2000 Sb. ze dne 7. dubna 2000, *o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů* (autorský zákon).

Kontaktní údaje:

Ing. Vladimír Šulc Ph.D.
Policejní akademie České republiky v Praze
Katedra bezpečnostního managementu
sulc@polac.cz

Etický hacking v organizácii v zmysle smernice o kybernetickej bezpečnosti

Peter Veselý, Vincent Karovič

Abstrakt:
Praktické využitie znalostí z oblasti etického hackingu podľa metodiky OWASP v organizácii najmä v zmysle posúdenia kybernetickej bezpečnosti, teda stavu, 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.
Kľúčové slová:
kybernetická bezpečnosť, virtualizácia, etický hacking

Abstract:
Analysis of cyber security breach models for the purpose of misuse of personal data, analysis of selected security incidents and proposal of appropriate measures to reduce the risk of these types of incidents, especially with the use of open source resources. Analysis of potential impacts on the organization in relation to the GDPR Regulation and the ePrivacy Directive.
Key words:
Personal data, cyber security, GDPR, ePrivacy

Úvod

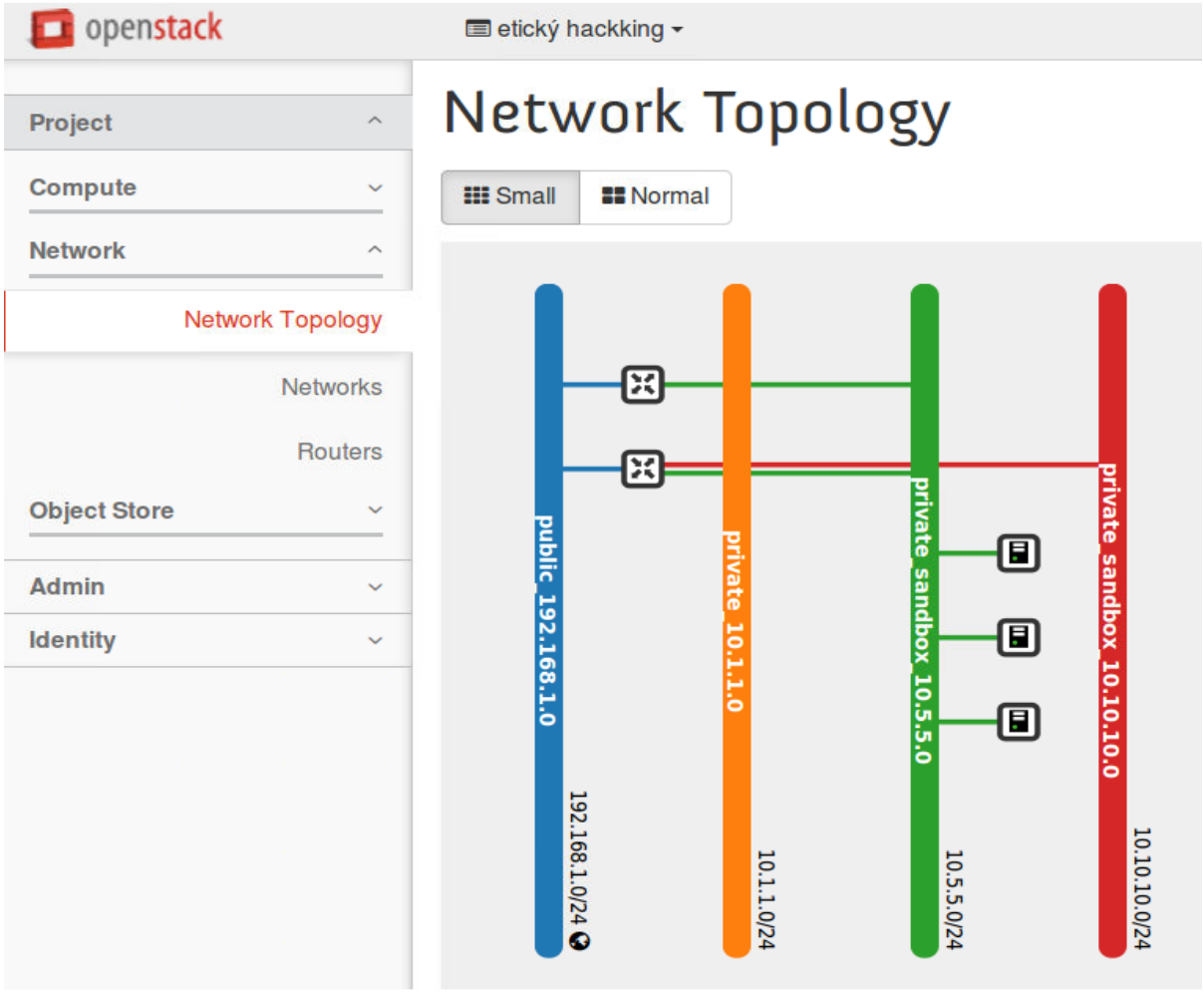
Problematika etického hackingu je momentálne v súčasnom globalizovanom svete informačných technológii popri existencii nových legislatívnych predpisoch typu CYBER SECURITY, GDPR a ePRIVACY výrazným prvkom, ktorý rozhoduje najmä o architektúre IS/ICT v podnikoch. Skoro všetky organizácie v súčasnosti spracovávajú veľmi citlivé dáta ako napr. osobné údaje, preto podľa legislatívy musia vytvoriť bezpečnostný projekt a musia sa významným spôsobom zaoberať manažmentom bezpečnosti. Praktickou stránkou testovania bezpečnosti IS/ICT v organizáciách je práve etický hacking.[1] Ide o využívanie bežne dostupných, ako aj menej dostupných techník ako sa dostať do informačných systémov, prípadne ich poškodiť. Manažér organizácie nikdy nemôže tvrdiť, že informačný systém organizácie je bezpečný, pokiaľ nie je spracovaná komplexná sada bezpečnostných testov a nie je spracované vyhodnotenie závažnosti ich výsledkov. Už dlhšiu dobu existuje medzinárodný štandard OWASP – Open Web Application Security Project,[2] ktorý definuje postupnosť krokov, ako vykonávať dané bezpečnostné testy. Vykonávanie týchto krokov v mene organizácie je však možné iba prostredníctvom špecialistu, tzv. „etický hacker“, ktorý disponuje dostatočnými znalosťami v tejto oblasti a najmä morálnymi hodnotami. Príprava špecialistov typu ethical hacker však vyžaduje nielen hlboké teoretické poznatky, ale najmä rozsiahle praktické skúsenosti v oblasti.

Nastavenie prostredia pre etického hackera

Hlavnou časťou systému pre vzdelávanie a prácu etického hackera v organizácii môže byť aj virtualizačný nástroj založený na open source softvéri OpenStack[3]. Systém virtualizácie typu Openstack je open source a zároveň spĺňa parametre pre vytvorenie bezpečného prostredia, ktoré je oddelené od okolitých technológií, tzv. sandbox a môže modelovať reálnu prevádzku informačných systémov organizácie. Daná technológia umožňuje vytvoriť

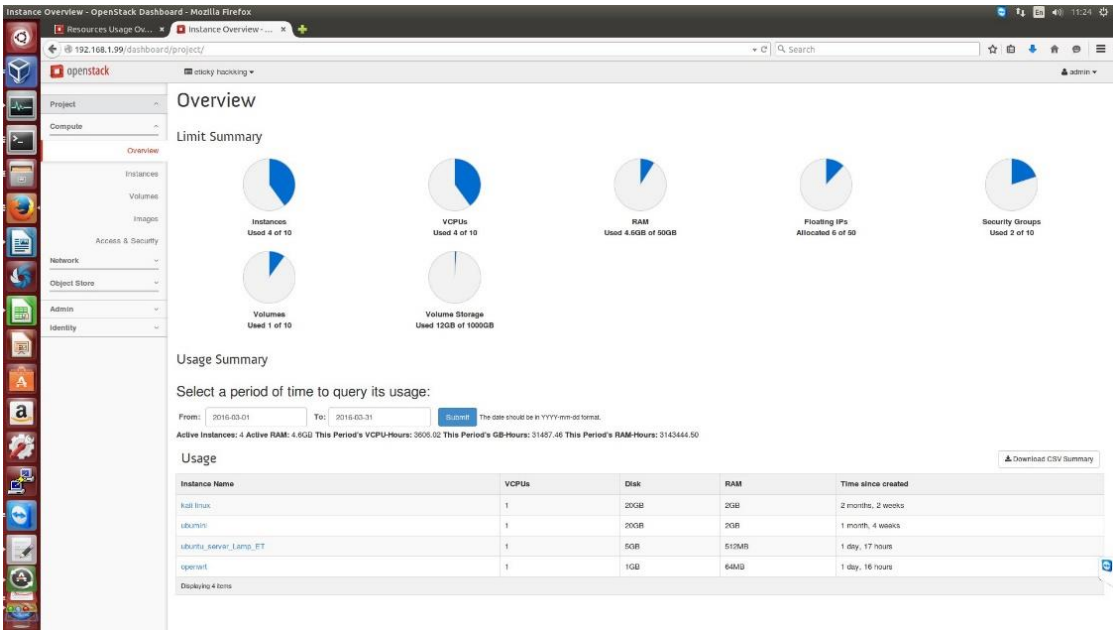
[1] Bezpečnosť na internete vďaka etickým hackerom. In: HackTrophy [online] [cit. 04.12.2017]. Dostupné na internete: https://hacktrophy.com/
[2] OWASP. In: [cit. 21.03.2018]. Dostupné na internete: https://www.owasp.org/index.php/Main_Page
[3] What is OpenStack? | Opensource.com. In: [cit. 13.06.2016]. Dostupné na internete: https://opensource.com/resources/what-is-openstack

izolovaný priestor siete, prípadne niekoľko sietí (viď obrázok 1), virtualizovať úložný priestor a výpočtový výkon za účelom modelovania reálnej prevádzky organizácie.



Obrázok 3 Virtualizačné prostredie OpenStack.
Zdroj: Vlastné spracovanie

V prostredí systému Openstack sú navrhované a vytvorené rôzne skupiny s bezpečnostnými oprávneniami a virtuálny firewall (je možné modelovať rôzne typy firewalov od rôznych výrobcov) pre jednotlivé virtuálne inštancie, ktorý zabezpečuje kontrolu na nadštandardnej úrovni nad prichádzajúcou a odchádzajúcou sieťovou komunikáciou. Prostredie Openstack virtualizácie sa ovláda z webového rozhrania.



Obrázok 4 Správa zdrojov v OpenStack.
Zdroj: Vlastné spracovanie

Ako pracovná stanica určená pre etického hackera slúži najčastejšie distribúcia Kali Linux, odporúčaný ako distribúcia pre prácu etického hackera a penetračného testera podľa metodiky OWASP. Práve operačný systém Kali Linux je vyvinutý spoločnosťou, ktorá vykonáva okrem školení aj medzinárodné certifikácie etických hackerov. Systém Kali Linux dokáže monitorovať siete a analyzovať kompletnú sieťovú komunikáciu komplexne až na úroveň fyzických paketov. V priebehu testovania bezpečnosti informačného systému organizácie môžu teda prebiehať penetračné testy jednotlivých serverov s postupným plnením krokov podľa OWASP metodiky.[4]

Smernica o kybernetickej bezpečnosti

Európska únia sa problematike kybernetickej bezpečnosti venuje už 2 desaťročia. Najvyššiu prioritu má príprava smernice o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (COM(2013) 48 final). Tento dokument bol predstavený vo februári 2013. Doteraz sa o smernici NIS (Network and Information Security) rokuje na viacerých fórach. Prvým skutočne komplexným dokumentom, ktorý pokrýva všetky kľúčové oblasti informačnej bezpečnosti je Stratégia kybernetickej bezpečnosti (Join (2013)1 final).Text hneď vo svojom úvode hovorí o povinnostiach členských štátov: „*Vlády majú niekoľko úloh: zabezpečiť prístup a otvorenosť, rešpektovať a chrániť základné práva online a udržiavať spoľahlivosť a interoperabilitu internetu.“*[5] V tomto období začalo pracovať Európske centrum boja proti počítačovej kriminalite (EC3), ktoré má za úlohu reagovať na očakávania Komisie, že dopyt po službách crackerov a iných kriminálnych živlov bude vyšší, hrozby sofistikovanejšie, globálnejšie a ľahšie sa šíriace, častejšie sa budú prať tzv. špinavé peniaze a útoky sa viac zamerajú na cloudové služby. Kybernetická bezpečnosť sa tak aj v ponímaní NATO dostáva do inej polohy. Kým EÚ zdôrazňuje ekonomické aspekty, NATO[6] vníma kyberpriestor ako rozšírenie bojiska, čo znamená, že dominantnú úlohu zohráva obrana vlastných informačných a komunikačných prostriedkov a kritickej infraštruktúry. Ďalšou

[4] STUDIO, T. Štandardný penetračný test || Nethemba. In: *Nethemba.com* [online] [cit. 04.12.2017]. Dostupné na internete: https://nethemba.com/sk/sluzby/aplikacna-bezpecnost/standardny-penetracny-test/
[5] KUČÍNSKÝ, A. Zákon o kybernetické bezpečnosti a směrnice NIS.
[6] OWASP [online] [cit. 21.03.2018]. Dostupné na internete: https://www.owasp.org/index.php/Main_Page

aktuálnou témou je napríklad vysoko aktuálne verbovanie extrémistov na internete. S povahou tejto zmeny vnímania kybernetickej bezpečnosti súvisí aj to, že niektoré kľúčové dokumenty podliehajú vyššiemu stupňu utajeniu. NATO na boj s kybernetickým zločinom v roku 2008 zriadilo vlastné centrum excelentnosti v estónskom Talline (NATO Cooperative Cyber Defence Centre of Excellence/CCD COE). Je to medzinárodná vojenská vzdelávacia inštitúcia, ktorej poloha je symbolická, estónska skúsenosť s kyberterorizmom z roku 2007 odhalila slabinu členov NATO a urýchlila prípravy spoločných iniciatív.

OWASP

Vo svete už dlhšiu dobu pôsobia organizácie, ktoré sa venujú bezpečnosti informačných systémov. Napríklad organizácia OWASP - The Open Web Application Security Project (OWASP) , ktorá ako svetová nezisková charitatívna organizácia si za svoj cieľ určila zvyšovanie úrovne bezpečnosti. Táto organizácia dokonca vydáva knižné publikácie na danú tému bezpečnosti informačných systémov a informačných technológií. Okrem toho zadefinovala etický kódex a z neho odvodené princípy. Množstvo odborníkov na bezpečnosť v danej organizácii v rámci celého sveta zbierajú skúsenosti a postupy na zabezpečenie vysokej úrovne bezpečnosti informačných systémov. Zároveň však definujú postupy, ako danú bezpečnosť prakticky otestovať. Majú vydaných niekoľko postupov, tzv. OWASP TESTING GUIDE[7], ktorá na stovkách strán definujú jednotlivé postupy ako otestovať informačný systém a informačné technológie, a najmä ako majú popísať zistené výsledky. OWASP v podstate zadefinovala pojem etický hacker. Niektorí im hovoria white hat hackers[8], iní používajú termín legálni hackeri, a iní ich pomenúvajú ako pentesters. Všetky tieto prívlastky však znamenajú to isté: hacker, ktorý organizáciám pomáha odhaliť problémy zabezpečenia s cieľom zabrániť vniknutiu a zneužitiu dát. Myšlienkou etického hackingu je platiť tzv. dobrých hackerov, aby našli neželané medzery v zabezpečení siete ešte skôr ako sa k nim dostanú tí nesprávni. Etickí hackeri používajú penetračné testovanie a iné, väčšinou útočné technológie, na odhalenie zraniteľností siete, systémov a aplikácií v organizácii. Môžeme povedať, že etickí hackeri používajú rovnaké technológie, nástroje a metódy, ktoré používajú škodliví hackeri.

Existujú aj kvalitné nástroje pre zisťovanie bezpečnosti informačných systémov, ako napríklad KALI LINUX [9] , ktorý je v súčasnej dobe považovaný medzi TOP produktami pre etických hackerov. Tento produkt je výsledkom práce skupiny OFFENSIVE SECURITY[10], ktorá sa zameriava na certifikáciu a penetračné testovanie.

Na Slovensku a v ČR pôsobí spoločnosť NETHEMBA alebo CITADELO, ktoré sú lídrami na trhu v oblasti aktívnej kontroly bezpečnosti – oblasť penetračného testovania[11]. Tieto penetračné testy sú aktívnym dokladom posúdenia bezpečnostného rizika ochrany osobných údajov v organizácii. Na Slovensku existuje aj predmet s názvom Etický hacking [12] , ktorý sa vyučuje na Fakulte managementu UK v Bratislave. Nemenej dôležité je spomenúť aj projekt HACKTROPHY[13], kde spájajú etických hackerov s organizáciami za účelom vybudovania

[7] OWASP Testing Guide v4 Table of Contents - OWASP. In: [cit. 17.12.2017]. Dostupné na internete: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

[8] Bezpečnosť na internete vďaka etickým hackerom [online] [cit. 04.12.2017]. Dostupné na internete: https://hacktrophy.com/

[9] KAROVIČ, V. Linux. In: *Digital Science Magazine* [online]. 2013. Dostupné na internete: http://digitalmag.sk/linux/

[10] Offensive Security Vision. In: [cit. 17.12.2017]. Dostupné na internete: https://www.offensive-security.com/our-vision/

[11] Our Most Advanced Penetration Testing Distribution, Ever. In: [cit. 17.12.2017]. Dostupné na internete: https://www.kali.org/

[12] KAROVIČ, V. et al. Nasadenie virtualizačného prostredia OpenStack na výučbové účely: časť 1. In: *Marketing science and inspirations*. 2016

[13] Bezpečnosť na internete vďaka etickým hackerom [online] [cit. 04.12.2017]. Dostupné na internete: https://hacktrophy.com/

bezpečnejšieho internetu pre všetkých. Praktické testovanie bezpečnosti informačných systémov, penetračné testy a etický hackeri sú nové pojmy, s ktorými sa budeme musieť v budúcnosti vysporiadať tak, aby sa dosiahla zhoda so základnými požiadavkami nariadenia GDPR, najmä však pre to, aby sa preukázalo pri porušeniach, že organizácia spravila všetko pre to, aby výrazne znížila riziká.

Dopad na bezpečnosť organizácie

V poslednej dobe sa vyskytlo príliš veľa závažných bezpečnostných incidentov, ktoré prinútili aj veľké gigantické spoločnosti v oblasti IS/IT k radikálnej zmene, príkladom je GOOGLE, ktorý po chybe INTELu[14] prechádza na nové technológie s cieľom eliminovať zásadne bezpečnostné riziká. Novinkou pre organizácie je požiadavka na pravidelné testovanie bezpečnosti osobných údajov, vyplývajúca z konceptu GDPR. Je predsa nemysliteľné, v dobe kedy je množstvo útokov na celé štáty kybernetickými útočníkmi, aby sme napríklad prehlásili, že počítačová sieť tvorená najmä OS Windows XP je bezpečná. Alebo aplikácia na webe prepojená priamo na internú databázu podniku je bezpečná, pretože dodávateľ prehlásil, že je bezpečná. V konečnom dôsledku je zodpovedná sama organizácia za dodržiavanie GDPR. Z paralely by sa mohlo prirovnať toto tvrdenie k automobilovému priemyslu. Porovnajte si dva osobné automobily. V základe sú rovnaké. Karoséria, štyri a viac kolies, sedačky pre vodiča minimálne, neprší zvyčajne do nich, majú nejaký druh motora a paliva. V skutočnosti, pokiaľ by Ste si chceli vybrať, tak budete mať záujem najmä o to, ako bezpečné je. Niektoré značky sú priam symbolom bezpečnosti. Niektoré naopak sú symbolom nebezpečnosti[15] . To isté však platí aj o bezpečnosti IS/IT.

Množstvo operačných systémov má svoje slabiny, užívatelia ich však vplyvom marketingu nevnímajú. Našťastie však existujú veľmi seriózne štúdie zaoberajúce sa bezpečnosťou. Napríklad štátne organizácie vo Veľkej Británii majú k dispozícii výsledky agentúry UK National security government agency (CESG)[16], kde porovnávali 11 bežne dostupných operačných systémov z hľadiska použitia v štátnych organizáciách. Výsledky testu, ktorý sa zaoberal 12 oblasťami bezpečnosti nebol v zásade šokujúci pre odborníkov v oblasti IS/IT, pre bežných užívateľov priniesol možno zdesenie o ich domácom operačnom systéme. Existuje však celá škála hrozieb pre operačné systémy. V poslednej dobe sa často vyskytujú tzv. ZERO DAY EXPLOIT[17], napríklad aj v overených produktoch pre operačné systémy[18] , ktoré bežne používa väčšina ľudí. Tieto bezpečnostné diery však vo veľmi veľkej miere generujú problém v dodržiavaní nariadenia GDPR. Nedávno v minulosti napríklad veľká nemocnica v Nitre padla za obeť kybernetickému útoku[19]. Podľa dostupných informácií mali aktuálny antivírový program, ransomware útok však zneužil práve ZERO DAY EXPLOIT v staršej verzii bežne používaného operačného systému.

Existuje niekoľko spôsobov ako prakticky testovať bezpečnosť osobných údajov v organizácii. Treba sa však zamyslieť nad tým, že GDPR nie je iba o bezpečnosti v oblasti

[14] BYCZECH. Google důvěřuje pouze Linuxu, zbaví se UEFI a Intel ME. In: *Root.cz* [online] [cit. 17.12.2017]. Dostupné na internete: https://www.root.cz/zpravicky/google-duveruje-pouze-linuxu-zbavi-se-uefi-a-intel-me/

[15] Auta s přístupem k internetu mohou být terčem útoků, varoval Kasperskij – Novinky.cz. In: [cit. 19.05.2016]. Dostupné na internete: http://www.novinky.cz/internet-a-pc/bezpecnost/400872-auta-s-pristupem-k-internetu-mohou-byt-tercem-utoku-varoval-kasperskij.html

[16] End User Devices Security Guidance: Introduction | CESG Site. In: [cit. 12.06.2016]. Dostupné na internete: https://www.cesg.gov.uk/guidance/end-user-devices-security-guidance-introduction

[17] [CSL STYLE ERROR: reference with no printed form.]

[18] DSL.sk - Microsoft po problémoch úplne zrušil bezpečnostné aktualizácie, Windows zostane zraniteľný 6 týždňov. In: *DSL.sk* [online] [cit. 04.12.2017]. Dostupné na internete: http://www.dsl.sk/article.php?article=19421

[19] [CSL STYLE ERROR: reference with no printed form.]

IS/IT tak, ako to bežne vnímame, teda počítače a ich softvéry. Ide aj o fyzické podoby dokumentov. Fyzická ochrana sa však dá vyriešiť výrazne jednoduchšie ako ochrana informačných systémov. Zamknuté dvere so špeciálnym zámkom, kde sú bezpečnostné triedy odolnosti[20], sú pravdepodobnejšie odolnejšie voči fyzickým útokom, pretože na prvý pohľad vravia útočníkovi, že tu bude problém a veľa práce s prekonaním prekážky. Počítačové systémy však predstavujú naopak veľmi lákavú ponuku k útoku. Pokiaľ útočník objaví na webe napríklad systém Windows XP, tak má širokú paletu nástrojov, ako sa do neho môže dostať bez vedomia majiteľa. Na rozdiel od bezpečnostných dverí to však nebude nikde vidieť.

Na trhu sú etablované organizácie zaoberajúce sa bezpečnosťou informačných systémov formou testovania bezpečnosti. Taktiež však sú na trhu organizácie zaoberajúce sa "špehovaním" iných organizácií[21] , pričom niekde medzitým sa pohybuje bežný užívateľ. Výnimočné nie sú ani veľmi jednoduché postupy, ako sa dostať do počítača s operačným systémom WINDOWS. Pri ilustráciu napríklad do bežného počítača s WINDOWS 7 a vyšším sa dá dostať pomerne jednoducho. Stačí nabootovať cez niektorú z dostupných LIVE edícií LINUX derivátov[22]. Tam stačí na disku zazálohovať súbor WINDOWS\SYSTEM32\magnify.exe a miesto neho spraviť kópiu súboru cmd.exe a následne ho premenovať na vyššie uvedený súbor. Po spustení počítača potom kliknutím na ikonu vpravo dole a následne sa spustí príkazový riadok. Stačí už dať v podstate iba dva príkazy - net user HACKER heslo /add a následne ďalší príkaz net localgroup administrators HACKER /add. Následne po reštarte máme admina pod menom HACKER s heslom heslo a máme počítač plne pod kontrolou. Existujú však aj iné formy, ktoré za určitých podmienok nepotrebujú reštart.

Návrhy zmeny procesov v organizácii

Organizácia v praxi musí preveriť stav pripravenosti na plnenie požiadaviek smernice. Teda bude musieť previesť analýzu súladu organizácie s požiadavkami nariadenia podrobne. Po analýze musí následne spracovať analýzu rizík a posúdenie vplyvu spracovateľských operácií na kybernetickú bezpečnosť. Na základe analýzy rizík a posúdenia vplyvu zavedie prípadne nové procesy, resp. modifikuje existujúce procesy v organizácii. S veľmi veľkou pravdepodobnosťou organizácia bude musieť zmeniť časť technológií a bude musieť implementovať systémy manažérstva informačnej bezpečnosti a manažérstva IT služieb.
zavádza ako jednu z vyplývajúcich požiadaviek aj požiadavku na zabezpečenie odolnosti systémov spracúvania osobných údajov a podporných služieb. S touto požiadavkou veľmi úzko súvisí aj požiadavka na zabezpečenie sieťovej bezpečnosti a ochrany infraštruktúry spracúvajúcej osobné údaje pred internými a externými hrozbami. Splnenie tejto požiadavky si pravdepodobne bude vyžadovať vyčlenenie podnikových zdrojov vo väčšej miere.

V rámci existujúcich legislatívnych požiadaviek v súčasnosti už množstvo organizácií má požiadavku splnenú, najmä ak majú jednu z medzinárodných certifikácií ISO, napríklad ISO 27001[23], alebo majú zavedený nejaká štandard typu ITIL[24] pre riadenie a správu IT v organizácii. Existujúcich noriem a štandardov je niekoľko, množstvo z nich je potrebných pre projekty informatizácie štátnej a verejnej správy. Proces zavedenia štandardov alebo certifikácií

[20] Bezpečnostné triedy. In: *Bezpečnostné dvere* [online] [cit. 04.12.2017]. Dostupné na internete: https://bezpecnostnedvere.com/rady/bezpecnostne-triedy/

[21] [CSL STYLE ERROR: reference with no printed form.]

[22] Contribute to Ubuntu | Ubuntu | Ubuntu. In: [cit. 04.12.2017]. Dostupné na internete: https://www.ubuntu.com/download/desktop/contribute?version=16.04.3&architecture=amd64

[23] MANAGEMENTMANIA. ISO 27001 Systém manažérstva bezpečnosti informácií. In: ManagementMania.com [online] [cit. 04.12.2017]. Dostupné na internete: https://managementmania.com/sk/iso-27001

[24] MANAGEMENTMANIA. ITIL (Information Technology Infrastructure Library). In: ManagementMania.com [online] [cit. 04.12.2017]. Dostupné na internete: https://managementmania.com/sk/itil-information-technology-infrastructure-library

na normy si však vyžaduje zvyčajne dlhší časový horizont a množstvo zdrojov ako ľudských tak i finančných zdrojov.

Včasná identifikácia bezpečnostných incidentov

Včasná identifikácia bezpečnostných incidentov v každom prípade nie je to, čo spravila spoločnosť UBER, ktorej odcudzili cca 50 miliónov osobných údajov[25] a rok o tom mlčala a platila hackerom. Alebo v roku 2013 kedy ukradli spoločnosti ADOBE[26] zhruba 38 miliónov údajov o užívateľoch vrátane 2,9 milióna údajov o kreditných kartách, to taktiež nebola včasná identifikácia bezpečnostných incidentov. Tých bezpečnostných incidentov v poslednej dobe je však veľmi veľa. Veľký poplach v oblasti bezpečnosti spôsobila v minulom období informácia o tzv. VAULT7 [27] Ide vraj o nástroje CIA, ktoré mala používať na infiltrovanie informačných systémov. Informácia bola oficiálne dementovaná. Následne skupina hackerov napadla NSA[28] a ukradla im celú zbierku nástrojov a verejne ich publikovala na známom serveri Github[29] v zdrojových kódoch. Niekoľko dní nato bol distribuovaný ransomware Wannacry[30] a následne ransomware Petya[31], ktorý spôsobil výrazné výpadky v infraštruktúre IT. Okrem toho existovali hrozby staršieho dáta typu STUXNET[32] a jeho následníci typu Duqu[33]. Jedna verzia pod názvom Flame[34] dokázala čítať dáta z mobilných telefónov ANDROID aj pri vypnutom Bluetooth. Vírusov bude žiaľ pravdepodobne iba pribúdať.

Po prečítaní hore uvedených incidentov sa môže neznalému v oblasti GDPR javiť, že táto požiadavka je prakticky neuskutočniteľná. Je možné nájsť na internete niekoľko vyjadrení o obtiažnosti splnenia požiadavky, ale je potrebné pozrieť sa na tú požiadavku reálne očami úradníka v EÚ. Tomu je jasné, že incident bude. Pravdepodobne aj na svojom informačnom systéme už mal incident. V praxi je preto potrebné zaviesť vlastne procesy riadenia bezpečnostných incidentov. Organizácie so zavedenými bezpečnostnými normami to už majú splnené. Zvyšné organizácie zavedú tento proces tak, aby zaviedli nejaký ten systém a zaviedli

[25] Hackeri ukradli Uberu dáta miliónov ľudí, firma im platila za mlčanie - Ekonomika - Správy - Pravda.sk. In: [cit. 04.12.2017]. Dostupné na internete: https://spravy.pravda.sk/ekonomika/clanok/448839-hackeri-ukradli-uberu-data-milionov-ludi-uber-im-platil-za-mlcanie/

[26] Adobe says source code, customer data stolen by hackers. In: [cit. 07.12.2017]. Dostupné na internete: https://www.reuters.com/article/us-adobe-cyberattack/adobe-says-source-code-customer-data-stolen-by-hackers-idUSBRE99212Y20131004

[27] DO, T. CIAHackingTools: WikiLeaks Vault 7 CIA Hacking Tools [online]. 2017 [cit. 07.07.2017]. Dostupné na internete: https://github.com/troydo42/CIAHackingTools

[28] KOLIBA, J. Nástroje na ovládnutí Windows jsou volně dostupné. Hackeři je prý získali od NSA. In: Živě.cz [online] [cit. 07.07.2017]. Dostupné na internete: https://www.zive.cz/bleskovky/nastroje-na-ovladnuti-windows-jsou-volne-dostupne-hackeri-je-pry-ziskali-od-nsa/sc-4-a-187203/default.aspx

[29] misterch0c/shadowbroker. In: GitHub [online] [cit. 07.07.2017]. Dostupné na internete: https://github.com/misterch0c/shadowbroker

[30] Počítače v nitrianskej nemocnici napadol vírus WannaCry, znefunkčnil rôzne operačné systémy [online] [cit. 04.12.2017]. Dostupné na internete: https://www.webnoviny.sk/wannacry-napadol-v-nemocnici-v-nitre-pocitace-s-roznymi-operacnymi-systemami/

[31] Hrozba silnie, nová verzia ramsomvéru Petya opravuje chybu v šifrovacom algoritme | Živé.sk. In: [cit. 22.07.2016]. Dostupné na internete: http://www.zive.sk/clanok/116433/hrozba-silnie-nova-verzia-ramsomveru-petya-opravuje-chybu-v-sifrovacom-algoritme#

[32] ŽIVÉ.SK. Červ podobajúci sa na Stuxnet zbiera informácie o riadiacich systémoch. In: *Živé.sk* [online] [cit. 07.12.2017]. Dostupné na internete: https://www.zive.sk/clanok/53552/cerv-podobajuci-sa-na-stuxnet-zbiera-informacie-o-riadiacich-systemoch/

[33] The four amigos: Stuxnet, Flame, Gauss and DuQu. In: *Concise Courses* [online] [cit. 07.12.2017]. Dostupné na internete: https://www.concise-courses.com/stuxnet-flame-gauss-duqu/

[34] ZETTER, K. Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload. In: *WIRED* [online] [cit. 16.05.2016]. Dostupné na internete: https://www.wired.com/2012/08/gauss-espionage-tool/

podporné nástroje na evidenciu a riešenie incidentov (napr. HP Service Manager [35], SIEM [36]). Pokiaľ organizácie budú spĺňať zvyšné požiadavky nariadenia, tak majú zabezpečený monitoring správania sa celého systému. Vo svojej podstate všetky odchýlky od zadefinovaného správania sa systému nahlásia v novom procese a následne sa budú spracovávať, vyhodnocovať a riešiť na základe vopred stanovených pravidiel a postupov. Obrazne sa to dá prirovnať k havárii motorového vozidla – automaticky konáme podľa nastavených pravidiel, robíme všetko preto aby sa nestala nehoda, ale pokiaľ bude, automaticky riešime podľa priorít.

Záver

V súčasnej dobe je ochrana a zabezpečenie informačného systému respektíve ochrana informácií veľmi zásadnou úlohou manažérov a to nielen v podnikovej sfére. Príprava manažérov na úlohu spojenú s ochranou informácií môže začať už na školách pomocou výučby a to nielen v teoretickej rovine.[37] Predmet Etický hacking pomocou praktického cvičenia, ukážkami techník a premýšľania nad slabými miestami informačných systémov môže napomôcť budúcim manažérom pri riadení bezpečnosti toku informácií v organizáciách. Výučba predmetu bez použitia virtuálneho prostredia openStack[38] bola veľmi náročnou úlohou a väčšina ukážok techník a nástrojov nebolo možné realizovať, vzhľadom na zabezpečenie školskej siete. Použitím softvéru openStack bolo dosiahnuté oddelenie systému zabezpečujúceho chod školy a výukového – testovacieho prostredia, v ktorom bolo možné rýchle nasadenie rôznych modelov a testovanie ich bezpečnosti. Najdôležitejším parametrom bolo zabezpečenie oddelenia kritických častí školskej siete od modelov sieti a technológií tvorených vo virtuálnom prostredí openStacku, avšak so zabezpečením prístupu do internetu, čím sme dosiahli, že sa systém javil ako reálny.

Zoznam použitej literatúry:

BRNKAĽÁKOVÁ, D., VOJTECHOVSKÝ, J. Testovanie použiteľnosti. In: *Digital Science Magazine [elektronický zdroj]*. 2015, roč. 4, č. 1

BYCZECH. Google důvěřuje pouze Linuxu, zbaví se UEFI a Intel ME. In: *Root.cz* [online] [cit. 17.12.2017]. Dostupné na internete: https://www.root.cz/zpravicky/google-duveruje-pouze-linuxu-zbavi-se-uefi-a-intel-me/

DÁVIDEKOVÁ, M., DÁVIDEKOVÁ, S. Case study of applied managerial techniques of selected team manager in practice. In: *International Scientific Conference on MMK 2015 Proceedings*. Hradec Králové: Magnanimitas, 2015, s. 264-274. ISBN ISBN 978-80-87952-12-2.

DÁVIDEKOVÁ, M., GREGUŠ ML., M., BEŇOVÁ, E. Feasibility Study of Virtual Collaboration Concept of Academic Institutions from the Point of View of Students. In: *AUER, M., GURALNICK, D., SIMONICS, I., ed. Teaching and Learning in a Digital World II, International Conference on Interactive Collaborative Learning (ICL 2017), Advances in Intelligent Systems and Computing (AISC)*. 2018. vyd. [s.l.]: Springer, zv. 716, s. 51-56. ISBN ISBN 978-3-319-73203-9.

[35] Spoločnosť HP Inc. predstavuje prvý notebook na svete s integrovaným filtrom ochrany súkromia. In: [cit. 04.01.2018]. Dostupné na internete: https://online.asbis.sk/default.asp?inc=userfiles%2Fsites%2Fhp%2Fhp_ts_17_10_2016.htm&utm_source=web&utm_medium=oznam&utm_campaign=hp_tlacova_srpoava_17_10_2016&utm_term=hp_tlacova_srpoava_17_10_2016&utm_content=hp_tlacova_srpoava_17_10_2016

[36] MIKESKA, P. SIEM: Ochrana citlivých informácií pred únikom zvnútra firmy. In: *INFOWARE*. 2012, roč. VIII., č. 12/2012

[37] KAROVIČ et al., Nasadenie virtualizačného prostredia OpenStack na výučbové účely

[38] KAROVIČ, V. et al. Nasadenie virtualizačného prostredia OpenStack na výučbové účely: časť 2. In: *Marketing science and inspirations*. 2016

DÁVIDEKOVÁ, M., HVORECKÝ, J. ICT Collaboration Tools for Virtual Teams in Terms of the SECI Model. In: *International Journal of Engineering Pedagogy (iJEP)*. 2017, roč. 7, č. 1, s. 95-116. ISSN ISSN 2014-3591.
DO, Troy. *CIAHackingTools: WikiLeaks Vault 7 CIA Hacking Tools* [online]. 2017 [cit. 07.07.2017]. Dostupné na internete: https://github.com/troydo42/CIAHackingTools
KAROVIČ, V. Linux. In: *Digital Science Magazine* [online]. 2013. ISSN ISSN 1339-3782. Dostupné na internete: http://digitalmag.sk/linux/
KAROVIČ, V. et al. Nasadenie virtualizačného prostredia OpenStack na výučbové účely: časť 1. In: *Marketing science and inspirations*. 2016, s. 43-52. ISSN ISSN 1338-7944.
KAROVIČ, V. et al. Nasadenie virtualizačného prostredia OpenStack na výučbové účely: časť 2. In: *Marketing science and inspirations*. 2016, s. 2-5. ISSN ISSN 1338-7944.
KOLIBA, J. Nástroje na ovládnutí Windows jsou volně dostupné. Hackeři je prý získali od NSA. In: *Živě.cz* [online] [cit. 07.07.2017]. Dostupné na internete: https://www.zive.cz/bleskovky/nastroje-na-ovladnuti-windows-jsou-volne-dostupne-hackeri-je-pry-ziskali-od-nsa/sc-4-a-187203/default.aspx
KRYVINSKA, N. An analytical approach for the modeling of real-time services over IP network. In: *Mathematics and Computers in Simulation* [online]. 2008, roč. 79, č. 4, s. 980-990. ISSN 03784754. DOI: 10.1016/j.matcom.2008.02.016
KRYVINSKA, N. Building consistent formal specification for the service enterprise agility foundation. In: *Journal of Service Science Research* [online]. 2012, roč. 4, č. 2, s. 235-269. ISSN 2093-0720, 2093-0739. DOI: 10.1007/s12927-012-0010-5
KRYVINSKA, N. et al. A Methodology for the Enterprise Information and Communication Infrastructure Design Process. In: TAKIZAWA, Makoto, BAROLLI, Leonard, ENOKIDO, Tomoya. eds. *Network-Based Information Systems* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, zv. 5186, s. 303-312 [cit. 16.05.2016]. ISBN 978-3-540-85692-4. Dostupné na internete: http://link.springer.com/10.1007/978-3-540-85693-1_32
KUČÍNSKÝ, A. Zákon o kybernetické bezpečnosti a směrnice NIS. , s. 3.
MANAGEMENTMANIA. ISO 27001 Systém manažérstva bezpečnosti informácií. In: *ManagementMania.com* [online] [cit. 04.12.2017]. Dostupné na internete: https://managementmania.com/sk/iso-27001
MANAGEMENTMANIA. ITIL (Information Technology Infrastructure Library). In: *ManagementMania.com* [online] [cit. 04.12.2017]. Dostupné na internete: https://managementmania.com/sk/itil-information-technology-infrastructure-library
GREGUŠ, M., LENHARD. T. H. Case study - virtualisation of servers in the area of healthcare-IT. In: *International journal for applied management science and global developments*. 2012, s. 1-10. ISSN ISSN 2195-4135.
MIKESKA, P. SIEM: Ochrana citlivých informácií pred únikom zvnútra firmy. In: *INFOWARE*. 2012, roč. VIII., č. 12/2012, s. 64. ISSN 1335-4787.
PAWERA, R. *Manažment európskej bezpečnosti*. [s.l.]: Eurounion, 2005.
STUDIO, Truben. Štandardný penetračný test || Nethemba. In: *Nethemba.com* [online] [cit. 04.12.2017]. Dostupné na internete: https://nethemba.com/sk/sluzby/aplikacna-bezpecnost/standardny-penetracny-test/
VOJTECHOVSKÝ, J., PROKSOVÁ, M., PORÁZIKOVÁ, E. Elektronické podnikanie. In: *Trendy v online marketingu [elektronický zdroj]*. Bratislava: Univerzita Komenského, 2016, s. nestr. ISBN ISBN 978-80-223-4106-6.
ZETTER, K. Flame and Stuxnet Cousin Targets Lebanese Bank Customers, Carries Mysterious Payload. In: *WIRED* [online] [cit. 16.05.2016]. Dostupné na internete: https://www.wired.com/2012/08/gauss-espionage-tool/
ŽIVÉ.SK. Červ podobajúci sa na Stuxnet zbiera informácie o riadiacich systémoch. In: *Živé.sk* [online] [cit. 07.12.2017]. Dostupné na internete:

https://www.zive.sk/clanok/53552/cerv-podobajuci-sa-na-stuxnet-zbiera-informacie-o-riadiacich-systemoch/
Adobe says source code, customer data stolen by hackers. In: [cit. 07.12.2017]. Dostupné na internete: https://www.reuters.com/article/us-adobe-cyberattack/adobe-says-source-code-customer-data-stolen-by-hackers-idUSBRE99212Y20131004
Auta s přístupem k internetu mohou být terčem útoků, varoval Kasperskij – Novinky.cz. In: [cit. 19.05.2016]. Dostupné na internete: http://www.novinky.cz/internet-a-pc/bezpecnost/400872-auta-s-pristupem-k-internetu-mohou-byt-tercem-utoku-varoval-kasperskij.html
Bezpečnosť na internete vďaka etickým hackerom. In: *HackTrophy* [online] [cit. 04.12.2017]. Dostupné na internete: https://hacktrophy.com/
Bezpečnostné triedy. In: *Bezpečnostné dvere* [online] [cit. 04.12.2017]. Dostupné na internete: https://bezpecnostnedvere.com/rady/bezpecnostne-triedy/
Contribute to Ubuntu | Ubuntu | Ubuntu. In: [cit. 04.12.2017]. Dostupné na internete: https://www.ubuntu.com/download/desktop/contribute?version=16.04.3&architecture=amd64
DSL.sk - Microsoft po problémoch úplne zrušil bezpečnostné aktualizácie, Windows zostane zraniteľný 6 týždňov. In: *DSL.sk* [online] [cit. 04.12.2017]. Dostupné na internete: http://www.dsl.sk/article.php?article=19421
End User Devices Security Guidance: Introduction | CESG Site. In: [cit. 12.06.2016]. Dostupné na internete: https://www.cesg.gov.uk/guidance/end-user-devices-security-guidance-introduction
Hackeri ukradli Uberu dáta miliónov ľudí, firma im platila za mlčanie - Ekonomika - Správy - Pravda.sk. In: [cit. 04.12.2017]. Dostupné na internete: https://spravy.pravda.sk/ekonomika/clanok/448839-hackeri-ukradli-uberu-data-milionov-ludi-uber-im-platil-za-mlcanie/
Hrozba silnie, nová verzia ramsomvéru Petya opravuje chybu v šifrovacom algoritme | Živé.sk. In: [cit. 22.07.2016]. Dostupné na internete: http://www.zive.sk/clanok/116433/hrozba-silnie-nova-verzia-ramsomveru-petya-opravuje-chybu-v-sifrovacom-algoritme#
misterch0c/shadowbroker. In: *GitHub* [online] [cit. 07.07.2017]. Dostupné na internete: https://github.com/misterch0c/shadowbroker
Offensive Security Vision. In: [cit. 17.12.2017]. Dostupné na internete: https://www.offensive-security.com/our-vision/
Our Most Advanced Penetration Testing Distribution, Ever. In: [cit. 17.12.2017]. Dostupné na internete: https://www.kali.org/
OWASP. In: [cit. 21.03.2018]. Dostupné na internete: https://www.owasp.org/index.php/Main_Page
OWASP Testing Guide v4 Table of Contents - OWASP. In: [cit. 17.12.2017]. Dostupné na internete: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
Spoločnosť HP Inc. predstavuje prvý notebook na svete s integrovaným filtrom ochrany súkromia. In: [cit. 04.01.2018]. Dostupné na internete: https://online.asbis.sk/default.asp?inc=userfiles%2Fsites%2Fhp%2Fhp_ts_17_10_2016.htm&utm_source=web&utm_medium=oznam&utm_campaign=hp_tlacova_srpoava_17_10_2016&utm_term=hp_tlacova_srpoava_17_10_2016&utm_content=hp_tlacova_srpoava_17_10_2016
The four amigos: Stuxnet, Flame, Gauss and DuQu. In: *Concise Courses* [online] [cit. 07.12.2017]. Dostupné na internete: https://www.concise-courses.com/stuxnet-flame-gauss-duqu/
What is OpenStack? | Opensource.com. In: [cit. 13.06.2016]. Dostupné na internete: https://opensource.com/resources/what-is-openstack

Kontaktné údaje:
PhDr. Peter Veselý, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
82005 Bratislava
Thomson Reuters Researcher ID: H-5695-2017
ORCID ID: 0000-0002-7857-6355
Scopus Author ID: 57195951243
peter.vesely@fm.uniba.sk

Mgr. Vincent Karovič, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
82005 Bratislava
vincent.karovic2@fm.uniba.sk

Zabezpečenie ochrany webového sídla pred útokmi typu DDoS a inými rizikami

Jaroslav Vojtechovský, Peter Veselý

Abstrakt:
Praktické využitie služieb IDS, IPS a ochrany pred DDoS útokmi na webové sídla organizácie, mechanizmus fungovania load balancing webového sídla a cachovanie obsahu webového sídla. Porovnanie výkonnosti a ochrany webového sídla po implementácii služby Cloudflare prevedením penetračného testu podľa metodiky OWASP.
Kľúčové slová:
kybernetická bezpečnosť, IDS, IPS, DDoS, OWASP

Abstract:
Practical use of services IDS, IPS and protections of DDoS attacks against the organization's web site, load balancing of website and caching of web site content. Comparing Web site performance and protection after implementing Cloudflare by passing a penetration test according to OWASP methodology.
Key words:
cyber security, IDS, IPS, DDoS, OWASP

Úvod

Slovenský online priestor v posledných dňoch čelí masívnym DDOS útokom hackerov z celého sveta. Informovala o tom Národná agentúra pre sieťové a elektronické služby (NASES). Okrem iných slovenských webových adries útočníci v posledných dňoch napadli stránky Slovenského hydrometeorologického ústavu (SHMÚ), ale aj portál slovensko.sk. Ako uviedol generálny riaditeľ NASES Lukáš Sojka, na systémoch v správe agentúry sa zatiaľ tieto útoky objavili len v malej intenzite a veľmi sporadicky. Agentúra je prevádzkovateľom portálu slovensko.sk aj vládnej siete Govnet, ktorá poskytuje služby napríklad spomínaným meteorológom.[1] Aj toto je realita dnešných dní. Početnosť útokov sa zvyšuje, sofistikovanosť taktiež. Udržať webové aplikácie v bezpečí a prevádzke začína byť pomerne zložitý proces. Smernica o kybernetickej bezpečnosti a nariadenie GDPR pri tom tento proces stanovuje povinným pre obrovské množstvo organizácií. Zabezpečiť bezpečnosť už je pre mnohé organizácie pod tlakom pokút otázkou prežitia na trhu.

IDS, IPS, DDoS

Bezpečnosť nie je iba o prevencii a ochrane, ale taktiež aj o detekcii a reakcii. IDS – Intrusion Detection System, je systém detekcie prienikov, ktorý deteguje narušenie alebo prípadné pokusy o narušenie počítačových systémov. Vychádza z predpokladu, že prípadný narušiteľ bude vykonávať také úkony, ktoré budú na základe priamych alebo nepriamych indícií odlíšiteľné od bežného používateľa. Umiestnenie IDS je veľmi dôležité, pretože z typu informácií, ktoré má k dispozícii, vyplýva jeho schopnosť detegovať rôzne druhy útokov, ale ae má vplyv aj na rozsah pokrytia danej oblasti. IDS sa môžu deliť podľa umiestnenia na nasledovné systémy[2]:

- HIDS (Host based IDS) - IDS orientované na hostiteľský systém. Zbierajú informácie z konkrétneho systému. Využívajú systémové záznamy generované jadrom a ďalšími systémovými zdrojmi

[1] Slovensko čelí masívnym DDOS útokom hackerov. In: Pravda.sk [online] [cit. 01.07.2018]. Dostupné na internete: https://spravy.pravda.sk/ekonomika/clanok/473027-slovensko-celi-masivnym-ddos-utokom-hackerov/

[2] IDS. In: [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni

- NIDS (Network IDS) - Sieťové IDS. Najčastejšie realizované na dedikovaných serveroch, spracúvajú informácie získané zo sieťových rozhraní
- Hybrid IDS - Komplexní systémy kombinujúci oba predchádzajúce typy.

Dôležitou vlastnosťou IDS je aj princíp činnosti pri detekcii útoku. Určuje schopnosť rozpoznávať doteraz neznáme typy útokov nebo mieru generovaných falošných varovaní, podľa princípu činnosti ich delíme nasledovne[3]:

- Porovnávanie vzorov - Detekcie podľa porovnávania so vzormi (pravidlá, signatúry). Ty zodpovedajú udalostiam nebo postupnosti udalostí typických pre známe útoky nebo narušení systémov. Vzory sú vytvárané na princípoch konečných automatov, rozhodovacích stromov, expertných systémov, neurónových sietí atď.
- Detekcie štatistickej anomálie - Upozorní na podozrivé odchýlky od dlhodobo sledovaného normálneho chovania.
- Korelačné IDS - Vyhľadávajú súvislosti medzi javmi prebiehajúcimi na niekoľkých miestach.

Okamžik vyhodnocovania určuje rýchlosť detekcie útoku. Vyhodnocovanie v reálnom čase je výkonovo náročnejšie, ale umožňuje okamžitú reakciu na útok. Podľa okamžiku vyhodnocovania delíme IDS na nasledovné systémy[4] :

- V reálnom čase - Priebežné zbieranie a vyhodnocovanie informácií. Systémy umožňujú generovať real-time poplachy a automatické odozvy na útok.
- Dávkovo orientovaný prístup - Periodický zber informácií s následným vyhodnocovaním. Vhodné pre prostredia s pomerne nízkymi rizikami a potenciálnymi stratami.

IPS - Intrusion Protection System – je systém veľmi podobný systémom IDS. Hlavným rozdielom medzi IDS a IPS je to, že IPS nie je len pasívny prvok v sieti, ktorý nás upozorňuje na hrozby, ale dokáže sa aktívne podielať aj na filtrovaní dát. Táto schopnosť brániť sa hrozbám za hranice tretej sieťovej vrstvy z IPS robí veľmi užitočné zariadenia v oblasti sieťovej bezpečnosti. Podľa nastavených pravidiel môže vykonávať akcie ako sú alert, drop, reset a block. IDS/IPS pracujú od tretej vrstvy OSI modelu (L3 až L7), alebo sieťovej vrstvy. Táto vrstva zabezpečuje sniffing[5] v sieti a sieťové adresovanie. Na tejto vrstve prevezmú IDS/IPS pakety, ktoré v danom sieťovom uzly zaznamenajú a postupne prevedú ich rozloženie až do siedmej sieťovej vrstvy OSI modelu (hĺbková inšpekcia). Všetky tieto informácie postupne porovnávajú s definovanými pravidlami a ak príde k zhode s niektorým z tých pravidiel, prevedú príslušnú akciu podľa nastavení IDS/IPS.[6]

DDoS – Denial of Service – útoky typu odopretia služby sú útoky na sieťovú infraštruktúru vo svojej podstate relatívne jednoduchým, ale veľmi účinným kybernetickým útokom. Práve kvôli svojej jednoduchosti sú jedným z najčastejšie využívaným typom útokov. Sú založené na základom fakte, že všetky služby dostupné na internete sú poskytované servermi, ktoré majú určitý výkon a konektivitu. Cieľom útoku DDoS je práve znemožniť dostupnosť služby a to buď zahltením konektivity (útoky s veľkým dátovým tokom) alebo preťažením výpočtových prostriedkov servera. V oboch prípadoch nie je behom útoku možná

[3] IDS [online] [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni
[4] IDS [online] [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni
[5] Charakteristika a význam slova sniffing. In: [cit. 08.04.2018]. Dostupné na internete: http://pdf.truni.sk/e-ucebnice/sips/data/bc638bc8-8616-450f-b4f0-872a9c835cfa.html?ownapi=1
[6] ENDORF, C.F. *Detekce a prevence počítačového útoku*. [s.l.]: Grada Publishing a.s., 2005

komunikácia so serverom a tým ani so službami, ktoré sú poskytované. Útočník typicky server neovláda, nepozná mená a heslá ale napriek tomu znemožní používateľom prístup k službe. Útoky typu DDoS sa delia vo svojej podstate na tzv. záplavové DoS (DoS flood), útoky využívajúce zraniteľnosť, distribuované útoky (typu BOTNET) a iné typy útokov (napr. XDoS).[7] Delenie a popis DDoS útokov je pomerne rozsiahle a vyžadovalo by si samostatnú prácu vzhľadom na rozsah.

Balance loading a cache stránok

Load balancing (vyvažovanie záťaže) je v sieťových riešeniach technika, ktorá rozmiestňuje záťaž medzi dvoma a viacerými počítačmi, sieťovými pripojeniami, procesormi, pevnými diskami alebo inými zdrojmi. Cieľom je dosiahnutie optimálneho využitie zdrojov, maximalizovanie priepustnosti dát, minimalizovanie času odozvy alebo predídenie preťaženia zdrojov. Využívanie viacerých komponentov s load balancing namiesto jedného komponentu, môže zvýšiť spoľahlivosť pomocou redundancie. Servis Load Balancing je zvyčajne zabezpečený dedikovaným hardvérovým zariadením (ako viacvrstvový switch alebo DNS server). Pre internetové servisy môže byť load balancing zvyčajne program, ktorý počúva na určenom porte, na ktorý sa pripojí externý klient. Tento potom prepošle jeho požiadavku na jeden z koncových serverov a zvyčajne odpovie load balanceru. Toto povoľuje odpovedať klientovi bez toho, aby vedel o delení záťaže. Týmto spôsobom sa dá pomerne jednoducho predchádzať tomu, aby klienti priamo pristupovali na koncové servery. Niektoré load balancery poskytujú špecifickú funkciu, ktorá vykoná určitú operáciu ak sú všetky koncové servery nedostupné. Môže to zahrňovať preposielanie požiadaviek na záložný load balancer alebo zobrazovať poruchovú hlášku.[8]

Webová cache sa nachádza medzi jedným nebo viacerými webovými servermi (pôvodné servery) a klientom alebo viacerými klientami, sleduje požiadavky na HTML stránky, obrázky a súbory (spolu označované ako objekty), zbiera ich a ukladá si pro sebe kópie. Ak potom príde iná požiadavka na rovnaký objekt, cache použije kópiu, ktorú už má, miesto toho aby znova o rovnaký objekt žiadala pôvodný server. Existujú dva hlavné dôvody, prečo sa používajú webové cache stránok:

- Zmenšujú omeškanie - požiadavka je miesto pôvodného serveru uspokojená z cache, zaberie získanie a zobrazení objektu klientovi menej času. Webové stránky majú rýchlejšiu reakciu.
- Zmenšujú objem prenosu - každý objekt je zo serveru prenášaný iba raz, zmenšuje sa prenos dát a množstvo spojení používaných klientom.

Základné typy cache webových stránok, používané v súčasnosti sa dajú definovať nasledovne [9]:

- Cache internetového prehliadača - Tato nastavení umožňuje zarezervovať časť disku na ukladanie objektov. Táto cache pracuje na základe jednoduchých pravidiel. Zvyčajne jedenkrát za session (pri každom spustení prehliadača) sa u každého objektu overí, že je objekt čerstvý.
- Proxy cache - cache webových proxy fungujú na rovnakom princípe, ale v oveľa väčšom rozsahu. Proxy obsluhuje stovky alebo tisíce používateľov rovnakým spôsobom.
- Cache na bránach – sú taktiež známe ako "reverzné proxy cache" alebo ako „náhradné cache“. Cache na bránach sú taktiež prostredníci, ale miesto toho, aby boli nasadené

[7] Najlepšie webhostingové spoločnosti v kategórii Služby DDoS ochrany – rok 2018. In: *HostAdvice* [online] [cit. 18.02.2018]. Dostupné na internete: https://sk.hostadvice.com/hosting-companies/ddos-protection/

[8] MARKETINGER.SK. LOAD-BALANCING. In: *Sectec.sk* [online] [cit. 08.04.2018]. Dostupné na internete: https://www.sectec.sk/bezpecnost/load-balancing

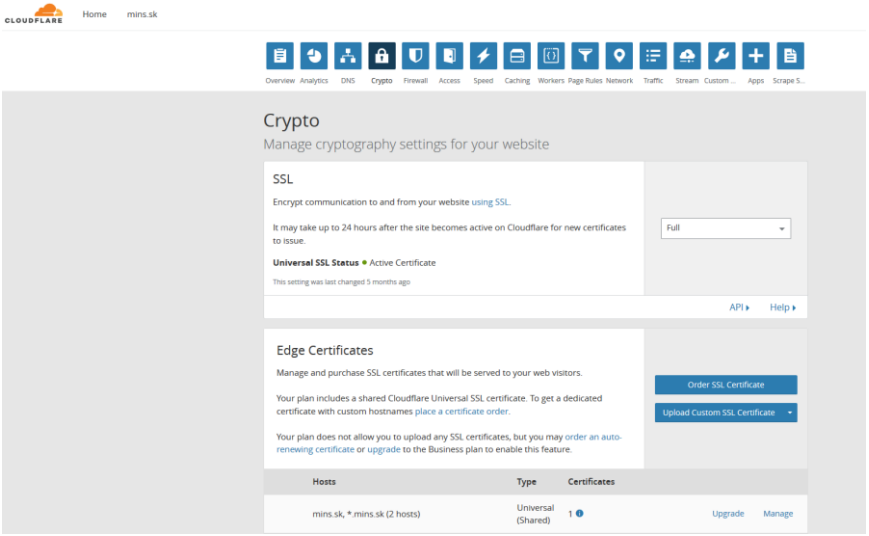
[9] Kešovací návod pro autory webu a webmastery. In: [cit. 08.04.2018]. Dostupné na internete: https://www.jakpsatweb.cz/clanky/caching-tutorial-czech-translation.html

administrátormi siete na zníženie objemu prenosu, sú typicky nasadzované samotnými webmastermi, ktorí sa snažia mať web dostupnejší, spoľahlivejší a funkčnejší.

- Siete na poskytovanie obsahu (Content delivery networks) - CDN - distribuujú reverzní proxy cache celým Internetom (nebo jeho časťou) a predávajú cachovanie prevádzkovateľom webov, ktorí o to majú záujem. Príkladom CDN sú Speedera, Amazon Cloudfront, Cloudflare a Akamai.

CDN Služba Cloudlare.com ako možnosť ochrany

Služba Cloudflare je jedným z gigantov na trhu služieb na uchovábanie obsahu. Na rozdiel od konkurenčných Akamau alebo Amazon Cloudfront sa však zameriava výhradne iba na tieto služby. Počtom serverov je menší ako Akamai, ale väčší ako Amazon Cloudfront, na rozdiel od konkurencie je geograficky rozmiestnený po celom svete. Systém Cloudflare poskytuje možnosť klientovi použiť priamo jeho doménu, kedy je možnosť DNS záznamy smerovať na servery Cloudflare a tak eliminujú v Cloudflare potrebu riešenia reverznej proxy. Ďalej poskytuje klientom aj SSL certifikát zdarma. Klienti si potom môžu nastaviť automatické smerovanie na HTTPS a nastavuje sa to priamo v službe.



Obrázok 5 Nastavenie SSL certifikátu.
Zdroj: Vlastné spracovanie

Služba cloudflare taktiež poskytuje dobrú ochranu voči útokom DDoS, čo sa preukázalo už v minulosti, kedy odolala útoku[10] na portál GITHUB až do 1,35 Tbps, čo je momentálne jeden z najväčších útokov na svete. Po pár dňoch ho prekonal svojou veľkosťou iný útok v sile 1,7 Tbps.[11]. Pre porovnanie, maximálny denný trafic celej Slovenskej republiky je na úrovni 232,2 Gbps, čo je zhruba 5,6 krát menší dátový tok oproti útoku na GITHUB.

Penetračný test webovej stránky MINS.SK

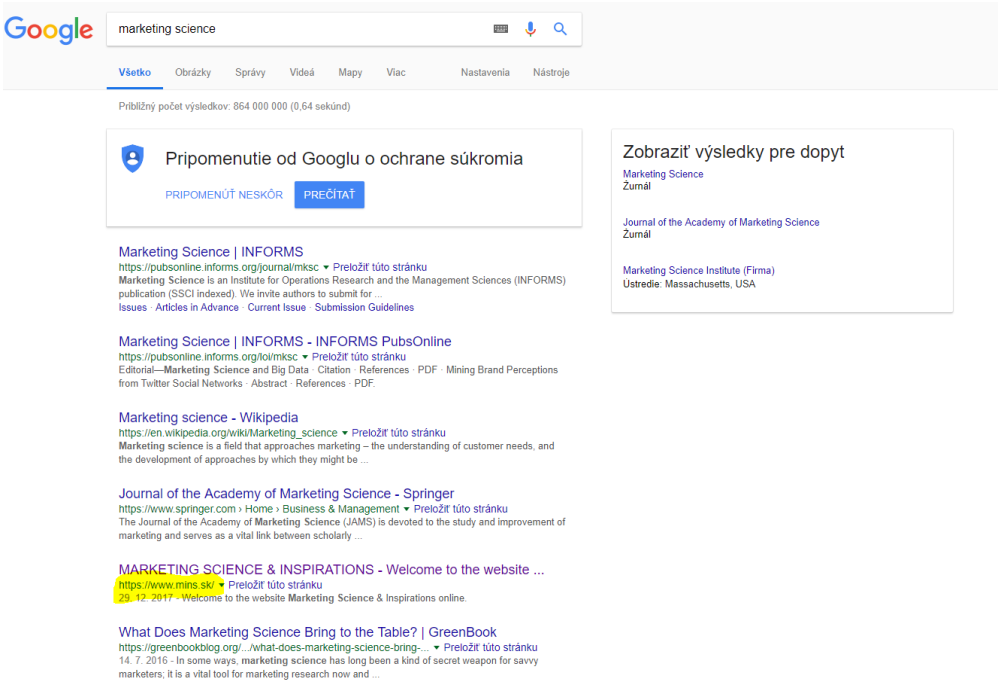
Webová stránka https://www.mins.sk je školským projektom vedeckého časopisu s riadne prideleným ISSN číslom 1338-7944. V praxi to znamená, že v zmysle platnej legislatívy musí časopis v elektronickej podobe byť neustále dostupný v nezmenenej podobe.

[10] KAN, B.M., MARCH 6, 2018 2:21PM EST, MARCH 6, 2018. Powerful DDoS Attack Sets New Record at 1.7 Tbps. In: *PCMAG* [online] [cit. 17.03.2018]. Dostupné na internete: https://www.pcmag.com/news/359693/powerful-ddos-attack-sets-new-record-at-1-7-tbps

[11] KUMAR, M. 1.7 Tbps DDoS Attack — Memcached UDP Reflections Set New Record. In: *The Hacker News* [online] [cit. 21.03.2018]. Dostupné na internete: https://thehackernews.com/2018/03/ddos-attack-memcached.html

Tlačená verzia časopisu sa vydáva ako prvá, následne sa jednotlivé články a príspevky zadávajú do webovej podoby.

Po optimalizácii kódu stránky na technológiu WORDPRESS a SEO optimalizácii celej štruktúry webovej stránky sa posunula stránka MINS.SK vo vyhľadávači GOOGLE.COM na popredné miesta, najmä po zadaní vyhľadávacích výrazov marketing a science, kedy z 864 miliónov indexovaných stránok s danými výrazmi sa nachádza stránka na 5 mieste. Tento jav však spôsobuje sekundárne problémy, kedy návštevnosť zobrazení stránok presiahla hodnotu 750 tisíc zobrazení za 6 mesiacov. Množstvo zobrazení je však bez identifikácie prehliadača, čo implikuje, že ide o boty za účelom indexácie obsahu alebo ide o automatizovaný útok za účelom napríklad SQL injection útoku.

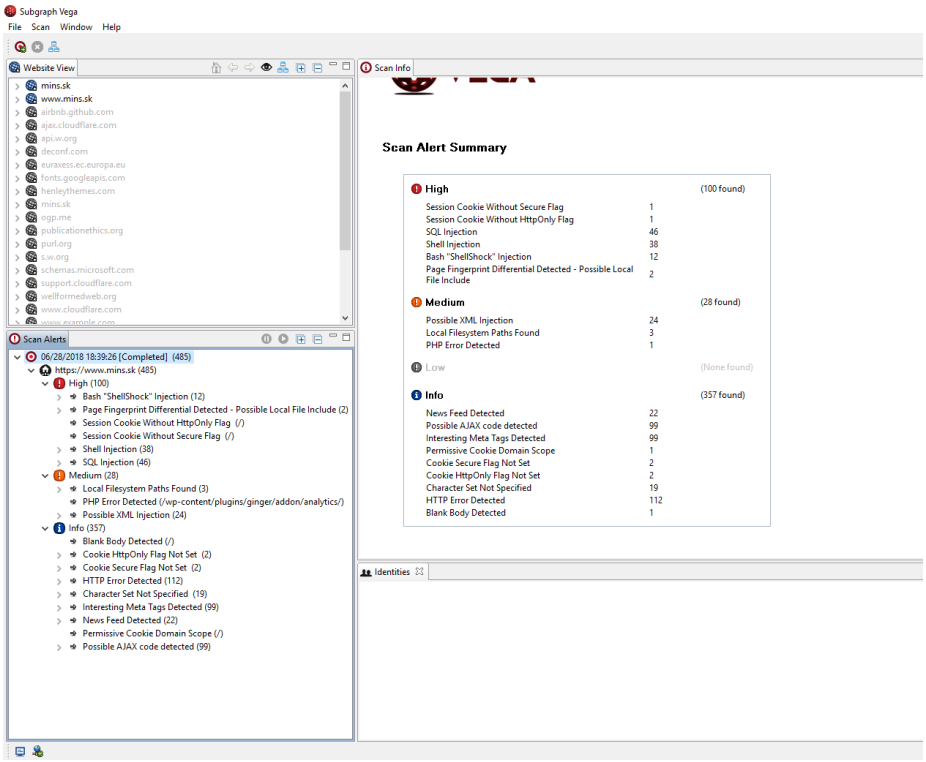


Obrázok 6 Výsledok vyhľadávania v google.com.
Zdroj: Vlastné spracovanie

Vyhodnotenie bezpečnosti stránky MINS.SK

Vyhodnotenie bezpečnosti webovej stránky je možné previesť viacerými spôsobmi. V zmysle fungovania etického hackingu vo svete je vhodné pridržiavať sa niektorej skupiny oficiálne združenej v organizácii etických hackerov. Jednou z najvýznamnejších je OWASP - Open Web Application Security Project. V rámci projektu OWASP existuje špecifická edícia KALI Linux, špecificky navrhnutého operačného systému na báze DEBIAN Linux. Táto edícia však obsahuje množstvo nástrojov vhodných pre prácu etického hackera. Jedným z nástrojov je aj VEGA SUBGRAPH, špeciálne navrhnutý nástroj na automatizované testovanie webových aplikácií. Tento nástroj je pravidelne aktualizovaný tak, aby pre testovanie zraniteľností stiahol zoznam známych zraniteľností webových aplikácií. Tým by malo byť docielené stavu, že testovaná webová stránka bude testovaná vo veľkom rozsahu na známe zraniteľnosti tak, akoby ju testoval prípadný útočník. Aktualizácia však neznamená, že budú otestované úplne všetky zraniteľnosti a všetky typy zraniteľností. Na otestovanie WORDPRESS webových aplikácií existujú ešte dva nástroje. Jeden je špecificky navrhnutý iba pre WORDPRESS aplikácie, využíva úplne špecifické zraniteľnosti zamerané na tzv. PLUG-IN a THEMES, ktoré sú zväčša programované tretími stranami a ktoré obsahujú najčastejšie zraniteľnosti. Druhou aplikáciou je tzv. BRUTE FORCE aplikácia zameraná na BRUTE FORCE ATTACK, teda hádanie hesiel

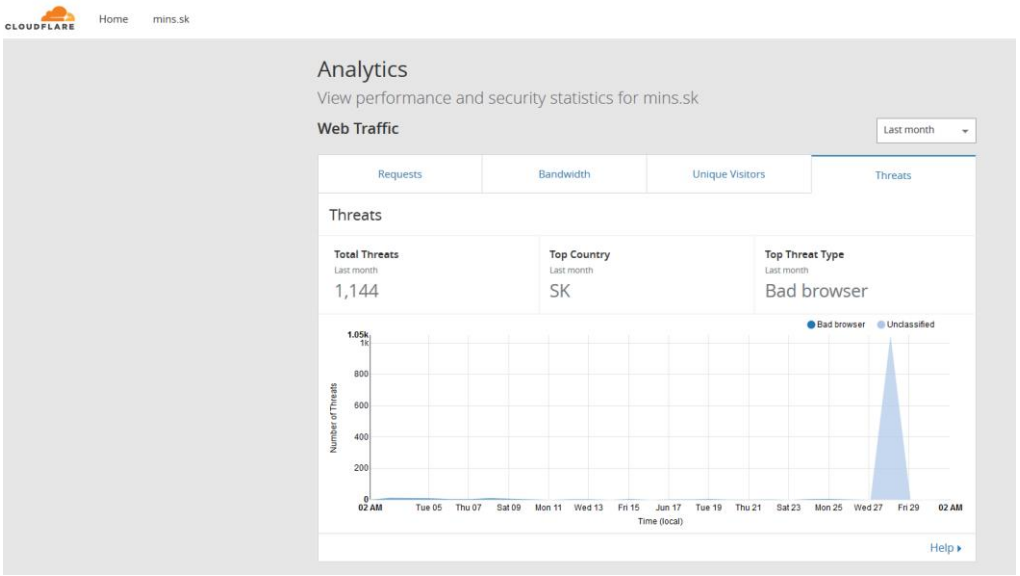
silou za pomoci slovníkov výrazov. Bezpečnosť by sa dala otestovať ešte niekoľkými ďalšími aplikáciami, tie však už nie sú automatizované a ich využitie si vyžaduje množstvo času.



Obrázok 7 VEGA - výsledok testovania stránky MINS.SK.
Zdroj: Vlastné spracovanie

Testovanie nástrojom VEGA zabralo časovo zhruba 1 hodinu 45 minút a výsledkom bolo 100 HIGH DANGEROUS zraniteľností, pričom stránka bola aktualizovaná na najnovšiu aktualizáciu, ktorá riešila závažné bezpečnostné zraniteľnosti.

Po prezretí štatistiky CLOUDFLARE sa dá vyhodnotiť, že ten za posledných 30 dní automaticky eliminoval 1144 útokov na stránku.



Obrázok 8 Cloudflare štatistika útokov.
Zdroj: Vlastné spracovanie

Záver

Zabezpečenie webových stránok je v súčasnej dobe nutnosťou. Spoliehať sa iba na štandardné zabezpečenie zo strany prevádzkovateľa technickej časti webového servera je nedostatočné. Ako je spomenuté vyššie, početnosť a sila útokov na webové aplikácie sa zvyšujú. Je preto potrebné nájsť adekvátne nástroje na elimináciu bezpečnostných rizík. Jedným z vyššie spomenutých nástrojov je aj využitie CDN CLOUDFLARE.COM, ktorý dokáže efektívne chrániť webové stránky pred útokmi typu DDoS. Okrem toho je ale potrebné spraviť si obraz o bezpečnosti vlastných webových stránok napríklad pomocou nástrojov etických hackerov ako je VEGA. V kombinácii s ďalšími procesmi tak je možné primerane zabezpečiť webové aplikácie pred neželanými útokmi.

Zoznam použitej literatúry:

ENDORF, C. F. *Detekce a prevence počítačového útoku*. [s.l.]: Grada Publishing a.s., 2005. Google-Books-ID: AWYduASeDlEC. ISBN 978-80-247-1035-8.

HOLCR, K. et al. *Policajné vedy : úvod do teórie a metodológie*. Praha: Aleš Čeněk, 2011. ISBN ISBN 9788073803292.

KAN, By Michael, MARCH 6, 2018 2:21PM EST, MARCH 6, 2018. Powerful DDoS Attack Sets New Record at 1.7 Tbps. In: *PCMAG* [online] [cit. 17.03.2018]. Dostupné na internete: https://www.pcmag.com/news/359693/powerful-ddos-attack-sets-new-record-at-1-7-tbps

KRYVINSKA, N. Building consistent formal specification for the service enterprise agility foundation. In: *Journal of Service Science Research* [online]. 2012, roč. 4, č. 2, s. 235-269. ISSN 2093-0720, 2093-0739. DOI: 10.1007/s12927-012-0010-5

KRYVINSKA, N. et al. A Methodology for the Enterprise Information and Communication Infrastructure Design Process. In: TAKIZAWA, Makoto, BAROLLI, Leonard, ENOKIDO, Tomoya. eds. *Network-Based Information Systems* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, zv. 5186, s. 303-312 [cit. 16.05.2016]. ISBN 978-3-540-85692-4. Dostupné na internete: http://link.springer.com/10.1007/978-3-540-85693-1_32

KUMAR, M. 1.7 Tbps DDoS Attack — Memcached UDP Reflections Set New Record. In: *The Hacker News* [online] [cit. 21.03.2018]. Dostupné na internete: https://thehackernews.com/2018/03/ddos-attack-memcached.html

MARKETINGER.SK. LOAD-BALANCING. In: *Sectec.sk* [online] [cit. 08.04.2018]. Dostupné na internete: https://www.sectec.sk/bezpecnost/load-balancing

PAWERA, R. *Manažment európskej bezpečnosti*. [s.l.]: Eurounion, 2005.

Charakteristika a význam slova sniffing. In: [cit. 08.04.2018]. Dostupné na internete: http://pdf.truni.sk/e-ucebnice/sips/data/bc638bc8-8616-450f-b4f0-872a9c835cfa.html?ownapi=1

IDS. In: [cit. 08.04.2018]. Dostupné na internete: http://www.cs.vsb.cz/grygarek/SPS/projekty0405/IDS/ids.html#deleni

Kešovací návod pro autory webu a webmastery. In: [cit. 08.04.2018]. Dostupné na internete: https://www.jakpsatweb.cz/clanky/caching-tutorial-czech-translation.html

Najlepšie webhostingové spoločnosti v kategórii Služby DDoS ochrany – rok 2018. In: *HostAdvice* [online] [cit. 18.02.2018]. Dostupné na internete: https://sk.hostadvice.com/hosting-companies/ddos-protection/

Slovensko čelí masívnym DDOS útokom hackerov. In: *Pravda.sk* [online] [cit. 01.07.2018]. Dostupné na internete: https://spravy.pravda.sk/ekonomika/clanok/473027-slovensko-celi-masivnym-ddos-utokom-hackerov/

Kontaktné údaje:

Ing. Jaroslav Vojtechovský, PhD.
Fakulta managementu Univerzity Komenského v Bratislave

Odbojárov 10
82005 Bratislava
jaroslav.vojtechovsky@fm.uniba.sk

PhDr. Peter Veselý, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Odbojárov 10
82005 Bratislava
Thomson Reuters Researcher ID: H-5695-2017
ORCID ID: 0000-0002-7857-6355
Scopus Author ID: 57195951243
peter.vesely@fm.uniba.sk

Anonymizácia komunikácie zmenou IP adresy ako metóda bezpečného prehliadania internetu

Štefan Zachar

Abstrakt:
Autor príspevku má v úmysle vysvetliť problematiku anonymity na internete za účelom bezpečného prehliadania WEBu. V rámci príspevku objasňuje princíp fungovania komunikácie Internetových prehliadačov so servermi a možné hrozby. Ďalej autor uvádza metódy skrývania IP adresy používateľa ako spôsob skrytia identity.
Kľúčové slová:
anonymita, proxy server, VPN, HTTP, HTTPS, TOR,

Abstract:
Author of this article intends to explain the issue of anonymity on the internet for the purpose of safe WEB browsing. The article describes principles of the communication between internet browsers and servers and possible threats. Further, the author gives methods of changing IP addresses for the purpose of hidding identity of the user.
Key words:
anonymity, proxy server, VPN, HTTP, HTTPS, TOR,

Úvod

S rozvojom internetu úzko súvisí aj rozvoj a rozsah služieb, ktoré ponúka. Čoraz častejšie sa stretávame s informáciami, o sledovaní užívateľov, zneužívaní osobných údajov, či o obchodovaní s nimi. Používatelia sa mnohokrát pred sledovaním bránia využívaním anonymizačných metód, služieb či aplikácií. Samozrejme aj v týchto prípadoch má minca dve strany. V povedomí verejnosti je anonymné pripojenie na internet chápané skôr negatívne hlavne kvôli Darknetu (alebo DarkWEBu)[1], ktorý je tvorený v anonymnými sieťami ako je napríklad onion network (TOR[2]), či I2P[3]. Anonymný spôsob pripojenia však nevyužívajú len osoby páchajúce kriminálnu činnosť, ale aj osoby, ktoré anonymitou chránia seba, či svojich blízkych. Sú to napríklad investigatívni reportéri, disidenti, politicky prenasledovaní občania diktátorských režimov, či používatelia, ktorí nechcú byť sledovaní vládnymi inštitúciami, či poskytovateľmi elektronických služieb.

Spôsoby prenosu údajov na WEBe

Byť online a využívať služby internetu znamená výmenu dát medzi používateľovým zariadením (PC, notebook, tablet, smartphone...) a serverom z ktorého získavame požadované údaje. V súčasnosti väčšina serverov poskytuje bezpečné HTTPS (HyperText Transfer Protocol Secure) pripojenie namiesto staršieho HTTP[4] (HyperText Transfer Protocol).

HTTP je protokol zabezpečujúci prenos html dokumentov medzi klientom a serverom. Tento protokol nevyužíva žiadne šifrovanie, teda jeho dátový tok medzi klientom a serverom je zobraziteľný a čitateľný pre akékoľvek zariadenie na počítačovej sieti cez ktoré je dátový tok smerovaný. Nakoľko sa zobrazujú jednotlivé príkazy, ako aj obsah html dokumentov, pre potenciálneho útočníka nie je problém zistiť aké stránky používateľ navštevuje.

[1] Darknet – počítačová sieť ktorá je súčasťou hlbokého WEBu. Jej obsah má prevažne nelegálny charakter. Dostupné na internete: https://www.thedarkwebsites.com/

[2] The Onion Router – názov projektu a zároveň celej siete založenej na princípe viacerých bezpečnostných vrstiev – odtiaľ názov onion (cibuľa) dostupné na https://www.torproject.org/docs/faq#WhyCalledTor.

[3] I2P – anonymná sieť typu peer to peer v ktorej sú si všetky uzly navzájom anonymné.

[4] Network Working Group Hypertext Transfer Protocol -- HTTP/1.1 1999, 175 s. dostupné na internete http://www.ietf.org/rfc/rfc2616.txt.

Na komunikáciu využíva HTTP protokol príkazy (metódy) ktoré môžu byť útočníkom použité na prienik do systému. Sú to napríklad metódy:

- **GET** ktorou žiada protokol o zaslanie informácií zadaním presnej adresy.
- **POST** podobne ako GET ale obsahuje aj dáta na vyplnenie formulára (vloženie nových dát).
- **PUT** podobne ako POST ale upravuje uložené dáta.
- **HEAD** podobne ako get, no vyžiadaná je len hlavička html dokumentu obsahujúca metadáta.

Ďalším prvkom komunikácie sú stavové kódy, ktoré používateľa, respektíve používateľom používaný internetový prehliadač informujú o stave vykonania jednotlivých metód. Bežný používateľ sa stretne len s niektorými z nich, ostatné sú skryté v komunikácii medzi klientovým prehliadačom a serverom. Najznámejšie stavové kódy, s ktorým sa môže používateľ stretnúť sú:

- **401 - Not Authorised** – vyžaduje sa autorizácia používateľa
- **404 – Not Found** - požadovaná stránka nebola nájdená,
- **407 - Proxy Authentication Required** – požadované prihlásenie sa na proxy server
- **408 - Request Timeout** – vypršal čas na zadanie požiadavky

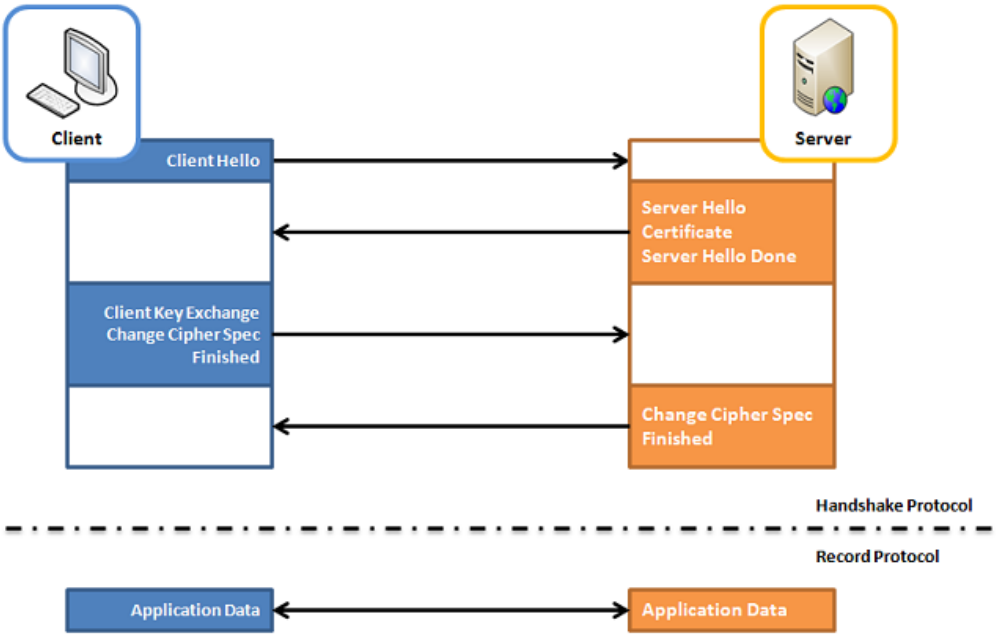
HTTPS je zabezpečená forma protokolu HTTP. Na zabezpečenie sa využíva šifrovanie TSL (Transport Layer Security) alebo SSL (Secure Socket Layer). Ide o rozšírenie protokolu o bezpečnostnú vrstvu. Komunikácia medzi klientom a serverom (Obrázok 1) pri využití SSL prebieha nasledovne[5]:

- Klient (internetový prehliadač) sa pripojí na server (WEB stránku) a požiada ho aby sa identifikoval.
- Server odošle späť kópiu svojho SSL certifikátu spolu s verejným kľúčom (public key).
- Klient porovná certifikát so zoznamom certifikátov a skontroluje jeho platnosť. Ak je certifikát platný, vytvorí a zašifruje kľúč na spojenie (symetric session key) s použitím verejného kľúča servera a pošle ho serveru.
- Server dešifruje kľúč na spojenie prostredníctvom svojho privátneho kľúča a pošle klientovi potvrdenie zašifrované kľúčom na spojenie pre potvrdenie začatia zašifrovaného spojenia.
- Od tohto momentu klient aj server šifrujú prenášané dáta prostredníctvom kľúča na spojenie

Takýto typ pripojenia je dostatočne odolný voči jednoduchšej verzii útoku nazývaného **„Man in the middle[6]“** (človek v strede) čo je najčastejšie používaný útok pri nezabezpečenom HTTP. Pri tomto type útoku útočník sleduje prenášané dáta. Podmienkou je, aby dáta prúdili cez útočníkove zariadenie – odtiaľ je aj názov muž v strede. Útočníkovi stačí byť v tej istej sieti ako používateľ a nakonfigurovať svoje zariadenie na prijímanie všetkých paketov, nie len paketov jemu určených. Výpisom paketov konkrétnej IP adresy potom môže sledovať komunikáciu medzi klientom (používateľom) a serverom. V prípade HTTP protokolu vidí všetky údaje ako surový text, s ktorým možno ďalej pracovať, no pri použití HTTPS protokolu je tento text zašifrovaný a tým pádom nečitateľný. Aj v tomto prípade je síce možné použiť útok Man in the middle, avšak je to podstatne komplikovanejšie, nakoľko by útočník musel odchytiť prvé pakety komunikácie ktoré obsahujú šifrovacie kľúče a nahradiť ich vlastným kľúčom. Riešením je výmena kľúčov iným komunikačným kanálom, alebo ich kontrola hash funkciou.

[5] An Introduction to Mutual SSL Authentication. Dostupné na internete: https://www.codeproject.com/Articles/326574/An-Introduction-to-Mutual-SSL-Authentication

[6] What is a Man In The Middle attack? Dostupné na internete: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html



Obrázok 1 SSL nadviazanie komunikácie klient - server
Zdroj: https://www.codeproject.com/KB/IP/326574/1WaySSL.png

Princíp anonymizácie

Používaním protokolu HTTPS síce zamedzíme útočníkovi aby prečítal naše údaje, no nezamedzíme mu v sledovaní našej IP adresy ako aj IP adries serverov. To to nie je častokrát žiadúce, nakoľko z našej verejnej IP adresy je možné zistiť nášho poskytovateľa internetu a našu približnú polohu. Rovnako vie zistiť polohu serveru a účel, kvôli ktorému sa naň používateľ pripája (banka, obchod, chat, email a podobne). S týmito informáciami vie ďalej pracovať a použiť ich ako doplňujúce informácie pri sofistikovanom útoku napríklad pomocou sociálneho inžinierstva. Skrytie, alebo výmena IP adresy je kľúčovým úkonom pri snahe byť na WEBe anonymný. Túto úlohu čiastočne spĺňajú IP Masquerading alebo NAT inštalované v linuxových internetových bránach alebo routeroch. Ďalšou možnosťou je využitie proxy servera, VPN, alebo čoraz častejšie využívaného TOR.

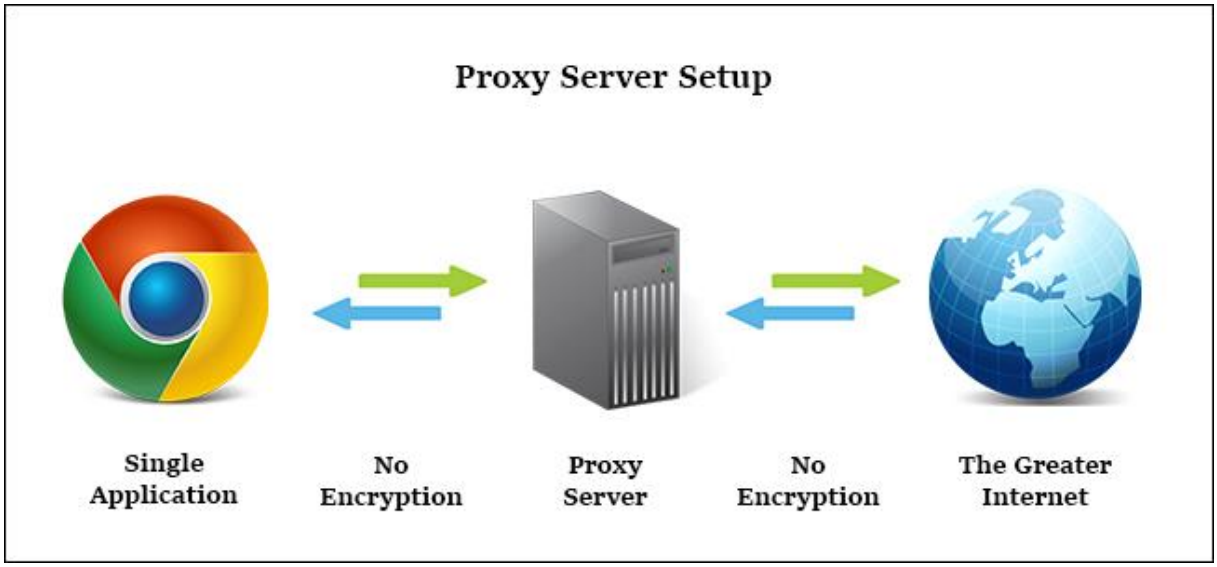
Nástroje a metódy anonymizácie

IP masquerading a NAT (Network address translation) - je spôsob akým počítačová sieť maskuje IP adresy počítačov v nej obsiahnutých. Často sa využíva na prístup počítačov z počítačovej siete na internet kde vystupujú pod jednou verejnou IP adresou. Zvonka siete to teda vyzerá, ako by bol na sieť pripojený len jeden počítač.

Proxy[7] – pripojenie cez proxy server znamená, že používateľ celú svoju komunikáciu s internetom presmeruje cez jeden prístupový bod, ktorý zmení jeho IP adresu. Celá komunikácia je bez využitia šifrovania. Pôvodne boli proxy servery využívané prioritne na komunikáciu internetového prehliadača s internetom, no je možné ich nastaviť aj pre iné služby siete. Nie je to však využívané tak často ako VPN pripojenie, ktoré je na túto úlohu predurčené. Často je proxy server využívaný v sieťach podnikov a organizácií ako bezpečnostný prvok na riadenie prístupu k internetu a súčasne aj intranetu. Správca siete vie takýmto spôsobom zabezpečiť:

[7] What's the Difference Between a VPN and a Proxy? Dostupné na internete: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/

- Riadený prístup k internetovým zdrojom a službám,
- Obmedzenie prístupu na nežiadúce stránky internetu, prípadne povolenie len vybraných stránok internetu,
- Zabezpečenie centralizácie prístupu z internetu do intranetu,
- Sledovanie správania jednotlivých užívateľov a ich prístupov na internet.



Obrázok 2 Prístup na internet cez proxy server
Zdroj: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/

Poznáme viac typov proxy serverov a síce HTTP, HTTPS, SOCKS[8] (Socket Secure) alebo WEB proxy. Prvé tri spomínané vyžadujú pre svoju činnosť konfiguráciu internetového prehliadača v ktorom nastavíme adresu a port využívaného proxy serveru.

HTTP a HTTPS proxy pracujú na úrovni týchto protokolov, to znamená, že prenášajú len údaje použiteľné pre internetový prehliadač.

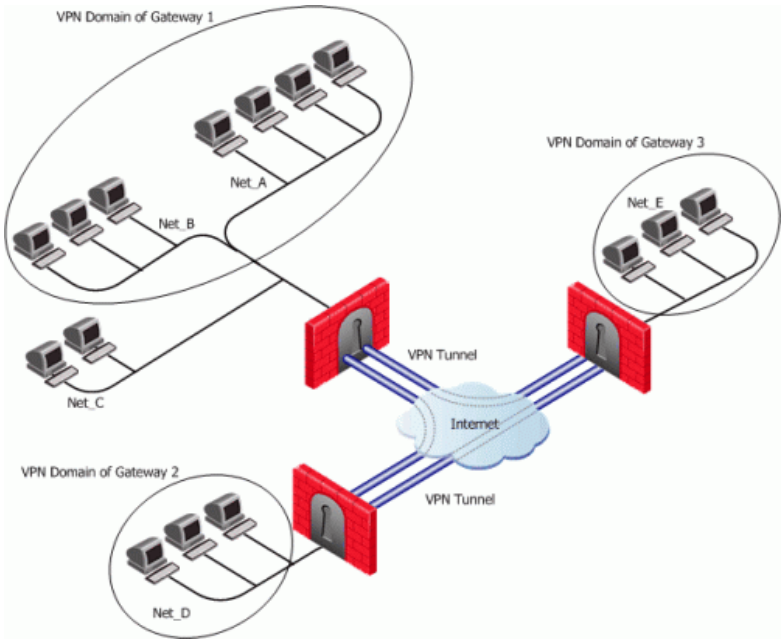
SOCKS pracuje na nižšej úrovni a vie spracovať aj UDP (User Datagram Protocol) čo mu dáva väčšie možnosti využitia.

WEB proxy je služba proxy serveru prístupná prostredníctvom internetovej stránky. Užívateľ na WEB proxy stránku vloží požadovanú URL a tá mu je následne zobrazená. Takéto proxy servery figurujú na internete buď to ako voľné verzie ale so zobrazovaním reklám, alebo platené verzie bez reklám. Ďalšími obmedzeniami voľných verzií môže byť počet otvorených okien na jednu IP, nedostupnosť niektorých stránok, prípadne nižšia rýchlosť.

VPN[9] – rozširuje možnosti lokálnej siete. Pôvodne bol vytvorený na prepojenie viacerých lokálnych sietí. Typickým príkladom sú organizácie, ktoré nemajú len jedno sídlo a vyžadujú, aby všetky pobočky mali prístup k spoločným zdieľaným zdrojom a službám. Za

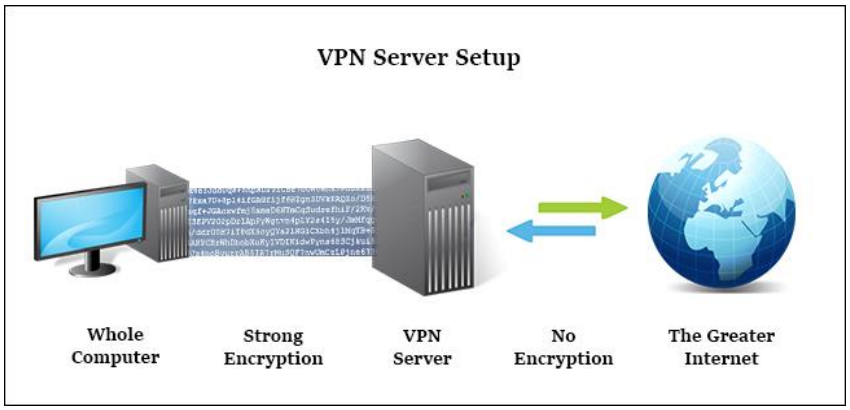
[8] The Ultimate Proxy Server Guide & How It Differs From a VPN odsek Types of Proxy Server Dostupné na internete: https://www.bestvpn.com/proxy-server/
[9] What's the Difference Between a VPN and a Proxy? Dostupné na internete: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/

týmto účelom je vytvorené tunelové spojenie medzi jednotlivými sieťami prechádzajúce cez internet.



Obrázok 3 Prepojenie sietí prostredníctvom VPN
Zdroj: https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/34609.gif

Ďalšou možnosťou je využitie VPN na bezpečné surfovanie. V tomto prípade sa klient pripojí šifrovaným spojením na VPN server a ďalej na internet už pokračuje nešifrovane avšak s IP adresou VPN serveru. Je to vhodné napríklad pri využívaní verejných WiFi hot spotov kedy sa prostredníctvom hot spotu pripojíme na VPN server vo vlastnej domácej sieti, ktorú považujeme za bezpečnú. Z tohto bodu môžeme využívať služby internetu ako by sme sedeli za domácim počítačom.



Obrázok 4 VPN server – klient komunikácia
Zdroj: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/

TOR – je anonymná sieť, s možnosťou prístupu na bežný internet. Pracuje na podobnom princípe ako VPN, avšak je omnoho sofistikovanejšia. V sieti TOR nie je vytvárané len jedno šifrované tunelové spojenie, ale hneď niekoľko za sebou, pričom každý z bodov pozná len predchádzajúci a nasledujúci bod (systém vrstiev), čím je zabezpečené, že poskytovateľ požadovanej WEB stránky alebo služby nevie z akej počiatočnej IP prišla požiadavka. Sieť TOR je zložená zo vstupných, prechodových a výstupných bodov. Dáta v sieti TOR sú

šifrované až do výstupného bodu, z ktorého vychádzajú v nešifrovanej podobe. Sieť TOR poskytuje pomerne vysokú mieru anonymity.

Okrem vyššie uvedených aplikácií, či služieb samozrejme existujú aj ďalšie (I2P, Freenet, OpenVPN a podobne), ktoré pracujú na podobných princípoch alebo vytvárajú separátnu anonymnú sieť.

Problematika deanonymizácie

Využívanie anonymných prístupov na internet je síce jednoduché, no pri nedodržaní niektorých zásad pre anonymné prehliadanie WEBu môže stratiť na efektivite. Problémom je deanonymizácia klienta pri používaní:

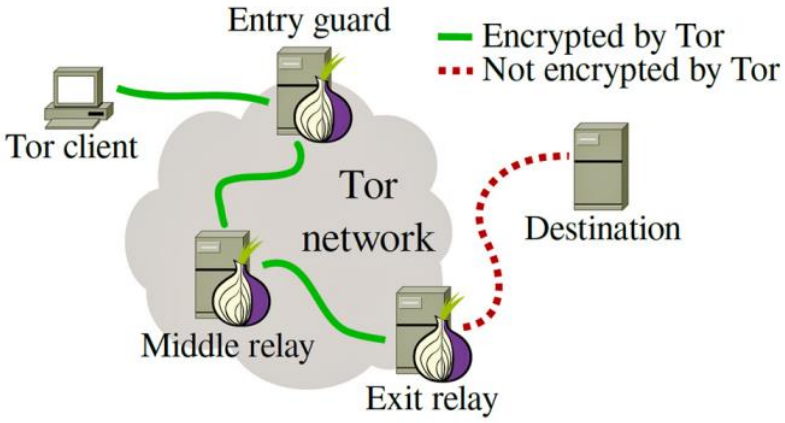
- cookies,
- spúšťaní neoverených skriptov Java,
- Adobe - Flash obsahu,
- otváraní dokumentov s povolením makier,
- inštalovaní neoverených zásuvných modulov či rozšírení prehliadača,
- prihlasovaní sa na stránky služieb, ktoré overujú identitu používateľa.

V internetových prehliadačoch sa bežne ukladajú cookies, spúšťajú sa skripty Java, prehráva obsah Adobe - Flash alebo si používateľ doinštaluje rozšírenie či zásuvný modul, ktorý má zjednodušiť, alebo spríjemniť prácu s prehliadačom. Používanie spomenutých prvkov môže narušiť koncepciu anonymného prehliadania WEBu. Ich používanie môže odkrývať identitu používateľa, a to aj v prípade že sú použité nástroje a metódy anonymizácie. Napríklad pri povolení ukladania cookies počas anonymného prehliadania je síce spojenie anonymné, no pri jeho vypnutí a náhodnej návšteve WEBu ktorý je pôvodcom cookies môže dôjsť ku korelácii aktivity, spárovaniu IP adries s touto aktivitou a tým nechcenému odhaleniu identity. Ďalším problémom, je spúšťanie akýchkoľvek skriptov, makier, či neoverených zásuvných modulov a rozšírení. Tieto môžu na pozadí svojej činnosti prečítať používateľovu skutočnú IP adresu, prípadne topológiu celej privátnej siete a prostredníctvom používateľom vytvoreného anonymného spojenia tieto zistenia oznámiť pôvodcovi skriptu či programu.

V súvislosti s uvedeným je pri anonymnom prehliadaní používateľom odporúčané:

- využívanie overených anonymizačných služieb či aplikácií[10],
- aplikácie spúšťané v sandboxe
- používať internetové prehliadače upravované so zameraním na vyššiu bezpečnosť a súkromie, prípadne vyhradiť si jeden z prehliadačov len na anonymné spojenia,
- mazanie cookies po každom pripojení, prípadne ich úplné zakázanie,
- vyhýbanie sa inštalácii neoverených doplnkov a zásuvných modulov,
- obmedzenie prihlasovania sa do bežne využívaných služieb internetu (WEB-mail, sociálne siete, dátové úložiská) na minimum.

[10] Napríklad niektoré zo súčasných antivírusových programov majú internetový anonymizér ako platenú službu. Ďalšou možnosťou je využitie voľne dostupných programov spravovaných veľkou komunitou užívateľov ako napríklad sieť TOR, I2P či Freenet.



Obrázok 5 Tok dát prostredníctvom siete TOR
Zdroj: https://vpn-services.bestreviews.net/best-vpns-for-tor/

Záver

Anonymita, je súčasťou dnešného internetu a to bez ohľadu na účel, kvôli ktorému sa používatelia snažia byť anonymní. Používateľ si v prvom rade musí uvedomiť, za akým účelom chce využívať anonymné pripojenie. Napríklad pri využívaní sociálnych sietí, či bežných WEB-mail služieb je použitie anonymizácie sporné[11], nakoľko už prístupom na sociálne siete používateľ odkrýva svoju identitu a zo strany sociálnych sietí sú takéto pripojenia často blokované alebo majú obmedzené služby. Legitímnosť anonymizácie je v rukách používateľov. Tá závisí od účelu využívania anonymného pripojenia a rovnako aj od miesta[12] využívania. Ako príklad by sme mohli uviesť Čínsku ľudovodemokratickú republiku, ktorá pri pripojení na Internet aplikuje takzvaný „The Great Firewall of China[13]“, ktorý okrem blokovania vybraných WEB stránok, dohľadu na DNS a cenzúry blokuje všetky VPN pripojenia. Podobne odporcovia režimu v KĽDR využívajú anonymné metódy komunikácie so svetom za hranicami svojho štátu. V domácom prostredí môžu anonymitu využívať napríklad firmy, ktoré sa takýmto bezpečným pripojením bránia pred priemyselnou špionážou, prípadne nekalými praktikami konkurencie. Rovnako, v oblasti žurnalistiky je pre investigatívnych reportérov a ich zdroje bezpečnejšie využívať zabezpečené anonymné pripojenia na internet.

Zoznam použitej literatúry:

Štandardizačné dokumenty na internete:
Network Working Group *Hypertext Transfer Protocol -- HTTP/1.1,* 1999, 175 s. Dostupné na internete http://www.ietf.org/rfc/rfc2616.txt
Network Working Group *The Secure Sockets Layer (SSL) Protocol Version 3.0,* 2011, 65 s. Dostupné na internete: https://tools.ietf.org/html/rfc6101
Odborné články na internete:
PALME J. *Anonymity on the Internet.*

[11] Výnimku v tomto prípade tvorí pripájanie sa na internet z voľne dostupných WiFi Hot Spotov prostredníctvom VPN do vlastnej zabezpečenej siete. V tomto prípade sa dá skôr hovoriť o využívaní bezpečného tunelového spojenia ako o anonymizácii, nakoľko sa využíva verejná IP adresa vlastnej siete.

[12] Anonymné využívanie internetu v krajinách ktoré porušujú ľudské práva môže byť miestnymi bezpečnostnými orgánmi chápané ako priestupok či trestný čin.

[13] How It Works: Great Firewall of China. Dostupné na internete: https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475

Dostupné na internete: https://people.dsv.su.se/~jpalme/society/anonymity.pdf
EKLUND E., ESSEN E., JONSSON F., JOHANSSON M. *To be or not to be on the internet: unpacking online anonymity*, SIRG Research Reports 2018 24 s. Dostupné na internete: http://www.sirg.se/wp-content/uploads/2013/12/SIRR2018_1.pdf
Článok na internete:
Why is it called TOR.
Dostupné na internete: *https://www.torproject.org/docs/faq#WhyCalledTor*
What is „The Dark WEB". Dostupné na internete: https://www.thedarkwebsites.com/
An Introduction to Mutual SSL Authentication.
Dostupné na internete: https://www.codeproject.com/Articles/326574/An-Introduction-to-Mutual-SSL-Authentication
What is a Man In The Middle attack?
Dostupné na internete: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
What's the Difference Between a VPN and a Proxy?
Dostupné na internete: https://www.howtogeek.com/247190/whats-the-difference-between-a-vpn-and-a-proxy/
The Ultimate Proxy Server Guide & How It Differs From a VPN odsek Types of Proxy Server.
Dostupné na internete: https://www.bestvpn.com/proxy-server/
How It Works: Great Firewall of China.
Dostupné na internete: https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475

Kontaktné údaje:
Mgr. Štefan Zachar
Katedra informatiky a manažmentu
Akadémia PZ v Bratislave
stefan.zachar@minv.sk
stefan.zachar@akademiapz.sk

Zhodnotenie konferenie a prijatie záverov

Možno konštatovať, že vytýčené ciele vedeckej konferencie s medzinárodnou účasťou **„Aktuálne výzvy prevencie počítačovej kriminality“**, ktorá sa realizovala ako súčasť projektu prevencie počítačovej kriminality *„Buď bezpečný“*, sa podarilo naplniť aj vzhľadom na rozličnosť prístupov venujúcich sa tejto problematike.

V rámci jednotlivých bodov programu konferencie išlo prioritne o riešenie nižšie uvedených otázok, ku ktorým boli prijaté konkrétne závery:

JUDr. Miroslav Brvnišťan, PhD. zo spoločnosti BMSEC ako manažér projektu „Buď bezpečný“ bližšie predstavil účastníkom konferencie uvedený projekt. Vysvetlil jeho ciele, ako aj prínos pre prax. Ide hlavne o vytváranie bezpečnostného povedomia prostredníctvom on-line vzdelávania, interaktívnych kurzov a výučbových aktivít dostupných pre každého. Vyzval prítomných na aktívne sa zapojenie do prieskumu, ktorý je súčasťou projektu. Pozri: www.budbezpecny.sk

Závery:
- prevencia v oblasti počítačovej kriminality je oblasťou, ktorá je relatívne nová, je potrebné vypracovať postupy prevencie, ktoré budú zodpovedať kybernetickému prostrediu a jeho dynamike,
- vzdelávanie a primerané bezpečnostné povedomie koncových používateľov je základným predpokladom bezpečnosti kybernetického prostredia,
- zavedenie využívania moderných a atraktívnych prostriedkov a nástrojov.

JUDr. Veronika Marková, PhD., vedúca KTP A PZ v Bratislave sa vo svojom vystúpení venovala trestno-právnym aspektom počítačovej kriminality. Poukázala na nedostatočné a absentujúce ustanovenia týkajúce sa počítačovej/ kybernetickej kriminality a nutnosť ich doplnenia.

Závery:
- terminologická nejednotnosť v oblasti (počítačová verzus kybernetická kriminalita),
- absentujúca metodika pre OČvTK,
- potreba zefektívnenia postupov OČvTK, štandardné postupy a procesy sú neefektívne,
- vzniká tlak na zmeny v trestnoprávnej úprave problematiky.

Mgr. Stanislav Španko, riaditeľ odboru počítačovej kriminality ÚKP PPZ venoval svoju pozornosť otázkam počítačovej kriminality v súvislosti s výkonom policajnej praxe, pričom poukázal na najčastejšie trestné činy, s ktorými sa stretávajú príslušníci PZ zaradení na tomto odbore.

Závery:
- nárast počítačových incidentov, ktoré majú potenciál naplniť znaky skutkovej podstaty trestného činu,
- budovanie odbornosti príslušníkov PZ,
- potreba zabezpečiť vzdelávanie príslušníkov PZ,
- technické a odborné vybavenie,
- potreba zmien v postupoch a prístupoch polície v oblasti počítačovej kriminality.

Zástupca **spoločnosti Corpus Solutions** prezentoval pohľad nezávislej odbornej spoločnosti na možnosti vyšetrovania a dokumentovania kybernetickej kriminality orgánmi

činnými v trestnom konaní s dôrazom na rolu príslušníkov Policajného zboru pri boji s kriminalitou v kybernetickom prostredí.

Závery:
- pomalosť a neefektívnosť zaužívaných postupov OČvTK,
- medzinárodný charakter počítačovej kriminality verzus uplatňovanie národných pravidiel
- absencia pravidiel pre koncových užívateľov,
- OČvTK ako súčasť bezpečnosti kybernetického prostredia.

Iný pohľad na riešenú tému priniesol **Michal Dragan,** ktorý sa venoval sociálnym sieťam a rizikám prinášajúcich ich využívanie. Načrtol otázky krádeží kybernetických identít a zneužívania verejne dostupných dát, ako aj riziká spojené so zverejňovaním informácií o svojom súkromí vo virtuálnom priestore, pričom uviedol aj viaceré praktické príklady. Dôležitým bodom príspevku bolo prezentovanie vlastnej skúsenosti s týmto typom nelegálnej činnosti s dôrazom na pripomenutie skutočnosti, že útočníkovi stačí pár informácií, pretože ľudia si neuvedomujú riziká sociálnych sietí.

Závery:
- nárast rôznych incidentov týkajúcich sa prostredia sociálnych sietí a nepripravenosť OČvTK efektívne reagovať,
- dôležitosť správneho a efektívneho zaistenia dôkazov,
- potreba vzdelávania OČvTK,
- chýbajúce metodika pre PZ a občana týkajúca sa postupov pri oznamovaní a dokumentovaní trestnej činnosti, najmä spôsob, miesto a postup oznámenia.

Mgr. Rastislav Janota, zástupca riaditeľa SK-CERT a predseda výboru pre kybernetickú bezpečnosť Bezpečnostnej rady SR účastníkom konferencie priblížil tvorbu a obsah Zákona o kybernetickej bezpečnosti, ktorého účinnosť je 1. 4. 2018.

Závery:
- zákon o kybernetickej bezpečnosti sa nezaoberá priamo bezpečnosťou občana,
- oznámenie o bezpečnostnom incidente nezakladá povinnosť pre NBÚ oznámiť uvedené OČvTK,
- zákon o kybernetickej bezpečnosti vo vzťahu k OČvTK nezaviedol nič nové,
- bezpečnosť kybernetického prostredia a občana nie je v kompetencii Policajného zboru.

Téme budovania proaktívneho bezpečnostného dohľadu na úrovni štátnej inštitúcie sa venoval zástupca **spoločnost Fidelis Cybersecurity** Jan Rydval, ktorý v nadväznosti na túto prednášku realizoval workshop.

Závery:
- monitorovanie bezpečnosti kybernetického prostredia a hodnotenie bezpečnostných incidentov ako predpoklad bezpečnosti,
- využitie moderných technológií (umelá inteligencia) pri analyzovaní bezpečnostných incidentov,
- potreba úzkej spolupráce medzi súkromným a verejným sektorom.

Vystúpenie **Ing. Mareka Laššáka**, vedúceho oddelenia analýzy dát OPSKA KEÚ PZ P PZ MV SR zaujalo účastníkov tým, že mali možnosť viac sa dozvedieť o digitálnej identite v kontexte počítačovej kriminality.

Závery:
- digitálna identita ako základ dokumentovania kybernetickej kriminality,
- rozpracovanie postupov a medód na efektívne zaisťovanie dôkazov, vrátane technického a technologického zázemia,
- nárast požiadaviek na odbornosť a vzdelávanie OČvTK.

Rokovanie konferencie svojim vystúpením obohatil **Mgr. Bc. Tomáš Trúsik** zo spoločnosti. ProtoWay, ktorý svoju pozornosť venoval problematike stanovenia výšky škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov. Prínosom jeho príspevku bolo prezentovanie vlastného návrhu vzorca výpočtu škôd, ktorý doteraz v praxi absentuje.

Závery:
- spôsobená škoda a jej hodnotenie a výpočet ako dôležitá súčasť trestného konania,
- chýbajúca metodológia pre vyčíslenie škody.

PhDr. Peter Veselý, PhD. MBA vo svojom vystúpení dotvoril tému prevencie počítačovej kriminality prostredníctvom etického hackingu.

Závery:
- etický hacking ako možná súčasť testovania kybernetickej bezpečnosti,
- chýbajúce legislatívne vymedzenie.

Praktický príklad testovania organizácie prostredníctvom phishingu ponúkol **Ing. Henrich Slezák.** Na tomto základe je možné overiť neopatrné až nezodpovedné správanie sa užívateľov v prostredí internetu, a tým následne upozorniť testovaných na nebezpečenstvo otvárania neoverených e-mailov a webových adries.

Závery:
- jednoduchosť útokov a relatívna vysoká zraniteľnosť koncových užívateľov,
- ľudský faktor ako základné bezpečnostné riziko v oblasti kybernetickej bezpečnosti,
- potreba neustáleho vzdelávania.

V poobedňajších hodinách sa uskutočnil workshop vedený odborníkmi zo spoločnosti Fidelis Cybersecurity, počas ktorého došlo k interaktívnej komunikácii s publikom a k praktickým ukážkam systému Security Operations Center na detekovanie, efektívne vyšetrovanie a eliminovanie bezpečnostných incidentov.

* * *

Je zrejmé, že nárastom využívania moderných informačných a komunikačných systémov (počítače, mobily, tablety) a **rastúcou informatizáciou spoločnosti a štátu počítačová kriminalita predstavuje čoraz väčiu hrozbu** pre koncových používateľov **a ochranu ich osobných údajov, citlivých dát a súkromia**. **Latentnosť počítačovej kriminality** predstavuje výrazný faktor ovplyvňujúci celkový stav tejto problematiky v spoločnosti priamo súvisiaci s úrovňou bezpečnostného povedomia koncových užívateľov. Ochrana a zvyšovanie bezpečnosti samotných informačných systémov a poskytovaných on-line služieb sú takisto priamo závislé od koncových užívateľov. Ľudský faktor, ako bezpečnostné riziko, predstavuje čoraz dôležitejší aspekt bezpečnosti počítačového prostredia.

Za prínosné považujeme, že sa podarilo sprostredkovať názory verejného sektora, súkromného sektora a akademickej obce na spoločnú tému - možnosti prevencie páchania trestnej činnosti v kybernetickom prostredí. Práve takáto spolupráca bude podľa nášho názoru

kľúčovou pri riešení problematiky kybernetickej bezpečnosti, vrátane rozvoja oblasti prevencie.

Prevencia a možnosti prevencie v kybernetickom prostredí poukazujú na potrebu redefinovania zaužívaných postupov a vypracovania nových. Hodnotenie bezpečnosti kybernetického prostredia nadobúda nové charakteristiky. Bezpečnostný incident ako základný faktor posudzovania bezpečnosti kybernetického prostredia (počet, intenzita, dôsledky) sú všeobecne uznané, a to najmä odborníkmi na IT bezpečnosť. Dôsledky bezpečnostných incidentov sú analyzované a hodnotené, prijímajú sa rôzne opatrenia na ich predchádzanie.

Práve vzťah bezpečnostného incidentu a jeho postavenie v kontexte bezpečnosti občana v kybernetickom prostredí sa ukazuje ako určujúcim pre činnosť OČvTK. Teoreticky vzaté, každý bezpečnostný incident (vírus, malwér, phishingový mail, DDoS útok a pod.) má potenciál naplniť znaky skutkovej podstaty trestného činu. Od zaregistrovania bezpečnostného incidentu po naplnenie znakov skutkovej podstaty trestného činu môže uplynúť veľmi malý alebo naopak relatívne dlhý čas. Je potrebné tomu prispôsobiť celé spektrum nástrojov a postupov, vrátane vzdelávania koncových užívateľov počítačových systémov.

Štandardné postupy OČvTK sú v oblasti počítačovej kriminality neefektívne, vznikali pre potreby materiálneho sveta. Od oznámenia trestného činu podľa Trestného poriadku po započatie základných úkonov a zaistenie stôp a dôkazov uplynie dlhý čas, ktorý priamo ovplyvní možnosti objasnenia. To je pravdepodobne aj jeden z faktorov, ktoré odrádzajú občanov od oznamovania počítačovej kriminality kompetentným orgánom, čím uvedený stav prispieva k vysokej latentnosti. Je potrebné zmeniť zaužívané postupy OČvTK.

Prevenciu bezpečnostných incidentov je zároveň možno považovať za súčasť prevencii trestnej činnosti v kybernetickom prostredí. Využívanie už zavedených nástrojov pochádzajúcich z oblasti informačnej bezpečnosti pre oblasť prevencie počítačovej kriminality sa javí ako vhodný začiatok cesty, ktorá bude definovať všeobecné rámce v tejto oblasti. Samozrejmosťou je ich postupné rozpracúvanie a neustále prispôsobovanie aktuálnej bezpečnostnej situácii.

Za jednoznačný prínos konferencie je možné považovať skutočnosť, že téma bola prezentovaná tak z hľadiska trestnoprávneho, ako aj špecificky policajno-odborného, kriminalisticko-expertízneho, ale aj vyslovene technického, resp. technologického. Bolo zaujímavé získať pohľad na oblasť prevencie počítačovej kriminality komplexne z rôznych uhlov pohľadu. Na druhej strane je zrejmé, že väčšina účastníkov vedeckej konferencie sa zhodla na nutnosti úpravy príslušnej legislatívy, keďže v súčasnej dobe takáto nie je komplexná. Následkom uvedeného stavu vzniká vysoká miera latencie, neochota občanov nahlasovať takúto formu kriminality (najmä z dôvodu nízkeho povedomia o spôsoboch oznamovania - komu a ako je potrebné takéto konanie oznámiť), čím vzhľadom na narastajúci počet používateľov počítačových systémov narastá aj motivácia páchateľov dopúšťať sa kybernetickej kriminality.

Z prezentovaného vyplýva, že konferencia priniesla mnohé zaujímavé pohľady na možnosti ochrany pred takýmito nelegálnym konaním, či už za pomoci využitia špeciálnych systémov, etického hackingu alebo testovania a školenia zamestnancov dotknutých organizácií.

* * *

Jedným z konečných výsledkov konferencie je základný súbor zistení a odporúčaní, týkajúcich bezpečnosti v kybernetickom prostredí a postupu v prípade podozrenia zo spáchania počítačovej kriminality.

Dôvodom bolo hľadanie odpovede na otázky: **Som občan, vznikla mi v dôsledku kybernetického útoku škoda, čo mám robiť? Ako mám postupovať?** Nájdenie odpovedí

však nebolo jednoduché. Je zrejmé, že v tejto oblasti bude potrebné uskutočniť ešte množstvo práce. Výsledkom je súbor základných téz a všeobecných odporúčaní, ktoré nie sú konečné. Je potrebné ich rozpracovať a zaviesť do aplikačnej praxe.

Občan:
1. Zodpovedá za svoje konanie a bezpečnosť v kybernetickom prostredí.
2. Pozná a dodržiava základné bezpečnostné pravidlá, chápe podstatu bezpečnosti v kybernetickom prostredí.
3. Pozná základné bezpečnostné riziká a vie im predchádzať.
4. V prípade zistenia bezpečnostného incidentu a podozrenia z počítačového trestného činu vie, ako postupovať a na koho sa obrátiť.
5. V prípade podozrenia, že sa stal obeťou kybernetickej kriminality, je potrebné, aby si zodpovedal nasledujúce otázky: *Čo sa mi stalo? Viem to popísať a zdokladovať? Vznikla mi škoda? Viem odhadnúť a preukázať škodu?*
6. Ovláda postup po technickej stránke, t.j. ako vypnúť počítač, nepoužívať, odpojiť sieťový kábel a pod.

Pri oznámení podozrenia zo spáchania počítačovej trestnej činnosti platia všeobecné pravidlá Trestného poriadku, ako pri oznamovaní inej trestnej činnosti.

Policajný zbor:
1. Postupuje efektívne - od prijatia oznámenia, cez vypočutie, zaistenie dôkazov, vyčíslenia škody a odhalenie páchateľa.
2. Vytvorenie podmienok, pravidiel a postupov na nahlasovanie počítačovej kriminality.
3. Minimalizuje dopady vyplývajúce z dokumentovania počítačovej kriminality na občana.
4. V podmienkach PZ je potrebné sa zaoberať vypracovaním komplexného prístupu k oblastiam počítačovej kriminality a kybernetickej bezpečnosti, vrátane vzdelávania príslušníkov PZ.

RECENZNÝ POSUDOK

NA ZBORNÍK Z VEDECKEJ KONFERENCIE S MEDZINÁRODNOU ÚČASŤOU

KATEDRY INFORMATIKY A MANAŽMENTU AKADÉMIE POLICAJNÉHO ZBORU V BRATISLAVE

Názov recenzovaného zborníka

AKTUÁLNE VÝZVY PREVENCIE POČÍTAČOVEJ KRIMINALITY

Recenzent: RNDr. Eva Kostrecová, PhD.
Fakulta managementu Univerzity Komenského v Bratislave
Katedra informačných systémov

Autori recenzovaného výstupu: autorský kolektív aktívnych účastníkov vedeckej konferencie s medzinárodnou účasťou.

Vzhľadom na súčasný stav vysokej elektronizácie implikovanej vo všetkých oblastiach ekonomických, spoločensko-politických i sociálnych aktivít, ktoré sú každodenne vykonávané obyvateľmi našej planéty, rastie aj podiel počítačovej kriminality na celkovej kriminalite. Tento novodobý fenomén si vyžaduje zvýšenie úsilia v prevencii a v boji proti nemu, k čomu rozhodne prispela aj vysoko aktuálna problematika „Aktuálne výzvy prevencie počítačovej kriminality“ riešená v rámci vedeckej konferencie s medzinárodnou účasťou, ktorá sa konala na Akadémii Policajného zboru (APZ) v Bratislave dňa 21. marca 2018 pod záštitou rektorky APZ v Bratislave Dr. h. c. doc. JUDr. Lucie Kurilovskej, PhD. a s podporou Rady vlády SR pre prevenciu kriminality. Konferencia bola organizovaná v rámci realizácie projektu zameraného na prevenciu páchania počítačovej kriminality s názvom „Buď bezpečný“ a zborník z prezentovaných a predložených príspevkov zostavili JUDr. Matej Kostrec, PhD. (APZ) a Mgr. Jana Kuchtová (APZ).

Recenzovaný zborník je výstupom, ktorý je možné odporúčať ako odbornú publikáciu pre nadobudnutie nielen teoretických, metodických, odporúčacích, ale i praktických znalostí pre akademickú i odbornú verejnosť. Súčasne môže, v rámci prevencie, slúžiť aj pre podporu osvety a informovanosti širokej verejnosti v oblasti uplatňovania v súčasnosti veľmi aktuálneho nariadenia GDPR (General Data Protection Regulation), ktoré je nariadením EÚ, a ktorého aplikácia je zameraná na ochranu fyzických osôb v súvislosti so spracúvaním ich osobných údajov.

Po obsahovej stránke je možné v posudzovanom zborníku príspevky klasifikovať do štyroch nasledujúcich tematických blokov:

1. *Legislatívne a medzinárodné štandardy, teoretické východiská a možnosti prevencie a oznamovania prípadných podozrení z páchania počítačovej kriminality, resp. realizácie protiprávnych konaní a trestných činov v tejto oblasti* - v tomto bloku autori príspevkov erudovane prezentujú východiská legislatívnej prevencie počítačovej kriminality v SR, medzinárodné právne štandardy prijaté v SR pre túto oblasť, ale aj inštitúcie, kde je možné získať odbornú a právnu podporu alebo oznamovať kriminalitu páchanú v kybernetickom priestore.

2. *Metodika, nástroje a odporúčania* – odborníci z výskumu, akademickej pôdy i praxe v tomto bloku prezentujú metódy ako definovať bezpečnostné hrozby, ako získať znalosti o dátach spracúvaných v informačných systémoch a ako ich manažovať v rámci prevencie proti ich zneužitiu. V rámci tohto bloku sú v príspevkoch poskytnuté i odporúčania ako zvýšiť úroveň bezpečnosti elektronickej komunikácie i zachovania relevantného obsahu webových stránok.
3. *Výsledky prieskumov a štatistík* – príspevky v tomto tematickom bloku poskytujú v prehľadnej forme dáta nielen o vývoji informačnej bezpečnosti, ale i o dynamike vývoja počítačovej kriminality.
4. *Príklady z praxe* – najväčší počet príspevkov uvedených v zborníku je možné zaradiť práve do tohto bloku. Čitateľ zborníka sa tu dozvie ako aplikovať informačnú bezpečnosť v praxi, ako implementovať v organizácii ochranný systém pre detekciu podozrivých aktivít, ktoré predchádzajú počítačovému útoku, ako detegovať možnosť napadnutia počítača vydieračským typom softvéru, ako sa v praxi prejavujú niektoré formy sociálneho inžinierstva a ako prichádza k zneužívaniu osobných údajov, ale aj aké sú možnosti stanovenia výšky škôd po zneužití informačno-komunikačných zariadení pre páchanie trestnej činnosti.

Po formálnej stránke všetky príspevky uverejnené v predkladanom zborníku obsahujú všetky povinné náležitosti kladené na vedecké a odborné príspevky, sú logicky usporiadané a obsahovo vyvážené. Autori príspevkov založili jednotlivé prezentácie na svojich vedeckých i odborných skúsenostiach a špecifickú odbornú terminológiu sa snažili čo najzrozumiteľnejšie predstaviť tak, aby bola v logickom slede prístupná i pre odborné komunikačné potreby príslušníkov PZ pri vykonávaní každodenných policajných úloh a opatrení.

Záver:

Predkladaný zborník príspevkov prezentovaných v rámci vedeckej konferencie s medzinárodnou účasťou je možné, vzhľadom na vysokú odbornú úroveň všetkých príspevkov k pertraktovanej a veľmi aktuálnej problematike boja proti počítačovej kriminalite, považovať za kvalitný a prínosný publikačný výstup, ktorý bezpochyby zaplní určitú medzeru v knižničnom trhu v oblasti prevencie pred týmto špecifickým druhom kriminality. Samotná konferencia splnila očakávané ciele a po odbornej stránke dokonca kvalitou prevýšila očakávanú úroveň, pretože zborník z nej môže slúžiť nielen pre potreby aplikačnej praxe príslušníkov PZ a prípravy študentov APZ v oblasti kriminality, ale aj pre zvýšenie informovanosti a povedomia odbornej i laickej verejnosti o možných útokoch na počítačovú a komunikačnú infraštruktúru.

Na základe vyššie uvedených skutočností konštatujem, že zborník pod názvom **„Aktuálne výzvy prevencie počítačovej kriminality“** v predloženej podobe má všetky potrebné atribúty s vysokým potenciálom budúcej úspešnosti využitia aj pre aplikačnú prax a vzdelávacie kurzy, a preto **o d p o r ú č a m jeho schválenie a publikovanie v predloženom obsahu.**

V Bratislave, 20.7.2018

RNDr. Eva Kostrecová, PhD.

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 prevencie počítačovej kriminality**“ konanej dňa 21.3.2018

1. Aktuálnosť a prínos riešenej problematiky

Informačná bezpečnosť digitálneho priestoru, vrátane súvisiacich technických, programových a sieťových zariadení, ako aj zabezpečenie obsahu pred zničením alebo zneužitím, sú čoraz dôležitejšie pre správne fungovanie každého štátu. V súčasnej dobe je pozornosť zo strany Európskej komisie, ako aj štátnych orgánov a inštitúcií SR venovaná okrem iného aj zvýšeniu bezpečnosti a prevencii počítačovej kriminality v priestore internetu, prenosových sietí a informačných systémov zabezpečujúcich dostupnosť elektronických služieb nevyhnutných pre fungovanie spoločnosti. Z týchto dôvodov hodnotím Zborník príspevkov z vedeckej konferencie s názvom „Aktuálne výzvy prevencie počítačovej kriminality“ ako vysoko aktuálny.

Zborník je výsledkom vedeckej činnosti pracovníkov Akadémie PZ v Bratislave, Policejní akademie ČR v Prahe, odborníkov zaoberajúcich sa kybernetickou bezpečnosťou z viacerých slovenských univerzít, ako aj z odbornej praxe. Problematika kybernetickej bezpečnosti je v zborníku riešená z viacerých aspektov. Obsahuje 23 príspevkov zameraných na aspekty právne, technologické, sociálne, a prirodzene aj na dopady opatrení zabezpečujúce kybernetickú bezpečnosť v práci Policajného zboru.

2. Obsahová a formálna stránka zborníka

Významný prínos jednotlivých príspevkov a prípadné poznámky uvádzam v nasledujúcom texte posudku.

Príspevok Ľ. Baričičovej s názvom INFORMAČNÁ KOMPETENTNOSŤ V KONTEXTE AKTUÁLNYCH POTRIEB INFORMAČNEJ SPOLOČNOSTI na základe analýzy pozitívnych aj negatívnych dôsledkov budovania a postupnej implementácie prvkov informačnej spoločnosti rieši problematiku informačnej kompetentnosti policajných manažérov. Zdôrazňuje informačnú podstatu policajnej práce a možnosti nadobudnutia informačných kompetencií prostredníctvom vzdelávacej a vedeckej činnosti Katedry informatiky a manažmentu Akadémie PZ v Bratislave.

B. Beláňová vo svojom príspevku VÝVOJ INFORMAČNEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE – VÝSLEDKY PRIESKUMU 2006-2017 komparuje výsledky celoštátneho výskumu informačnej bezpečnosti v podnikoch pôsobiacich na Slovensku v rokoch 2006, 2008, 2012, 2015 a 2017, identifikuje najvážnejšie hrozby pre bezpečnosť informačných systémov, a poukazuje na závažné prekážky presadzovania bezpečnostnej politiky a bezpečnostných opatrení v oblasti IS/IT. Najväčšie rezervy identifikuje v oblasti malých a stredných podnikov, pre ktoré napadnutie alebo poškodenie ich vnútropodnikového informačného systému môže byť likvidačné.

M. Brvnišťan sa v príspevku s názvom KYBERNETICKÁ KRIMINALITA A MOŽNOSTI PREVENCIE zaoberá kybernetickou kriminalitou všeobecne, z pohľadu občana, ako aj z pohľadu legislatívy. Prezentuje postup činností pre občana v prípade, ak je

obeťou kybernetickej kriminality. Identifikuje ľudský faktor ako najväčšie bezpečnostné riziko a súčasne vzdelávanie a osvetu ako základ prevencie kybernetickej kriminality.

J. Demčáková v príspevku s názvom VYUŽITIE METÓD PRI DEFINOVANÍ BEZPEČNOSTNÝCH HROZIEB V OBLASTI INFORMAČNÝCH SYSTÉMOV rieši problematiku riadenia rizika a venuje sa predovšetkým metódam analýzy a riadenia rizík v oblasti IS/ IT. Podľa môjho názoru názov príspevku nevystihuje jeho obsah, preto navrhujem zmeniť názov, napr. na „Metódy riadenia rizika v oblasti bezpečnosti IT“ (alebo podobne). Po formálnej stránke je potrebné upraviť spôsob citovania podľa predpísanej šablóny.

Konkrétnu implementáciu systému na pasívnu detekciu narušenia kybernetickej bezpečnosti prezentujú vo svojom príspevku IMPLEMENTÁCIA IDS SYSTÉMU NETXMS.ORG V ORGANIZÁCII M. Greguš a P. Veselý. Systém poskytuje komplexnú správu udalostí a monitorovanie výkonu. Jeho výstupom sú upozornenia, hlásenia a grafy pre všetky vrstvy infraštruktúry IS/IT. Prínosom riešenia je zníženie nákladov na prevádzku bezpečnostného riešenia sieťovej prevádzky ako aj výrazné zvýšenie bezpečnosti IS/IT v organizácii.

ZNALOSTI INFORMAČNÍHO MANAGEMENTU – JEDEN Z NÁSTROJŮ PREVENCE POČÍTAČOVÉ KRIMINALITY zdôrazňuje vo svojom príspevku P. Jedinák. Ide predovšetkým o znalosti princípov informačných systémov, znalosti z oblasti ich ochrany a zabezpečenia. Základom sú však znalosti týkajúce riadenia a správy dát s cieľom ochrany dát, ktoré každý používateľ zálohuje vo svojom počítači.

M. Kelemen a J. Klátik vo svojom príspevku s názvom ZNALOSTNÁ ALIANCIA KYBERNETICKEJ BEZPEČNOSTI – KONZORCIUM PRE ODBORNÚ A PRÁVNU PODPORU NÁRODNÉHO KOMPETENČNÉHO CENTRA KYBERNETICKEJ BEZPEČNOSTI SR predstavili návrh znalostnej aliancie ako jedného zo stredísk kompetencií podporovaných EU s cieľom podnietiť vývoj a zavádzanie technológií v oblasti kybernetickej bezpečnosti.

Ďalším príspevkom je príspevok S. Kočišovej s názvom ONLINE PODNECOVANIE K TERORIZMU, ktorý je zameraný na právne otázky špecifikácie pojmov spojených s kybernetickou kriminalitou, kam patrí aj podnecovanie terorizmu prostredníctvom internetu. Autorka ďalej predstavuje projekt Clean IT navrhnutý holandským Ministerstvom bezpečnosti a spravodlivosti, ktorého výsledkom je súbor zásad a postupov s názvom „Zníženie využívania internetu na účely terorizmu“. V záverečnej časti sa venuje transpozícii smernice Európskeho parlamentu a Rady (EÚ) 2017/541 o boji proti terorizmu do právneho poriadku SR.

Legislatívou sa zaoberá aj autorka E. Kresl v príspevku s názvom VÝCHODISKÁ LEGISLATÍVNEJ PREVENCIE POČÍTAČOVEJ KRIMINALITY. Venuje sa základným pojmom, definíciám, princípom, dokumentom, inštitúciám a aktivitám, ktoré predstavujú východiská legislatívnej prevencie počítačovej kriminality v EÚ a na Slovensku. Prehľad dokumentov, inštitúcií a aktivít charakterizuje súčasné štádium budovania legislatívnej prevencie počítačovej kriminality v EÚ a na Slovensku.

Autori R. Kubička a O. Kubička v príspevku s názvom POČÍTAČOVÉ ÚDAJE V TRESTNOM KONANÍ riešia problematické otázky súvisiace s trestno-procesným postupom pri zisťovaní, zabezpečovaní a zaisťovaní počítačových údajov, napr. údajmi získanými z mobilných telefónov iných inteligentných zariadení, údajmi z elektronickej pošty a pod. Autori analyzujú názory na danú problematiku vyjadrené v rámci judikatúry a odbornej literatúry. Vysvetľujú technickú charakteristiku jednotlivých zariadení, v nadväznosti na ktorú zaujímajú stanovisko k obsahu pojmu počítačové údaje v zmysle § 90 Trestného poriadku.

J. Kuchtová v príspevku s názvom AKTUÁLNE TRENDY SÚVISIACE S VYUŽÍVANÍM MODERNÝCH TECHNOLÓGIÍ poukazuje na vybrané aktuálne trendy v oblasti IS/IT, prostredníctvom ktorých sa spracovávajú aj osobné a iné citlivé údaje. Tie sú častým predmetom útokov páchateľov kybernetickej kriminality. Ide predovšetkým o Internet

vecí (IoT) a inteligentné mestá. Autorka prezentuje aj reálne existujúce nebezpečenstvá a navrhuje odporúčania na zlepšenie súčasného stavu.

Autor M. Marcinek v príspevku MEDZINÁRODNÉ ŠTANDARDY KVALITY KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE sa zaoberá sa skupinou noriem ISO 27000 (ISO 27001 až ISO 27 799), predovšetkým normou ISO 27001, ktorá popisuje návrh a zavedenie SMIB (Systém manažérstva bezpečnosti informácií), ako modelu upravujúceho hodnotenie rizík a riadenie bezpečnosti informácií. Autor ďalej uvádza právne normy v SR, ako napr. Jednotku pre riešenie počítačových incidentov (CSIRT.SK) a Zákon o kybernetickej bezpečnosti 69/2018.

V. Marková sa v príspevku SÚČASNÝ STAV A VÝCHODISKÁ POČÍTAČOVEJ KRIMINALITY V PRÁVNOM PORIADKU SR venuje trestnoprávnym otázkam počítačovej kriminality, pričom uvádza vymedzenie základného pojmového aparátu vo vzťahu k počítačovej kriminalite, ako aj jej klasifikáciu. Podrobne sa venuje východiskám a dopadu medzinárodných dokumentov a právnych predpisov EU na súčasné znenie skutkových podstát trestných činov.

Príspevok R. Paweru a P. Veselého s názvom ZNEUŽÍVANIE OSOBNÝCH ÚDAJOV V PRAXI sa zaoberá analýzou modelov narušenia kybernetickej bezpečnosti za účelom zneužitia osobných údajov, analýzou vybraných bezpečnostných incidentov a návrhom primeraných opatrení za účelom zníženia rizika daných typov incidentov. Ďalej analyzuje prípadné dopady nariadenia GDPR a smernice ePrivacy na organizáciu.

Teoretickým a konceptuálnym vymedzením pojmu ransomware sa zaoberá M. Petrik v príspevku ÚVOD DO PROBLEMATIKY VYDIERAČSKÉHO SOFTVÉRU (RANSOMWARE). Popisuje procesy viažuce sa k ransomware útoku a techniky používané na šifrovanie alebo zamknutie zariadenia po úspešnom infikovaní. Analyzuje hlavné ciele, na ktoré útok mieri a spôsoby platby výkupného. Autor poukazuje aj na rozmáhanie sa trendu ransomware ako služby.

Príspevok P. Poláka a T. Trúsika MOŽNOSTI STANOVENIA VÝŠKY ŠKODY SPÔSOBENEJ NEOPRÁVNENÝMI ZÁSAHMI DO POČÍTAČOVÝCH SYSTÉMOV A PROGRAMOV je zameraný na všeobecné vysvetlenie pojmu škoda a výška škody spôsobenej počítačovými trestnými činmi, na analýzu typov neoprávnených zásahov do počítačových systémov a programov ako aj na predstavenie metód určenia škody spôsobenej neoprávnenými zásahmi do počítačových systémov a programov.

L. Réveszová sa v príspevku POČÍTAČOVÁ KRIMINALITA A JEJ DYNAMIKA VÝVOJA V ROKOCH 2014 – 2017 zameriava na zosumarizovanie teoretických poznatkov z oblasti počítačovej kriminality a na základe štatistických údajov mapuje reálnu dynamiku vývoja počítačovej kriminality v Slovenskej republike v rokoch 2014 – 2017.

Príspevok M. Širilovej s názvom SOCIÁLNE INŽINIERSTVO A PÁCHANIE TRESTNÉHO ČINU PODVODU V KONTEXTE POČÍTAČOVEJ KRIMINALITY je konkrétne zameraný na pharming a phishing ako vybrané formy sociálneho inžinierstva. Zdôrazňuje prepojenie medzi pharmingom a phishingom s trestným činom podvodu.

V. Šoltés a L. Mariš v príspevku MOŽNOSTI OZNAMOVANIA KRIMINALITY PÁCHANEJ V KYBERNETICKOM PRIESTORE BEZPEČNOSTNÝM ZLOŽKÁM analyzujú online platformy využívané v rôznych krajinách Európskej únie pre nahlasovanie kriminality páchanej predovšetkým v kybernetickom priestore. Závery príspevku môžu byť využité pri návrhu a implementácii podobného systému aj v podmienkach Slovenskej republiky.

Príspevok V. Šulca s názvom INFORMAČNÍ BEZPEČNOST A JEJÍ APLIKACE V PRAXI rieši problematiku bezpečnosti z pohľadu elektronického bankovníctva, na základe platnej legislatívy charakterizuje jednotlivé druhy trestných činov páchaných v kybernetickom priestore a poskytuje návod na bezpečné využívanie IT pre bežných používateľov.

P. Veselý a V. Karovič sa v príspevku ETICKÝ HACKING V ORGANIZÁCII V ZMYSLE SMERNICE O KYBERNETICKEJ BEZPEČNOSTI zameriavajú na praktické využitie znalostí z oblasti etického hackingu podľa metodiky OWASP v organizácii, predovšetkým v zmysle posúdenia kybernetickej bezpečnosti. Za bezpečný stav považujú stav, v ktorom sú siete a informačné systémy schopné odolávať konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb.

J. Vojtechovský a P. Veselý v príspevku ZABEZPEČENIE OCHRANY WEBOVÉHO SÍDLA PRED ÚTOKMI TYPU DDOS A INÝMI RIZIKAMI prezentujú praktické využitie služieb IDS, IPS a ochrany pred DDoS útokmi na webové sídla organizácie, mechanizmus fungovania load balancing webového sídla a cachovanie obsahu webového sídla.

Autor Š. Zachar v príspevku ANONYMIZÁCIA KOMUNIKÁCIE ZMENOU IP ADRESY AKO METÓDA BEZPEČNÉHO PREHLIADANIA INTERNETU vysvetľuje problematiku anonymity na internete za účelom bezpečného prehliadania WEBu. Súčasne objasňuje princíp fungovania komunikácie internetových prehliadačov so servermi a možné hrozby a uvádza metódy skrývania IP adresy používateľa ako spôsob skrytia identity.

3. Záver

Celkovo je možné Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou „Aktuálne výzvy prevencie počítačovej kriminality“ hodnotiť ako aktuálny a veľmi kvalitný publikačný výstup. Cenné je predovšetkým prezentovanie riešenej problematiky zo strany vedeckých pracovníkov z viacerých univerzít ako aj z odbornej praxe.

Keďže problematika počítačovej kriminality, prevencie a bezpečnosti 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 PREVENCIE POČÍTAČOVEJ KRIMINALITY“ po odstránení drobných nedostatkov má všetky potrebné atribúty, preto **o d p o r ú č a m** jeho schválenie a publikovanie.

V Bratislave, 13.8.2018 doc. Ing. Anna Hamranová, PhD.

Názov:	**Aktuálne výzvy prevencie počítačovej kriminality**
Vydala:	Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava
Pracovisko:	Katedra informatiky a manažmentu
Zostavili:	JUDr. Matej Kostrec, PhD. Mgr. Jana Kuchtová
Technická redakcia:	doc. Ing. Ľubica Baričičová, PhD. Mgr. Jana Kuchtová Mgr. Štefan Zachar
Recenzenti:	doc. Ing. Anna Hamranová, PhD. RNDr. Eva Kostrecová, PhD.
Formát:	B 5
Rozsah:	235 strán
Rok a poradie vydania:	2018, prvé

Za odbornú a jazykovú stránku príspevkov zodpovedajú autori.
Rukopis neprešiel jazykovou úpravou.

ISBN 978-80-8054-774-5
EAN 9788080547745