KYBERNETICKÁ KRIMINALITA A MOŽNOSTI PREVENCIE[1]

Miroslav BRVNIŠŤAN[2]

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.*

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*

I. 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

---

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

2 JUDr. Miroslav Brvnišťan, PhD., Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17, brvnistan@bmsec.sk.

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[3]. Jednou 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.

II. 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.

---

[3] 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.

Samotný pojem počítačová kriminalita nie je explicitne definovaný v Trestnom zákone[4] 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:

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

---

[4]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.

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 likvidácií 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 likvidácií 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[5]. Na nárast významu vzdelávania a budovania bezpečnostného povedomia zamestnancov (koncových užívateľov) poukazuje aj prieskum stavu informačnej bezpečnosti spracovaný Ministerstvom financií SR v roku 2013[6]. 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[7], 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[8] je zrejmé aj nasledovné:

---

[5] Pozri bližšie napr. Desiaty ročník Globálneho prieskumu spoločnosti Ernst & Young o informačnej bezpečnosti www.efocus.sk/images/archiv/file_1183_0.pdf.

6 Pozri www.informatizacia.sk/ext_dok-prieskum_ib_2013_-sk-en-/16943c

[7] Pozri bližšie http://recent-ecl.blogspot.fr/2012/07/cybercrime-new-eu-statistics.html:

8 Pozri bližšie https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

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

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.

III. 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[9]. 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.

III.A. 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”[10]. 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

---

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

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

k bezpečnosti, a zároveň budovanie dôvery vo vlastnú organizáciu"[11]. 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.

III.B. 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, 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,

---

[11] www.sansecurity.com, 2015

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”[12].

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[13]. 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[14].
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 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

---

12 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.

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

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

prípravy”[15]. Tým sa vytvárajú všeobecné rámce pre vytvorenie potrebných vzdelávacích programov a uceleného systému vzdelávania pre oblasť kybernetickej bezpečnosti.

III.C. 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.

---

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

IV. 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 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[16],
- 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.

Literatúra:

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, A PZ 2015, ISBN 978-80-8054-662-5, str. 76-83.

Brvnišťan, M.: Bezpečnostné povedomie v kontexte boja proti novodobým bezpečnostným hrozbám, In Zborník príspevkov z IX. medzinárodnej vedeckej konferencie v Banskej

[16] 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.

Bystrici 11. – 12. februára 2016, Fakulta politických vied a medzinárodných vzťahov UMB, 2016, ISBN 978-80-557-1093-8, str. 520-530.

STRÉMY, T. 2011. Počítačová kriminalita. In: DIANIŠKA, G. a kol. 2011. Kriminológia. Plzeň: Aleš Čeněk s.r.o., 2011, s. 245.

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, ISBN 978-80-554-1024-1, str. 36-43.

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. 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
Akčný plán kybernetickej obrany NATO (NATO Cyber Defence Action Plan), www.mosr.sk
Posilnená stratégia kybernetickej obrany NATO (Enhanced NATO Policy on Cyber Defence), 2014, www.mosr.sk
Stratégia kybernetickej bezpečnosti Európskej únie Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN (2013), www.mosr.sk
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
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.
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

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/