

EDUKATOR

NAJVEĆI STRUČNI INFORMATIVNI ČASOPIS

Godina 3, br. 4, august 2016. godine

ISSN 2303-5560-el. izd., ISSN 2303-5684-st. izd.

DIGITALNA FORENZIKA-MOBILNI TELEFON KAO IZVOR DIGITALNIH DOKAZA
NAJPOZNATIJE VRSTE CYBER KRIMINALA | ULOGA DNK ANALIZE



A large, detailed fingerprint watermark is overlaid on a background of binary code (0s and 1s). The fingerprint is oriented vertically, with its ridges and valleys corresponding to the binary digits. The background is a dark grey with the binary code in a lighter shade of grey.

CYBER
TERORIZAM

» PREVENCIJA NASILJA

» ZAVISNOST OD INTERNETA-
PREDRASUDE ILI REALNOST



IMPRESSIUM

Gl. i odgovorni urednik **doc.dr Hadžib Salkić**

Tehnički urednik: **Nermina Konjalić**

Naslovница: **Mr. sc Almira Salkić**

Redakcija: **doc. dr Hadžib Salkić, doc. dr Ibrahim Obhodaš, doc. dr Džemal Kulašin, doc. dr Jamila Jaganjac, mr. sc Almira Salkić, mr. sc Mahir Zajmović, mr. sc Adnan Pirić, Nermina Konjalić, BA, Dinka Šakić, BA.**

Recezenti: **prof. dr Lazo Roljić, prof. dr Branko Latinović, prof. dr Nedim Smailović, doc. dr Hadžib Salkić, doc. dr Ibrahim Obhodaš, doc. dr Džemal Kulašin, doc. dr Jamila Jaganjac**

SADRŽAJ

CYBER KRIMINAL

Dinka Šakić, BA

Sveučilište/Univerzitet „Vitez“, Vitez, BiH, dinka_91@hotmail.com

1

PHISHING KAO MANIFESTACIJA CYBER KRIMINALA

Doc. dr. Džemal Kulašin

Fakultet za menadžment i poslovnu ekonomiju, Kiseljak

6

ZAVISNOST OD INTERNETA-PREDRASUDE ILI REALNOST

Goran Blagojević, mr¹ i Goran Guska, MA²

¹MUP Republike Srpske, Uprava za policijsko obrazovanje - Banja Luka, RS-BiH, Doktorand na Fakultetu bezbednosti Univerzitet u Beogradu, e-mail:blagojevicgoran@yahoo.com

²MUP Republike Srpske, Uprava za policijsko obrazovanje - Banja Luka, RS-BiH, Doktorand na Pravnom fakultetu Univerzitet u Novom Sadu, e-mail: goranguska@gmail.com

12

CYBER SIGURNOST U EU ZEMLJAMA

Perenda Halid, perenda.halid@gmail.com

21

ODREDNICE EKSTERNALIZIRANIH PROBLEMI ADOLESCENATA U VIRTUELНОM OKRUŽENJU

Mr Edina Heldić-Smailagić

Visoka škola unutrašnjih poslova Banjaluka, edina_heldic@yahoo.com

27

NAČINI ZAŠTITE OD ZLONAMJERNOG SOFTWARE-A I NARUŠAVANJA SIGURNOSTI KORISNIČKIH PODATAKA

Jasmin Kahriman, BA

jasmin.kahriman@unvi.edu.ba

35

VRŠNJAČKO NASILJE NA INTERNETU

Mr. sci Musić Nijaz

41

NASILJE NA FEJSBUKU

Prof. dr Mile Matijević,

Fakultet pravnih nauka Univerziteta za poslovne studije Banja Luka

Aleksandar Miladinović, mr

Visoka škola unutrašnjih poslova Banja Luka

48

CYBER TERORIZAM - TERORISTIČKE AKTIVNOSTI UPOTREBOM RAČUNARSKIH MREŽA

Siniša Karanović, mr

57

КОНЦЕПТ САЈБЕР ОРУЖЈА У РАЧУНАРСКИМ И ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

МСц Небојша Иваниш дипл.инж.инф.

ИТ Вештац, Београд, Србија, nebojsaivanis@sezampro.rs

68

DIGITALNA FORENZIKA-MOBILNI TELEFON KAO IZVOR DIGITALNIH DOKAZA

Prof.dr Vojo Laković¹, Doc. dr Slobodan Simović², Mr Jovana Simović³

¹Univerzitet „Hercegovina“ Mostar-FDZMB

²Fakultet za diplomatiju i bezbednost-Beograd,Srbija, slobodandsimovic@gmail.com

³The Learning Academy UK, London ,Engleska, Operations director

82

NAJPOZNATIJE VRSTE CYBER KRIMINALA I NAJBOLJA ZAŠTITA OD NAVEDENIH NAPADA

Nehad Gašić, BA

Sveučilište/Univerzitet „VITEZ“ Vitez, nehad.gasic@unvi.edu.ba

91

IDENTIFIKACIJA I PREVENCIJA POJAVNIH OBLIKA NASILJA MEĐU DJECOM U SREDNJIM ŠKOLAMA NA PODRUČJU OPĆINE TRAVNIK

Mr Adnan Pirić¹, Mr Almira Salkić², Selim Hibić dipl krim³

¹Viši asistent Fakultet pravnih nauka - Sveučilišta/Univerziteta „Vitez“ u Vitezu

²Viši asistent Fakultet informacijskih tehnologija – Sveučilište/Univerzitet „Vitez“ u Vitezu

³Predsjednik udruženja kriminalista SBK/KSB Travnik

98

SAVREMENI OBLICI KOMPJUTERSKOG KRIMINALITETA I NJIHOVA PREVENCIJA

Snježana Radošević, Testing centar d.o.o Gradiška.

110

KRIMINALISTIČKO-FORENZIČKA OBRADA MJESTA IZVRŠENJA KRIVIČNOG DJELA – UVIĐAJ

Petar Đukić¹, Dr Borislav Đukić²

¹Visoka škola unutrašnjih poslova, Banja Luka, BiH, petar.djukic96@yahoo.com

²Visoka škola unutrašnjih poslova, Banja Luka, BiH, bobandjukic70@gmail.com

118

ULOGA DNK VJEŠTAČENJA U RASVJETLJAVANJU NAJTEŽIH OBLIKA NASILNIH DELIKATA

Mladen Vuković, mr

Doktorand na Pravnom Fakultetu, Univerzitet u Novom Sadu, zaposlen u MUP RS, Uprava za policijsko obrazovanje, Visoka škola Unutrašnjih poslova, mladen_vukovic1983@yahoo.com

124

PRAKTIČNA PRIMJENA KRIPTOGRAFIJE U SQL-U KAO NAČINA ZAŠTITE BAZE PODATAKA U SLUČAJU CYBER NAPADA

Mahir Zajmović¹, Hadžib Salkić², Haris Hamidović³

Fakultet informacijskih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez, BiH,
mahir.zajmovic@unvi.edu.ba

Fakultet informacijskih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez, BiH,
hadzib.salkic@unvi.edu.ba

Stalni sudski vještak IKT struke, Tuzla, Bosna i Hercegovina,
haris.hamidovic@ieee.org

129

VIJESTI IZ SVIJETA CYBER KRIMINALA I FORENZIKE

135

CYBER KRIMINAL

Dinka Šakić, BA

Sveučilište/Univerzitet „Vitez“, Vitez, BiH, dinka_91@hotmail.com

ABSTRACT: Napredovanjem kako razvoja, tako i korištenja informacionih tehnologija u svakodnevnom životu raste i cyber kriminal. U današnjem poslovanju je to relativno nov pojam i još uvijek predstavlja nepoznanicu prilikom susreta. Cyber kriminal susrećemo svakodnevno nebitno da li samo pretraživamo internet putem tražilice Ili plaćamo kreditnom karticom, jer htjeli mi to ili ne možemp postati žrtve cyber kriminala. U ovom radu biti će moguće pronaći neke oblike cyber kriminala, kao kako i na koji način je moguće da se zaštитimo od njih.

KLJUČNE RIJEČI: cyber kriminal, kreditne kartice, zaštićeni sistemi, sigurnost, zaštita.

UVOD

Ukoliko uzmem u obzir informacije koje možemo pronaći svakodnevno u medijima i drugim izvora informacija jasno je da je zapažen trend porasta cyber kriminala, kao i broj povratnika u ovo kazneno djelo. Prema Ministarstvu sigurnosti Bosne i Hercegovine djela koja se klasificiraju pod pojmom cyber kriminala su ometanje rada sistema i elektroničke obrade podataka, prevare na internetu, neovlašten pristup zaštićenom sistemu i mreži elektroničke obrade podataka, krivotvorene kreditnih i ostalih kartica bezgotovinskog načina plaćanja, posjedovanje i distribucija dječije pornografije, kaznena djela u vezi sa zloupotrebnama wireless mreža te društvenih mreža, kaznena djela povrede autorskih prava. Također, u Bosni i Hercegovini sve češća je pojava ekonomske špijunaže, širenja malware – a, neovlaštenog upada u zaštićene sisteme, krađe bankovnih kartica, a najčešća pojava je slučajeva koji se tiču internet prevare.

1. NEOVLAŠTENI UPAD U ZAŠTIĆENE SISTEME

Svaka kompanija ima svoje informacije koje su vrijedne i koje je potrebno zaštiti. Informacija se može pronaći u više različitih oblika. Danas je najčešći oblik informacije u elektronskom obliku, kao i informacije koje se mogu pronaći u pisanoj formi tj. odštampane na papir. Stoga, sigurnost informacionog sistema u kojem se nalaze informacije je neophodna kako bi kompanija mogla poslovati, kao i ostvarivati dobit. Kako bi očuvali informacije u informacionim sistemima potrebno je najprije osigurati povjerljivost što podrazmijeva da informaciju mogu samo koristiti ovlašteni korisnici. Također, potrebno je osigurati integritet i dostupnost, odnosno da je informacija tačna i kompletna i da je korištena od strane ovlaštenih korisnika. U današnjem poslovanju sve više se kompanije susreću sa računarskim virusima, hakovanjem, kao i DOS (Denial Of Service) napadima. Na informacioni sistem moguće je povezati se sa različitim lokacijama kroz telekomunikacione mreže i iz ovog razloga je povećana mogućnost napada na cijelu mrežu.

Napade je moguće organizovati i kroz bežičnu mrežu, jer ova mreža koristi radiotehnologiju i podložna je napadima iz razloga što je radiofrekvencije lako skenirati. Jako je bitno napomenuti da su telekomunikacione mreže jako osjetljive na pad softverskih i hardverskih sistema, neovlaštenu upotrebu od strane programera, kao i korisnika. Također, mogu biti ugrožene na različite načine kao što je napad hakera, DOS napadi, ubacivanje virusa u sistem, neovlašteno korištenje kao i još mnogo načina.

Malware, odnosno maliciozni softveri kao što su kompjuterski virusi najrasprostranjeniji su i najčešći oblik ugrožavanja informacionih sistema. Ukoliko se uzme u obzir način na koji funkcionišu i njihovu brzinu širenja, postaju najveća prijetnja informacionim sistemima. Jedan od primjera malware – a je kompjuterski virus, odnosno programi koji se pišu ili prave sa ciljem da prilikom izvršenja nanosi štetu određenom računaru na način da briše fajlove ili/i datoteke, da ih ošteti ili učini da padne cjelokupni sistem.

Sa obzirom na način brzine širenje ovih virusa, kao što je već pomenuto, moguće je da ukoliko se jedan od računara zarazi da se prenese i na druge putem mreže. Jedan od najčešćih načina prenošenja virusa je

preko e – mail poruka. Virus se može nalaziti u dodatku (attachment) mail – a i taj dodatak bude najčešće izvršni fajl.

Pokretanjem tog fajla virus se automatski aktivira i kupi informacije koje su prethodno napisane u tom virusu. Također, virus se sam replicira i šalje svim kontaktima koji su se nalazili u adresaru tog korisnika i funkcioniše isto kao na opisani način. Međutim, napredovanjem informacionih tehnologija, tako napreduju i virusi i više nije potrebno da bude dodatak mail – u, već je dovoljno da samo mail bude zaražen. Do sad pomenuto može se sprečavati na način da na računaru budu instalirani antivirusni programi kojih danas na tržištu ima jako mnogo. Neke od kompanije koje se bave razvojem i prodajom antivirusnih programa su: Norton, McAfee, Microsoft, Nord 32 itd. Bitno je napomenuti da antivirusni programi moraju biti update – ovani, jer se samo na ovaj način korisnici programa mogu biti sigurni da su zaštićeni od najnovijih virusa.

Slika 1: Logo Norton antivirusa



Izvor: <https://us.norton.com/>

1. ZLOUPOTREBA PLATNIH KARTICA

Globalna raspostranjenost platnih kartica, njihovo korištenje i dostupnost modernih tehnologija, učinili su da platne kartice budu jedna od meta napada. Najčešći oblici zlouotrebe platnih kartica su:

- zloupotreba ukradenih ili izgubljenih platnih kartica,
- zloupotreba neuručenih platnih kartica,
- zloupotreba i prevara od strane trgovaca,
- zloupotreba od strane korisnika,
- prikupljanje podataka za pravljenje lažne platne kartice,
- pravljenje i korištenje lažnih planih kartica,
- neovlaštena upotreba tuđe platne kartice.

Izdavaoc platnih kartica je predvio načine zloupotrebe i iz tog razloga je već pri samom preuzimanju kartice naznačio da je potrebno ukoliko dođe do gubitka ili krađe kartice prijaviti nestanak u roku od 24h. Do trenutka preuzimanja kartica, ta kartica je zaštićena pick up kodom koji se aktivira u trenutku preuzimanje od strane klijenta.

Nakon preuzimanja, kartica se štiti tako što na kartici ima ime i prezime osobe za koju je izdata kartica, kao i PIN kod koji je neophodan prilikom korištenja bankomata.

Zbog sigurnosti kartica i PIN kod nikada ne dolaze zajedno, niti ljudi koji rade na poslovima izrade nisu isti iz razloga da ne bi došlo do zloupotrebe. PIN se određuje pomoću računara, automatski se pakuje i dolazi na adresu klijenta i niko ne poznaje kod osim samog korisnika. Navedene mjere sigurnosti se moraju koristiti kako bi se izbjegla zloupotreba platnih kartica ili da se mogućnost zloupotrebe svede na najmanji nivo. Ove mjere također primjenjuju VISA, MASTER CARD, DINERS, kao i svoja interna pravila kako bi izbjegli eventualne mogućnosti zloupotrebe.

Kako ništa nije idealno tako i u ovom slučaju, zloupotreba se može javiti u postupku slanja pošiljke, odnosno platne kartice ili PIN koda poštom ili nekim drugim načinom, zatim kod proizvođača kartica itd. Sve ove uočene nepravilnosti potrebno je na vrijeme prijaviti da li izdavaocu kartice ili policiji zavisno od posljedica zloupotrebe.

Još jedan od načina zlouotrebe platnih kartica jeste da se na bankomate ugrađuje tzv. lažni čitač kartica na pravi čitač i kameru. Kamera se obično postavlja iznad bankomata na mjestu gdje je moguće vidjeti PIN kod prilikom upisivanja. Stoga je potrebno da prilikom korištenja bankomata obrati pažnja na bankomat, da li eventualno postoje kamere, kao i da prilikom upisivanja PIN koda zaštite drugom rukom kako se ne bi vidjelo šta se upisiva.

Jedan od načina da se prepozna bankomat koji ima skimmer uređaj jeste da taj bankomat ne učitava karticu. U većini slučajeva korisnici misle da bankomat ne radi i jednostavno odu samo do sljedećeg. Međutim, prilikom ubacivanja kartica je ostavila trag na skimming uređaju i u ovom slučaju korisnici mogu da imaju problem.

Slika 2: Izgled Visa kartice



Izvor: <https://usa.visa.com/partner-with-us/info-for-partners/info-for-small-business.html>

Sa rastom broja zloupotreba platnih kartica kompanije koje izdaju kartice pokušale su da pronađu jednostavno rješenje. To su uradile tako što su počele sa izdavanjem smart ili čip kartica. Te kartice funkcionišu na način da prilikom korištenja kartice, npr. podizanjem novca sa bankomata, nakon nekoliko minuta dobijete SMS poruku o korištenju kartice, kao i vrijeme i mjesto korištenja. Ukoliko vlasnik kartice nije bila osoba koja je koristila, onda jednostavno zna da je riječ o zloupotrebi kartice. Najbolji način zaštite platne kartice jeste da je uvijek na sigurnom mjestu, najbolje novčaniku, da PIN poznaje samo osoba koja je vlasnik, te da ne koristi sumnjive bankomate.

2. INTERNET PREVARA

Svi smo svjedoci kako se svakodnevno dešavaju razne internet prevare. Porastom broja korisnika interneta raste i broj prevara na internetu. Neke od njih su već pomenute kao što je neovlašten upad u razne sistemi, zatim slanjem virusa, kao i zloupotreba platnih kartica putem krađe informacije. Također, pored navedenih postoji još mnogo oblika internet prevare, a neke od njih su:

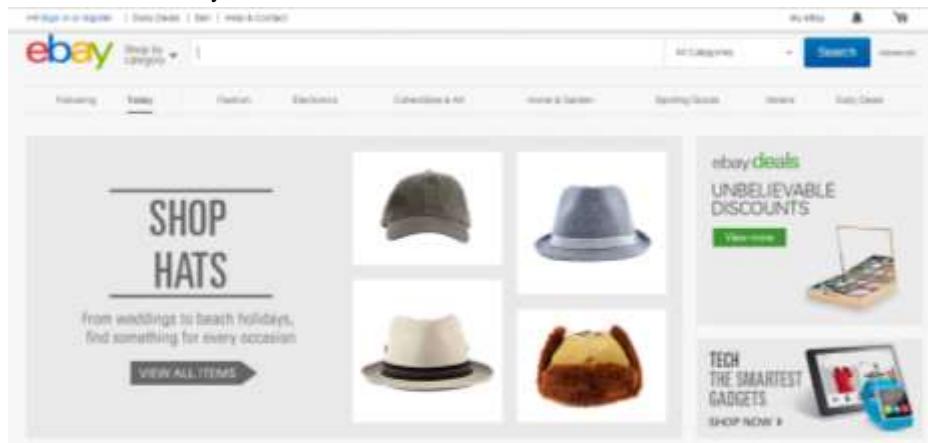
- Kupovina proizvoda za koje se na kraju ispostavi da uopšte ne postoje, nisu tačni opisu koji se nalazio na određenom sajtu ili su ukradeni,
- Online kupovina karata za koncerte ili putovanja koje uopšte ne postoje i odnose se na nepostojeće kompanije,
- Plaćanje nepostojećih naknada za iznajmljivanje prostora koji ne postoji, nije za iznajmljivanje ili se iznajmljuje velikom broju različitih osoba koje o tome ništa ne znaju
- Hakovanje naloga na društvenim mrežama, kao i e – mail – a.

Kada je riječ o online kupovini proizvoda onda je situacija veoma specifična. S obzirom na situaciju ne postoji mogućnost da se prodavač upozna, kao ni da se ostvari neka veća komunikacija, pa je zbog toga potrebna veća pažnja prilikom kupovine. Prva stvar na koju se mora obratiti pažnja jest web site sa kojeg se kupuje, posebno ako je riječ o nepoznatom site – u. Ukoliko je riječ o poznatoj web stranici kao što je npr. E – bay, postoji mogućnost da se pročita feedback prodavca i na osnovu toga ocijeni koliko je sigurno kupovati. Sljedeći korak na koji se mora obratiti pažnja jeste način plaćanja. Najčešće su u upotrebi platne kartice. Zavisno od kartice može kreditna i debitna. U ovim slučajevima bolje je koristiti debitnu karticu jer kod nje postoji limit za potrošnju, kao i trenutni uvid u stanje, tako da postoji manja mogućnost za manipulacijom. Neovisno o vrsti kartici svakako je potrebno obratiti pažnju na broj kartice i kontrolni broj. Najbolje je da se nigdje na zapisuje, a naročito da se ne daju informacije putem telefona ili mail – a.

Jedna od stavki na koju većina prilikom online kupovine ne obraća pažnju jeste poštarina. Najbolja mogućnost je korištenje opcije „free shipping“ tj. besplatna dostava ili u nedostatku ove opcije onda je potrebno gledati kod kojeg prodavca je najmanji iznos poštarine uz gore navedene uslove.

E – bay kao najveći servis online kupovine u svijetu ima najrazvijeniji sistem zaštite na koji je se moguće u potpunosti osloniti. Na E – bay sve informacije o prodavcu su javno dostupne i vidljive svima, a u slučaju reklamacije stvari se jako brzo riješe. Također, postoji opcija povrata novca ukoliko kupac nije zadovoljan proizvodom. Međutim, najbolje za kupca jeste da sve dva puta provjeri prije nego što se odluči za kupovinu.

Slika 3: Početna stranica E – bay



Izvor: <http://www.ebay.com/>

Prilikom online kupovine karata najčešća moguća prevara se dešava tako što se kupuje preko lažnih stranica. Stranice se naprave tako da izgledaju identično pravim i ukoliko ne uočite razliku na vrijeme, najvjerovaljnije je da će biti prevareni. Jedan od primjera takve prevare bila je za vrijeme Olimpijskih igara u Londonu 2012. godine. U tom periodu bilo je aktivno nekoliko internet stranica koje su lažno prodavali ulaznice, kao i rezervaciju smještaja. Neki od znakova da su u pitanju lažne stranice da nedostaju određeni certifikati (npr. VerySign) ili ako postoji da klikom na znak ne vodi direktno na tu web stranicu. Također, još jedan od pokazatelja lažne web stranice jeste da ne postoji mogućnost plaćanja putem PayPal – a ili kreditnih kartica, već se plaćanje vrši putem čeka slanjem preko pošte. Jedan od pozitivnih primjera web stranice u Bosni i Hercegovini jeste portal kupikartu.ba., gdje se može bez ikakvih problema i 100% sigurno kupiti karta/ulaznoca za neki događaj.

Slika 4: Početna stranica portala kupikartu.ba



Izvor: <https://www.kupikartu.ba/>

Svakako prije online kupovine karata ili rezervacije smještaja najbolje je provjeriti prodavca sa nekim ko je već koristio te usluge ako je u mogućnosti.

Kako je danas sve aktuelnije online oglašavanje, tako se i ovom dijelu nudi mogućnost manipulacije. Što se tiče zloupotrebe u ovom segmentu može se dešavati na više različitih načina. Jedan od primjera da se telefonski putem javi određena kompanija, odnosno predstavnik kompanije i nudi oglašavanje na svojoj web stranici za određenu sumu novca koju je potrebno prethodno uplatiti. Ukoliko se odlučite na ovaj korak najčešći rezultat je da tu reklamu nikada nećete vidjeti, kao ni novac koji ste uplatili.

Stoga, prije odluke o ovom načinu oglašavanja potrebno je da provjerite tu kompaniju koja nudi mjesto za oglašavanje, pa tek onda uplatiti novac.

Još jedan oblik cyber kriminala koji je danas među najzastupljenijim oblicima jeste hakovanje profila na društvenim mrežama. Kako je Facebook trenutno najpopularnija društvena mreža sa velikim brojem korisnika tako i mogućnost hakovanja profila je najšira. Najjednostavniji način hakovanja profila jeste da se zna e – mail adresa korisnika i da se „pogodi“ password korisnika. Međutim, u današnje vrijeme većina e – mail adresa korisnika je sakrivena (iz navedenog razloga), stoga se hakeri odlučuju na nešto više. Prvo pomoć trežailice pokušavaju na osnovu imena i prezimena da saznaju nešto više o određenoj osobi. Ako se i ovaj korak pokaže neuspješnim, sljedeće je da prave lažni profil, dodaju određenog korisnika u prijatelje i počinju konverzaciju. Na ovaj način pokušavaju da saznaju što je moguće više podataka o tom korisniku.

E – mail adresu najčešće se dobije na način da želi da proslijedi neke slike i to je prvi korak u preuzimanju tuđeg profila. Sljedeći jeste da tokom daljnje konverzacije saznanje koje stvari voli i koji je mogući password, a u nekim slučajevima i samo korisnici odaju te informacije. Na ovaj način većina facebook profila bude hakvana. Prva stvar koju korisnici treba da urade (ako već nisu) da sakriju svoju e – mail adresu, odnosno na postavkama da odaberu opciju „Samo ja“. Zatim, da ne prihvataju zahtjev za prijateljstvo od nepoznatih osoba, a posebno da ne započinju razgovor sa istim odavajući povjerljive informacije.

Slika 5: Početna stranica Facebook



Izvor: <https://www.facebook.com/>

ZAKLJUČAK

Iz svega do sada nevedenoga jasno nam je da bez interneta, kao i informacionih tehnologija nemoguće zamisliti svakodnevnicu. Nezavisno od potrebe, odnosno nevažno od načina upotrebe interneta da li je to za zabavu ili u poslovne svrhe moramo da budemo oprezni. Sve navedeno dešava se svakodnevno i osobama oko nas. Takav je način života da li mi htjeli ili ne moramo da koristimo internet, ali pri korištenju moramo da obraćamo pažnju na jako važne stvari. Još jednom je potrebno napomenuti da se važne informacije ne daju nepoznatim ljudima, ne ostavljaju na nesigurnim stranicama i da prilikom upisivanja podataka moramo da provjerimo da li je ta stračica sigurna i da navedene podatke niko neće zloupotrijebiti.

PHISHING KAO MANIFESTACIJA CYBER KRIMINALA

“PHISHING AS A MANIFESTATION OF CYBERCRIME”

Doc. dr. Džemal Kulašin

Fakultet za menadžment i poslovnu ekonomiju, Kiseljak

Apstrakt: Svakodnevno svjedočimo sve učestalijim manifestacijama cyber kriminala koji svojim razmjerama ozbiljno ugrožava ne samo individualne korisnike, već i poslovne sisteme uzrokujući respektabilne finansijske troškove. Pri tome, uočljivo je (i) sljedeće: a) tendencija rasta malicioznih programa, gdje je samo u prošloj godini registrirano čak 84 miliona novog malware-a te b) tendencija "novih" manifestacija cyber kriminala kroz različite oblike prevara na Internetu, najčešće s ciljem preuzimanja digitalnog identiteta korisnika.

U ovom radu predstavlja se jedan od dominantnih oblika prevara na Internetu, terminološki označen kao phishing ("pecanje"). U radu se ukazuje i na načine kako umanjiti rizike od ovog oblika cyber kriminala, gdje se pored softverskih alata posebno ukazuje na korisnika, odnosno na promjenu načina njegovog on-line ponašanja.

Ključne riječi: Cyber kriminal, "pecanje", "uzgajanje žrtve, presretanje", digitalni identitet

Abstract: Being everyday witnesses of frequent manifestations of cybercrime, it can be seen that its range severely threatens not only individuals as users but also business systems causing at the same time respectable financial costs. Thereby, the following can be noted: a) the increasing tendency of malicious programs with 84 mil of new malware registered only last year, and b) the tendency of "new" manifestations of cybercrime seen as different forms of Internet frauds, aiming to digital identity thefts.

This paper describes one of the dominant forms of such Internet frauds, called phishing (from English word "fishing"). This paper also points out the ways of decreasing risks for this form of cybercrime, where, besides those software tools, an emphasis is particularly put on online users and their way of behaving online which should be changed.

Keywords: Cybercrime, phishing, pharming, digital identity

UVOD

Među najprominentnijim i najštetnijim napadima cyber kriminalaca danas su tzv. phishing napadi. Predstavljaju oblik varanja, odnosno kriminalnu radnju gdje cyber prevarant (eng. cybercrook) šalje e-mail s ciljem da prevarom dođe u posjed osjetljivih podataka korisnika kao što su brojevi kreditnih kartica, PIN-ovi, pristupni podaci bankama, matični brojevi itd. Svi ovi podaci korisnika predstavljaju njegov digitalni identitet i ako napadač uspije u namjeri da ih preuzeme, može ih zloupotrijebiti na različite načine i time steći značajnu finansijsku dobit, što najčešće i jeste krajnji cilj.

Iz konteksta ove kriminalne radnje očito je da se odnosi na "pecanje" on-line korisnika elektronskim mamcem, te je stoga i nastala karakteristična terminološka odrednica **phishing** kao korijen riječi **fishing** (eng. *pecanje*). Iz terminološke odrednice *pecanje* otkriva se i ciljanje hakera na nedostatke svijesti ali i spoznaja korisnika o načinima i tehnikama očuvanja informacijske sigurnosti. Zbog toga se ova vrsta cyber kriminala svrstava u tzv. socijalni inženjering, jer se koristi varanjem zasnovanim na afektivnim segmentima pojedinca gdje se korist napadaču producira na "slabostima" žrtve u smislu lakovjernosti, ishitrenosti ali i neznanja.

1. TOK INTERNET PREVARA

Za predstavljanje načina funkciranja phishing-a korisno je opisati početke ove Internet kriminalne radnje. Ovaj oblik cyber kriminala prvi put se javlja u Americi 1996. godine kao radnja koja označava „upotrebu algoritma za hakovanje AOL sistema za naplatu online vremena“. Naime, unos ključnih podataka kreditnih kartica kojima se putem Interneta plaća(la) naknada AOL-u na njihovom serveru bio je izazov za hakere koji nisu mogli „varati“ server lažnim podacima te su svjesno razradili indirektnu strategiju putem „pecanja“ korisnika.

Strategija je podrazumijevala slanje velikog broja nasumičnih e-mail poruka koje su bile potpisane kao „Zaposleni u AOL“ sa tekstom koji od korisnika traži da iz nekog vanrednog razloga utipka svoje pristupne podatke (npr. nalog će biti suspendiran, i sl.), čime se otvarao put hakerima za upad u ciljane serverske sisteme.

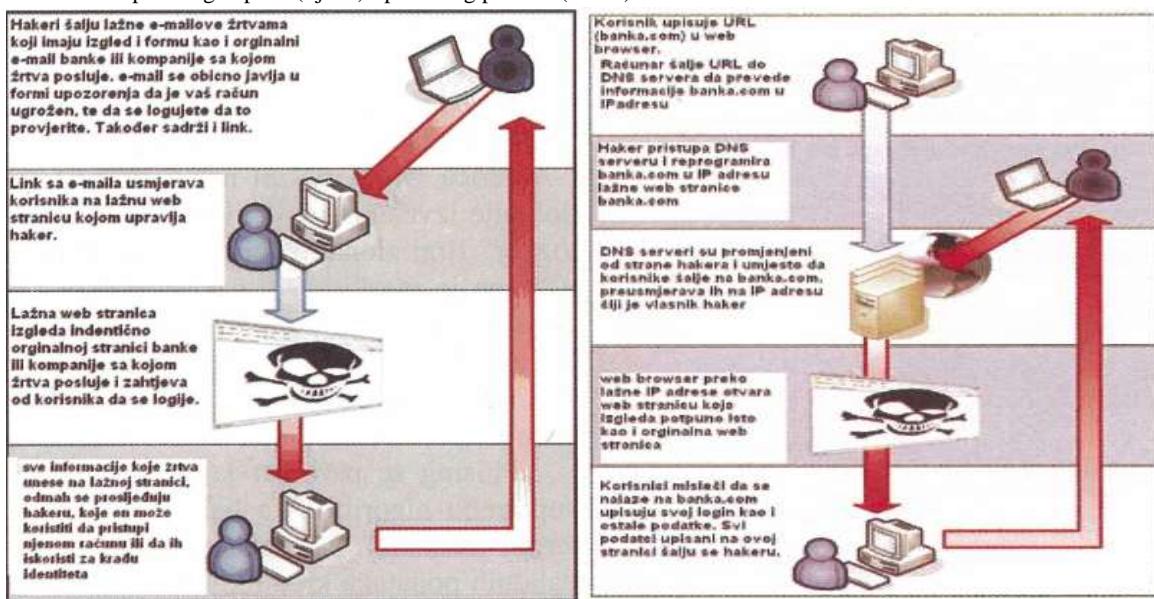
Način preuzimanja povjerljivih podataka dirigiran je tipom e-mail poruke koja se generira, gdje razlikujemo nekoliko slučajeva:

- a) lažni e-mail sa provokativnom sadržajem za primatelja (npr. bankarski nalog je pred blokiranjem, i sl.), kako bi se korisnik naveo na ishitrenu reakciju, gdje se često kao prilog (attachment) nalazi i key/logger kao spyware za praćenje rada tipkovnice žrtve,
- b) klonirani e-mail, gdje se zloupotrebljavaju poznate kompanije (poput ebay, amazon, america online i sl.) kako bi se korisnik naveo da utipka (i time „pokloni“) svoje podatke na sajtu kojeg uobičajeno koristi za novčane transakcije; ovaj tip Internet prevare predstavlja napredniji vid phishing-a označen kao pharming¹, što se u ovom kontekstu prevodi kao "uzgajanje žrtve" i "presretanje".

Pharming napad je sofisticiraniji, i zahtjeva znatno viši nivo znanja napadača i računarske opreme. Koristi se koncept prevare gdje korisnika „na putu“ do web sajta čiji URL utipkava *presreće* klonirani web sajt na koji sa punim povjerenjem unosi svoje podatke. Ukoliko se DNS (DNS - Domain Name Service, zadužen da pretvara Web i e-mail adrese u numeričke nizove) izmjeni tako da sadrži lažne informacije o tome koja Web adresa odgovara kojem nizu brojeva, svi korisnici koji otipkavaju odgovarajući (ispravnu) Web adresu bivaju preusmjereni na lažnu. Iako ovaj postupak (nazvan još i DNS poisoning) nije nov, kompleksnost pharming napada u punoj mjeri otkriva sigurnosne nedostatke Internet protokola, nastale još onda kada je kreiran. Za sprovođenje manjih pharming napada koriste se posebni virusi upućeni elektronskom poštom koji prepisuju lokalne host fajlove na napadnutim računarima. Host fajl pretvara URL adrese u numeričke nizove koji su razumljivi za računar, tako da ugroženi host fajl uzrokuje da korisnik bude usmjeren ka pogrešnom web sajtu, čak i ako korektno utipka URL adresu legitimne Web lokacije. Takođe, napadač može koristiti i XSS (Cross-site scripting) napad te iskoristiti propuste u dizajnu web stranica za preusmjeravanje žrtvi na lažne web stranice gdje žrtve otkrivaju osjetljive podatke potrebne cyber kriminalcu da dođe do novca ili osjetljivih podataka korisnika.

Opći tok phishing i pharming napada može se predstaviti i grafički (Slika 1).

Slika 1: Tok phishing napada (lijevo) i pharming prevare (desno)

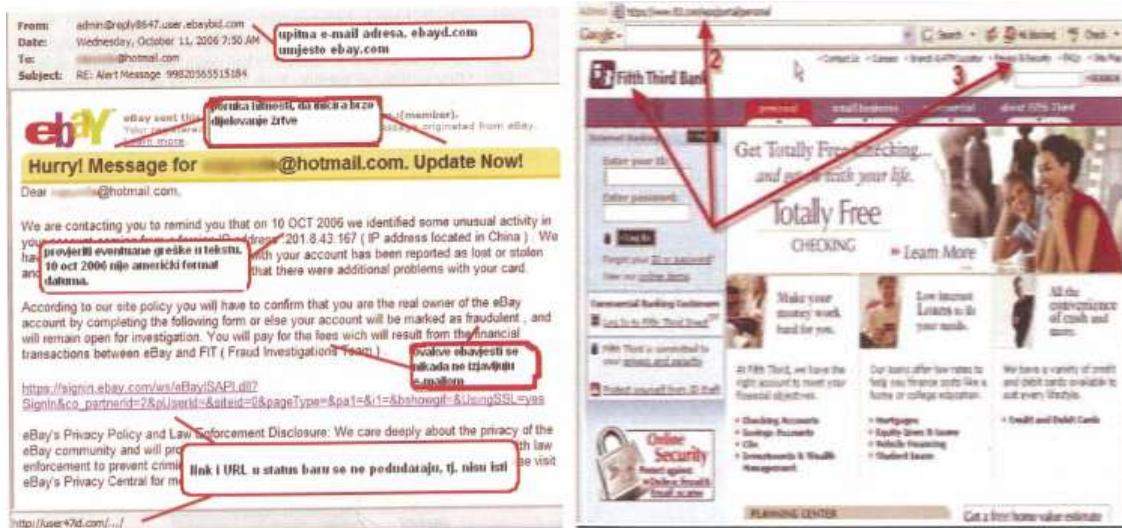


¹ Termin je izведен kao veza sa terminom **phishing** te eng. riječi **farming** (uzgoj, uzbijanje)

1.1. Prepoznavanje phishing-a

Phishing napadi su izuzetno učestali te se svakog dana šalje ogroman broj lažnih e-mail poruka po cijelom svijetu. Uz to, ovi napadi postaju i sve sofisticiraniji te lažne poruke e-pošte i web-mjesta sadrže linkove na prave logotipe stvarnih kompanija dobro poznatih brendova (Ebay, PayPal, Bank of America...) tako da izgledaju potpuno legalno (Slika 2). Zbog toga je prosječnoj osobi sve teže prepoznati da li je e-mail poruka ili određena web lokacija prevara, čime cyber kriminalci koji koriste phishing prevare postaju sve uspješniji. No, nekoliko karakteristika otkriva phishing, a najmarkatnije su: e-mail poruka dolazi od nepoznate osobe, ne sadrži naslov (subject) ali sadrži uočljive gramatičke greške, sadrži zahtjeve za osobnim podacima korisnika uz naglašenu hitnost u reagiranju, sadrži lažne linkove i maske na linkovima itd.

Slika 2. Lažna e-mail poruka (lijevo) i klonirana e-mail poruka (desno)



Svakako, očita je i sličnost phishing-a sa spam-om, što se vidi i iz definicije spam-a kojeg daje MAPS (Mail Abuse Prevention System - Sistem za sprečavanje zloupotrebe pošte), gdje se navodi da "...e-mail poruka je spam ako: a) identitet i kontekst primatelja su irelevantni zato što poruka može jednako da se primjeni na više potencijalnih primatelja, b) primatelj nije dao eksplicitnu dozvolu za slanje e-pošte i ne zna od koga ona dolazi i c) slanje i prijem poruke donosi pošiljaocu nesrazmjernu korist u odnosu na primatelja. Spam je, dakle, elektronski ekvivalent neželjenoj pošti - ali ne isključivo i lažnoj pošti, jer spam uglavnom ne sadrži namjeru ilegalnog preuzimanja privatnih podataka od primatelja.

2. ZAŠTITA OD PHISHING NAPADA

Kao prvi zid odbrane od phishing napada logično se nameće tehnologija, odnosno standardni sigurnosni alati kao temeljni sigurnosni bedem, a to su antivirusni i antispyware software, te firewall. Pri tome, podrazumijeva se redovno ažuriranje anti-malware software-a, kao i redovno instaliranje najnovijih zagrpa i instalacija verzija svih ostalih programa u kojima su ispravljeni sigurnosni propusti.

U tehnološkom smislu, usko vezano za zaštitu od phishing i pharming napada je i instaliranje tzv. sigurnosnih ekstenzija za pretraživače (browsers) koje koristimo na Internetu. Doduše, savremeni browseri, kao što je Google Chrome, koriste zaštitni sistem Safe browsing technology koji skenira svaku web lokaciju koju posjećuje korisnik te na određeni način upozorava ako je lokacija sumnjiva. Ipak, za browser-e pod aktuelnim operativnim sistemima (Windows, Mac, Linux) postoje i tzv. sigurnosne ekstenzije, a najčešće u upotrebi su sljedeće: **Netcraft Toolbar**, **TrustWatch Toolbar**, **ScamBlocker**, **PhishNet** i **SpoofStick**. Sigurnosne ekstenzije prikazuju se kao dodatni toolbar-i u pretraživačima skenirajući web promet slično Safe browsing technology-ju, te u slučaju navođenja korisnika na kloniranu web lokaciju ne ponavljaju njen naziv (npr. Ebay.com) već navode "odgovarajuću" IP adresu, što je signal da se radi o kompromitiranoj lokaciji na kojoj ne treba izvoditi bilo kakve transakcije.

Ipak, tehnološka osnova - iako važna i nužna, nije i dovoljna u zaštiti od phishing-a. Naime, phishing napadi su kategorija socijalnog inženjeringu te se stoga i zaštića u presudnoj mjeri svodi na korisnika, odnosno na njegovo ponašanje kada je on-line, tj. dok se nalazi na Internetu. Oprez se u ovom slučaju posebno odnosi na korištenje e-mail servisa, odakle se većinom i generiraju problemi. Dakle, korisnik treba značajno povećati dozu opreza kada je on-line, a posebno pratiti svoj Inbox u kojem svakodnevno stižu brojne e-mail poruke među kojima se kroz sigurnosne filtere "provlače" i sumnjive poruke kada treba znati adekvatno reagovati, kako slijedi:

- **E-mail poruka sadrži zahtjeve za osobnim podacima:** Legalne kompanije mahom ne traže osobne podatke od svojih korisnika putem e-pošte, već koriste direktnе kontakte. Dakle, treba biti maksimalno oprezan sa e-mail porukama koje izgledaju potpuno vjerodostojno i traže osobne podatke.
- **E-mail poruka od nepoznatog pošiljaoca:** Teorijski, svaku poruku od nepoznatog pošiljaoca treba pretpostaviti potencijalno sumnjivom. Dodatni oprez treba biti ako poruka nema naslov (subject), jer to predstavlja jednu vrstu narušavanja e-mail korespondencije.
- **E-mail poruka sadrži očigledne pravopisne greške:** Svaku poruku koja sadrži očigledne pravopisne greške ili greške u stručnim finansijskim terminima (ako poruka dolazi od "finansijske institucije", što najčešće i jeste slučaj) treba tretirati sumnjivom. Kodeks nalaže i pravilnu strukturu e-mail poruke ali i konzistentnost sadržaja u smislu da se koriste valjani ekonomski termini, te svako uočeno odstupanje ukazuje na lažni e-mail.
- **Hitnost u sadržaju:** Lažni e-mail karakterizira provocirajući sadržaj koji iziskuje hitnu reakciju primatelja, odnosno žrtve. Primjer iz jedne otkrivene phishing prevare je sljedeći: "Dragi korisniče banke, ustanovili smo kako je potrebno ažurirati podatke o vašem računu zbog neaktivnosti, prevare ili izvještaja o prevari. Ako ne ažurirate vaše podatke, račun će biti obustavljen. Slijedite ovaj link i potvrdite vaše podatke".
- **Prilozi (attachments):** Mnoge phishing prevare traže od korisnika otvaranje priloga koji zatim mogu na računar "prenijeti" virus ili spyware. Ako se na računar instalira key/logger kao aktuelna vrsta spyware-a, on može "snimati" rad tipki kojima se unosi korisničko ime i lozinku osobnih internetskih računa. Prilog koji se želi pregledati treba najprije spremiti i zatim skenirati korištenjem ažurnog antivirusnog programa prije nego što se otvori. Ovdje može pomoći i ozbiljan e-mail klijent (kakav je npr. MS Outlook) koji automatski blokira određene priloge koji mogu sadržavati viruse; u slučaju da Outlook otkrije sumnjivu poruku, prilozi s bilo kojom vrstom datoteke se blokiraju.
- **Lažni linkovi:** Prevaranti koji koriste phishing poruke su vrlo sofisticirani kad se radi o stvaranju lažnih linkova i prosječnoj osobi je gotovo nemoguće prepoznati je li veza legalna. Uvijek je najbolje u preglednik ručno unijeti web-adresu ili jedinstveni lokator resursa (URL) za koji se zna da je tačan, a posebno treba izbjegavati popularni Copy - Paste, tj. kopiranje i lijepljenje URL-a iz poruke u preglednik.
- **Maska na linku:** Iako link na koji upućuje sadrži čitav ili djelomični naziv prave kompanije, link može biti "maskiran". To znači da link koji se vidi ne vodi na tu adresu već negdje drugdje, obično na lažno web-mjesto.
- **Homografi²:** Na računarima, homografski napad je internetska adresa koja izgleda kao poznata internetska adresa, ali je zapravo izmijenjen; npr. www.microsoft.com može izgledati kao **www.micosoft.com** ili **www.mircosoft.com**. Svrha ovakvih lažnih web-linkova koji se koriste u phishing prevarama je prevariti žrtvu tako da ih klikne. Cyber kriminalci lažiraju uglavnom nazive domena banaka kako bi prevarile korisnike i uvjerile ih kako posjećuju poznata i povjerljiva web-mjesta, kakvo je svakako web mjesto svoje banke.
- **URL sadrži "nemoguću" domenu:** Osobe koje šalju phishing poruke često se oslanjaju na činjenice da mnogi email korisnici ne znaju način strukturiranja domena, gdje je zadnji dio domene najbitniji. Npr. domena info.facebook.com je poddomena facebook.com, jer se facebook.com pojavljuje na kraju cijelog naziva domene (na desnoj strani). Na osnovu toga, facebook.com.zlonamjernadomena.com ne potiče od facebook.com, jer se facebook.com nalazi na lijevoj strani naziva domene, umjesto na desnoj. Prevarant jednostavno kreira poddomenu s imenom Facebook ili slično, a rezultirajući naziv domene izgleda ovako:

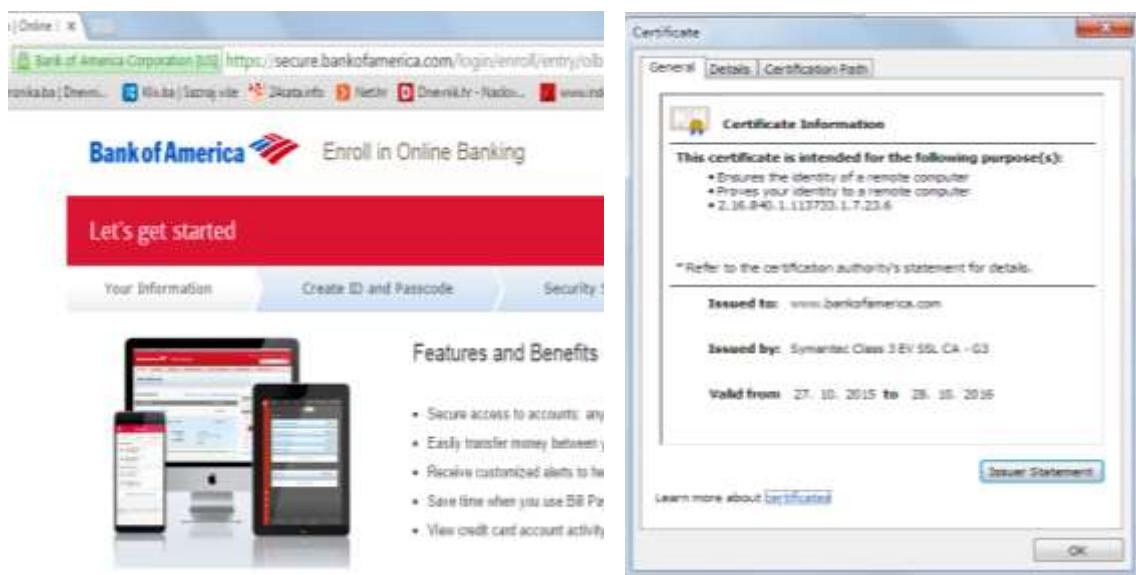
² Homograf je riječ koja se piše jednako kao druga riječ, ali ima drugo značenje

facebook.zlonamjernadomena.com. Na ovaj način prevaranti pokušavaju uvjeriti žrtve da poruka dolazi od brenda kao što je Facebook, Microsoft i sl.

- **URL bankovne institucije ne sadrži https:** Https u URL-u bankovne institucije potvrđuje da se između servera i browsera uspostavlja enkriptirani podatkovni kanal osiguran tzv. SSL sigurnosnim slojem (SSL - Security Socket Layer). Ovaj zaštitni sistem označava se i ikonom katančića, na kojem se može izvršiti i validacija određene lokacije koja treba rezultirati digitalnim certifikatom izdatog od strane odgovarajućeg CA autoriteta (CA - Certification Authority), čija validnost se, između ostalog, dokazuje i terminom valjanosti (Valid from).

U svakom slučaju, ako URL bankovne institucije (ili općenito online kompanije gdje se izvode finansijske transakcije) počinje sa http umjesto sa https - znak je da se radi o kloniranoj stranici na kojoj ni u kojem slučaju korisnik ne smije unositi bilo koje osobne podatke, a posebno brojeve kreditnih kartica ili pristupne podatke svoje banke (user, password) (Slika 3).

Slika 3. Ispravan URL banke (lijevo) i digitalni certifikat kao rezultat validacije (desno)



ZAKLJUČAK

Korištenje Interneta i u našoj zemlji sve više ulazi u poslovne sfere, te se shodno tome u sve većem obimu realiziraju i finansijske transakcije. Pokazuju to i zvanični podaci Centralne banke Bosne i Hercegovine, gdje se navodi da je uslugama Internet bankarstva i drugih oblika elektronskog trgovanja obuhvaćeno ukupno 314.777 subjekata, odnosno 44.802 pravnih subjekata i 269.975 fizičkih lica³. Sve to govori da su i korisnici Interneta u našoj zemlji izloženi ozbiljnim opasnostima koje nosi Internet, te da se moraju neprestano educirati o načinima i tehnikama očuvanja digitalnog identiteta.

Phishing napadi su među najčešćim oblicima cyber kriminala, ali koji se ipak mogu preduprijediti aktivnijim učešćem korisnika uz nezaobilaznu tehnološku osnovu. Dakle, pored aktivne tehnološke osnove, potrebno je povećati dozu on-line opreza te usvojiti karakteristike sumnjivih e-mail poruka kako bi se potom adekvatno reagiralo.

S obzirom da je razvoj IT-ja veoma dinamičan, a Internet prostor "beskrajan", jako brzo dolazi do novih, sofisticiranijih oblika djelovanja cyber kriminalaca, tako da se edukacija o zaštiti od phishing napada mora odvijati kontinuirano. Konačno, sasvim je jasno da zbog prirode ovih napada kategoriziranih kao tzv. socijalni inženjeri, svijest i ponašanje on-line korisnika stoe kao presudna tačka odbrane.

³ Zvanično saopštenje Centralne banke BiH, 09.mart 2016

LITERATURA

- [1] Hanić, H., Sučeska, M. (2008): Kompjuterski kriminal - pojavni oblici i preventiva, Fakultet kriminalističih nauka, Sarajevo.
- [2] Babić, V. (2009). Kompjuterski kriminal, RABIC, Sarajevo.
- [3] Pastore, M., Dulaney, E. (2007): Security+, Kompjuterska biblioteka - Sybex, Beograd.

Internet izvori:

- [1] <http://www.brighthub.com/computing/smb-security>
- [2] <https://support.office.com/hr-hr/article/phishing>
- [3] <http://www.prevare.info>
- [4] <http://www.20thingsilearned.com>
- [5] <http://www.kombib.rs/spam.html>
- [6] <http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-290.pdf>

ZAVISNOST OD INTERNETA-PREDRASUDE ILI REALNOST

Goran Blagojević, mr¹ i Goran Guska, MA²

¹MUP Republike Srpske, Uprava za policijsko obrazovanje - Banja Luka, RS-BiH, Doktorand na Fakultetu bezbednosti Univerzitet u Beogradu, e-mail:blagojevicgoran@yahoo.com

²MUP Republike Srpske, Uprava za policijsko obrazovanje - Banja Luka, RS-BiH, Doktorand na Pravnom fakultetu Univerzitet u Novom Sadu, e-mail: goranguska@gmail.com

Apstrakt: Razvoj interneta kao globalne kompjuterske mreže, doprinjeo je da se savremeni komunikacijski obrasci unaprijede i razmatraju u potpuno drugaćijem teorijskom i praktičnom kontekstu. Usljed svoje specifičnosti, evoluirala je ideja da ovaj fenomen postane predmet mnogobrojnih teorijskih razmatranja i naučnih rasprava. Svakako, najkontraverzniјa pojava iz ovog domena može se predstaviti pitanjem: „Da li internet može da postane predmet patološke upotrebe i posledično, dovede do pojave poznate kao „zavisnost od interneta“? U ovom radu će se sagledati argumenti koji se u naučnoj i široj javnosti nude kao potvrda da ova pojava zaista postoji, ali i njima suprotnih stanovišta. „Patološka upotreba interneta“ – koncept „za“ i koncept „protiv“, težište je ovoga rada sa ciljem minimiziranja bezbjednosnih izazova, rizika i prijetnji koje sa sobom nosi internet, te sagledavanje kriminalističkih aspekata zloupotrebe interneta.

Ključne riječi: Internet, patološka upotreba interneta, zavisnost od interneta, kriminalistički aspekti zloupotrebe interneta.

UVOD

Internet kao globalna mreža i sistem koji je namijenjen komunikaciji i razmjeni informacija u savremenom dobu, progresivnim napretkom uslovio je potrebu za većom pojavom bezbjednosne kontrole, iako u samom početku njegovog konceptualnog zamišljanja to i nije bila ideja, jer je njegova namjena zapravo bila potpuno drugačije koncipirana. Naime, u krugovima učenijih ljudi on je bio zamišljen kao sredstvo putem kojeg se dalekosežnije olakšava sam način i proces rada, dok se ekspanzijom komercijalizovanja njegove namjene i funkcije, dolazi do problematike koja se odnosi na njegovu zloupotrebu. Zahvaljujući korištenju interneta, njegovoj opštoj dostupnosti, subjektima koji ga mogu koristiti ali i teškom načinu kontrolisanja, praktično korištenje interneta kao „dobrog sredstva u lošim rukama“, rezultira pojavom bezbjednosnih rizika, ugrožavanjima i izazovima koji svakako zavređuju pažnju, naročito ako se uobziri činjenica da se sve više zloupotreba odnosi na devijacije sa višestrukim i dalekosežnim posledicama.^[1] Jedna od najkontraverznijih pojava iz ovog domena odnosi se na pitanje: „Da li internet može da postane predmet „patološke upotrebe“ i posledično dovede do fenomena poznatog kao „zavisnost od interneta“?

U ovom radu pokušaćemo da sagledamo argumente koji se u naučnoj i široj javnosti nude kao potvrda da data pojava zaista postoji, te da li ona i u kojoj mjeri može da utiče na izvršenje krivičnih djela ili drugih inkriminisanih radnji. Na samom početku treba istaći ograničenja sa kojima se istraživači suočavaju prilikom pokušaja da operacionalno definisu pojavu zavisnosti od interneta i utvrde njenu strukturu. Prvo, u razmatranju da li je neka pojava normalna ili patološka, neophodno je definisati granice dimenzije normalnosti, odnosno, gdje je mjesto na kontinuumu normalnost-patologija; gdje normalno prelazi u patološko i obratno?! Upravo ovdje nailazimo na viševjekovnu prepreku koju istraživači i teoretičari pokušavaju da prevaziđu na razne načine, nudeći mnoštvo modela kojima bi se ovo pitanje moglo razriješiti. Konkretnog i opšteprihvaćenog odgovora i dalje nema. Samim tim, odsustvo jasno definisanog kriterijuma normalnosti i patologije u značajnoj mjeri otežava mogućnost razmatranja pretjerane upotrebe interneta kao patološke pojave.

Drugo, upotreba interneta predstavlja interaktivan proces u kome učestvuju korisnici sa osobenim obilježjima na jednoj strani, i virtualni prostor sa svojim specifičnostima na drugoj strani. Upravo ovakav vid interakcije dovodi do razvoja mnoštva korisničkih stilova, od kojih se neki, opravdano ili ne, smatraju „patološkim“. Treće, generalizacija zaključaka dobijenih na malom broju istraživanja organizovanih sa ciljem ispitivanja pojave „patološke upotrebe“ interneta, koja su problematično metodološki zasnovana,

organizovana na neadekvatnom uzorku, bitno umanjuje značaj izvedenih zaključaka, a samim tim dovodi u pitanje i postojanje ove pojave.

Međutim, pored brojnih osporavanja fenomena „zavisnost od interneta“ ili „patološka upotreba interneta“, neosporno je da vrijeme provedeno koristeći virtuelni svijet višestruko utiče na čovjeka. Kako on utiče na čovjeka i koliko je progresivan u negativnom kontekstu aktivnosti u realnom svijetu, prevashodno misleći na kriminalno djelovanje, biće predmet ovog rada.

1. NASTANAK INTERNETA

Kvalitativni i kvantitativni konglomerat ljudskih komunikacija savremenim telekomunikacijama i drugim tehnološkim inovacijama, potpomognut fenomenom globalizacije svijeta i ljudske egzistencije, uslovio je stvaranje i kreiranje interneta. U prvom redu, nastanak interneta je usko povezan sa razvojem informaciono-komunikacione tehnike i tehnologije, odnosno sa razvojem i ekspanzijom računarske tehnologije. Međutim, za nastanak interneta značajna su i mnoga tehničko-tehnološka dostignuća iz XIX i XX vijeka (pojava telefona, telegrafa, telefaksa i televizije), a pogotovo određena računarska dostignuća iz druge polovine XX vijeka (pojava računara i procesora).[2] Navedena tehničko-tehnološka dostignuća, ali i druga dostignuća, te određena međunarodna politička dešavanja i događaji, (hladnoratovska podjela svijeta, mogućnost izbjijanja atomskog rata i sl.), uslovili su stvaranje arpaneta koji se smatra pretečom interneta, odnosno interneta u prvobitnom obliku. Arpanet je bila interna mreža (intranet) američkih naučnoistraživačkih i vojnih centara koja je nastala 1969. godine. Kvantitativna ekspanzija arpaneta uslijedila je veoma brzo.[3] Krajem osamdesetih godina XX vijeka ovu mrežu sve više prihvataju razni subjekti u društvu uslijed čega ona gubi karakteristike intraneta kao mreže koja je bila primarno vojnog karaktera, već postaje internet mreža na globalnom nivou kao mreža svih mreža. U tom periodu došlo je do spajanja većine takvih postojećih mreža širom svijeta u jednu mrežu, te se na osnovu ovakvog dešavanja smatra da je ovaj način doprinjeo nastanku, odnosno početku interneta.

1.1. Upotreba interneta kao patološka pojava i kao zavisnost

Ekspanzijom interneta kao korisničke mreže veoma brzo su prevaziđena sva očekivanja koja su se odnosila na broj korisnika, ali i broj internet aplikacija, koje su na ovaj način postale dostupne. Internet ubrzo postaje najveće tržište na planeti, naročito kada je riječ o dostupnosti informacija. Samim tim, stvoreni su uslovi za nastanak jedne nove pojave među korisnicima koja se odnosi na sve izraženiju potrebu za dužim boravkom na internetu. U kontekstu upotrebe interneta, sa aspekta patološke pojave i sa aspekta zavisnosti nije ujednačen stav u naučnim i stručnim krugovima. Prevashodno se neujednačenost stavova sastoji u pronalasku adekvatne definicije ponašanja koje bi rezultiralo negativnom, prekomjernom, problematičnom, kompulsivnom, nefunkcionalnom upotrebointerneta. Najzastupljenija terminološka određenja su: Zavisnost od interneta (*Internet addiction*), Kompulsivna upotreba interneta (*Compulsive Internet use*), Zloupotreba interneta (*Internet misuse*), Patološka upotreba interneta (*Pathological Internet use*), Prekomjerna upotreba interneta (*Internet over-use*) i drugo.[4] Termin „Internet zavisnost“ akcenat stavlja na posljedice koje upotreba interneta po korisnika ima na zdravstvenom, porodičnom planu, planu akademskog i profesionalnog razvoja. Dakle, internet zavisnost predstavlja impulsivnu težnju za upotrebotinterneta, praćenu gubitkom kontrole, preokupiranošću i kontinuiranom upotrebotbez obzira na ispoljene posljedice u poremećaju ponašanja.[5] U odnosu na internet zavisnost, njegova zloupotreba bi prevashodno predstavljala blaži oblik u kojem individua može pored svoje preokupiranosti da ima samokontrolu nad svojim ponašanjem, te u tom smislu može da postavi granice i reguliše upotrebu interneta. Internet zavisnost upućuje na psihološku zavisnost na relaciji „osoba – stimulus“ (najčešće neka supstanca) i da se zato zloupotreba interneta u tom smislu ne uvršćuje pod zavisnost, slično kockanju za koje se opravdano koristi izraz patološko kockanje.[6] U odnosu na internet zavisnost i zloupotrebu interneta, termin „patološka upotreba interneta“ je širi od navedenih pojmove i može obuhvatiti pojave poput sajber proganjanja, krađe identiteta i drugo. Kompulsivna upotreba interneta predstavlja neku vrstu bihevioralne zavisnosti sa sličnim manifestacijama kao kod kockanja, kupovine, ishrane i slično.[7] Izučavanje pojma internet zavisnosti vezuje se za rad profesorke Fakulteta za biznis i menadžment „St. Bonaventure“ Kimberli Jang, koja je ukazala na postojanje problema internet-zavisnosti, obrasce upotrebe interneta kod zavisnika, posljedice problematične upotrebe interneta i moguće puteve adekvatnog tretiranja problema.[4] Jangova je služeći

se kriterijumima „IV izdanja Dijagnostičkog i statističkog manuelnog priručnika DSM-IV za patološko kockanje“ (koje se smatralo najsličnjim pojavi internet zavisnosti), razvila test za otkrivanje internet-zavisnosti (*IAT – Internet Addiction Test*).[8] Prema tome, da bi se neka osoba nazvala internet zavisnikom potrebno je da ispuni pet ili više od osam navedenih kriterijuma u trajanju od šest mjeseci. To su: **1.**okupiranost objektom zavisnosti; **2.**tolerancija na upotrebu interneta (smanjeno zadovoljstvo vremenom koje se obično provodi na internetu, potreba za stalnim povećanjem vremena na internetu); **3.**pojava simptoma apstinencijalne krize pri pokušaju smanjenja upotrebe ili pri lišavanju interneta (anksioznost, depresija, razdražljivost); **4.**nemogućnost kontrole nad upotrebot interneta (neuspjeli pokušaji da se smanji vrijeme ili prekine upotreba interneta); **5.**na internetu se ostaje duže ili mu se pristupa češće nego što je planirano; **6.**pojava problema u socijalnim odnosima, u školi, na poslu, uslijed upotrebe interneta; **7.**skrivanje realnog vremena koje se provodi na internetu (obmanjuju se porodica, kolege, terapeut); **8.**percipiranje interneta kao načina da se pobegne od problema (anksioznost, tuga, krivica i slično).[9]

2. Fenomenologija internet zavisnosti

Fenomenološki oblici internet zavisnosti se prema pojedinim naučnicima svrstavaju u grupe kao što su: generalni i specifični tip internet zavisnika. Naime, ukoliko su korisnici zavisni od neke specifične aplikacije ili funkcije interneta, kao npr. kupovina preko interneta, kockanje preko interneta, sajber seks i pornografija, svrstavamo ih u specifični tip zavisnosti, pri čemu najčešće njihova patologija nije uslovljena internetom. Generalni tip zavisnosti, gdje je osoba zavisna od interneta po sebi, prekomjerno ga upotrebljava, bavi se različitim aktivnostima na mreži i ima nezaustavljivu potrebu da to i dalje radi, je znatno rijeđa pojava među korisnicima.[10] Jedna od najpopularnijih i najuticajnijih tipologija internet-zavisnosti klasifikovao je veliki broj različitih ponašanja i kompulsivnih radnji u pet tipova internet - zavisnosti:[11] **1.** Zavisnost od sajber seksa (*Cybersexual addiction*), kompulsivna upotreba web sajtova za sajber seks i sajber pornografiju, (predstavlja gledanje, daunloudovanje i razmjenu pornografskih sadržaja ili učešće u sobama za sajber seks za odrasle). Ovi tipovi internet zavisnosti najčešće nisu prestupnici već svoju zavisnost baziraju na fantaziji. Mada i u ovom slučaju svakako da treba biti oprezan. Naime, ovi internet zavisnici svoje seksualne fantazije u oblasti sajber seksa koriste kao model da se pobegne od problema u realnom životu, za razliku od klasičnih seksualnih prestupnika koji izražavaju potrebu za iskazivanjem i ispoljavanjem bijesa, moći, dominacije i slično). **2.** Zavisnost od socijalnog umrežavanja, (*Social networking addiction*), predstavlja pretjeranu involviranost u socijalne odnose na internet mreži. Sajtovi za socijalno umrežavanje najčešće integriraju većinu popularnih interaktivnih aplikacija koje izazivaju zavisnost, na četovanje, e-mail korespondencija i slično. Sajber emotivne veze mogu vrlo loše uticati na interpersonalne odnose čovjeka u realnom životu, funkcionisanje porodice i pojedinca, izvršavanje radnih obaveza itd. **3.** Net kompulsije (*Net compulsion*), predstavlja zavisnost od kockanja, kupovine i igranja igrica preko interneta i dr. **4.** Prezasićenost informacijama (*Information overload*), predstavlja opsativno surfovanje i pretraživanje baza podataka bilo da su u pitanju profesionalni interesi ili se to radi iz zabave. Ovaj tip se smatra oblikom zavisnosti koji je specifičan po tome što je lišen interaktivnosti i proizlazi iz funkcije interneta kao velike svjetske mreže (baze) podataka. **5.** Zavisnost od informaciono -komunikacionih tehnologija (*Information communication technology addiction*). Iako je izvorni naziv ove zavisnosti bio zavisnost od kompjutera, opravданo je uzeti u obzir razmatranje i zavisnosti od mobilnih telefona i drugih tehnologija. S tim u vezi, sasvim je odgovarajući termin zavisnost od informaciono - komunikacionih tehnologija.

2.1. Psiho-socijalni profil internet zavisnika

Začetnik ideje o izučavanju pojma internet zavisnosti jeste Kimberli Jang, koja je prilikom istraživanja skrenula pažnju na profil internet zavisnika. Govoreći o socijalnom profilu internet zavisnika a u pogledu njihovog društvenog statusa, može se reći da su to najčešće osobe koje su nezaposlene, studenti, penzioneri, domaćice, učenici osnovnih i srednjih škola. U opsegu njihovog korištenja interneta, najčešće se radi o različitim vrstama interaktivnih aplikacija. Kada je riječ o psihološkom profilisanju internet zavisnika, potrebno je napomenuti da se ovim putem zadovoljavaju određene potrebe kao što su: potreba za seksom, potreba za drugim stanjem svijesti, potreba za postignućem i nadmoćnošću, potreba za pripadanjem, potreba za održavanjem odnosa sa drugim ljudima, potreba za samoaktualizacijom i

samotranscendencijom. Kao posebno važne, tu su i potrebe za pripadanjem i potreba za održavanjem odnosa sa drugim ljudima.[12] Na našim prostorima, zavisnost od interneta se podjednako odnosi kako na mušku, tako i na žensku populaciju.

Često se radi o licima koja se nalaze u adolescentskoj dobi uzrasta i studentima. Najčešće su to lica koja su obrazovaniji korisnici, bolje ekonomskog statusa i koji se nalaze u urbanijim mjestima stanovanja, bilo da se radi o boravku ili prebivalištu. Najčešća dimenzija patološke upotrebe interneta kod nas, odnosi se na prenaglašenu potrebu za informacijama, socijalnom interakcijom i potreba za zabavom i ostvarenjem hobija onlajn (sajber pornografija, igrice, muzika, umjetnost, i sl.).[13] Kao pospješivače internet zavisnosti možemo navesti različite faktore. Međutim, oni koji se prevashodno izdvajaju su upotreba alkohola, socijalna anksioznost, depresija, hiperaktivnost, porodični i lični problemi. Kao refleksija internet zavisnosti, u smislu posledica, možemo navesti veliki nivo depresije, anksioznost, hostilnosti, interpersonalna senzitivnost, psihoticizam i na kraju, ali ništa manje važno, kriminal.

3. PRAVNA DETERMINACIJA ZLOUPOTREBE INTERNETA

U Bosni i Hercegovini i Republici Srpskoj, sam pojam zloupotrebe interneta obuhvaćen je u pojmu visokotehnološkog kriminaliteta. Ovo je naročito prisutno ako se u obzir uzmu stavovi koji dolaze iz krugova kriminalističkih, pravnih i bezbjednosnih sfera koji svakako svojim djelovanjem uobličavaju kako teoretski, tako i pravno-praktični smisao regulisanja i dozvoljenosti funkcionisanja ove oblasti. Sve te aktivnosti sagledavaju se na osnovu mogućnosti koje se primjenjuju u cilju suzbijanja i sprečavanja zloupotrebe interneta, socijalnog inženjeringu, odnosno visokotehnološkog kriminaliteta, i to na način da aktivnosti koje su suprotne propisima predstavljaju povrede određenih zakona koje za sobom povlače i odgovarajuću odgovornost i sankcionisanja. Načini sprečavanja i suzbijanja visokotehnološkog kriminaliteta na našim prostorima omogućeni su međunarodnim konvencijama i direktivama međunarodne zajednice, a koje su Bosna i Hercegovina i Republika Srpska potpisale, te se kao najznačajnija potpisana dokumenta koja regulišu ovu oblast na međunarodnom nivou spominju Direktiva Savjeta Evropske Zajednice o pravnoj zaštiti kompjuterskih programa i Konvencija o suzbijanju visokotehnološkog kriminala. Na osnovu ovih dokumenata, BiH i Republika Srpska produktivno su uspostavili pravnu regulativu primjenjivu u oblasti otkrivanja i sprečavanja visokotehnološkog kriminala, odnosno način preventivnog i represivnog tretiranja ove oblasti. Kao posledica navedenih međunarodnih dokumenata u Krivičnom zakonu Republike Srpske, kao i u Zakonu o izmjenama i dopunama Krivičnog zakona

Republike Srpske, propisana su krivična djela poput: neovlašćeno ulaženje u zaštićenu kompjutersku bazu podataka; proizvodnja i prikazivanje dječije pornografije; neovlašćeno fotografisanje, neovlašćeno korištenje ličnih podataka; iskorištavanje djece i maloljetnih lica za pornografiju; upad u kompjuterski sistem; oštećenje računarskih podataka i programa; računarska sabotaža; izrada i unošenje računarskih virusa; računarska prevara; neovlašćen pristup zaštićenom računaru, računarskoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka; sprečavanje i ograničavanje pristupa javnoj računarskoj mreži; neovlašćeno korišćenje računara ili računarske mreže. [1]

4. BEZBJEDNOSNI RIZICI I PRIJETNJE ZLOUPOTREBE INTERNETA I CYBER KRIMINALA

Zloupotreba interneta može da se vrši na različite načine i široka je lepeza mogućnosti kojima se internet može upotrijebiti u pravcu društveno negativnih tokova. Sajber kriminal je dakle, izuzetno širok pojam i on predstavlja oblik kriminala koji se prevashodno vrši putem kompjutera, kompjuterskih mreža i kompjuterskih sistema. Kako je to imaginaran, odnosno apstraktan prostor, jasno je da se on praktično vrši u elektronskom okruženju. Računarski kriminalitet se određuje kao skup različitih oblika delinkventnog ponašanja, gdje računar predstavlja sredstvo ili cilj kažnjivog djela (pri čemu bi ovdje spadala i ponašanja koja još uvijek nisu inkriminisana, ali koja bi, da su se koristila nekim drugim sredstvom sigurno predstavljala krivično djelo), dok se nadalje u računarski kriminalitet uključuju i svi umišljajni kažnjivi napadi na tuđu imovinu, počinjeni u vezi sa elektronskom obradom podataka.[14] Bezbjednosna problematika koja se odnosi na zloupotrebu interneta predstavlja svojevrsnu zamku u pogledu uticaja i iskorištavanja lakovjernosti i lakomislenosti internet korisnika. U društveno nesređenim okolnostima koje su propraćene velikim ekonomskim razlikama društvenih kategorija, rizik zloupotrebe

se može spočitavati u vrbovanju socijalno nezadovoljne kategorije društva u smislu iskazivanja nezadovoljstva sa aktuelnim stanjem u društvu bilo da je riječ o ekonomskim, političkim, vjerskim ili bilo kojim drugim segmentom društvenog uređenja a što za konačnicu ima destabilizovanje poretka, zarad ostvarivanja viših ciljeva i interesa. Naravno, kriminalne aktivnosti koje pozitivno pravo prepoznaje kao inkriminisane radnje ovdje nisu isključene, ali se prioritet daje problematici koja direktno utiče na državni mehanizam funkcionisanja. Kao neograničen medijski prostor kojim se internet i smatra, može se u svrhu postizanja određenih destabilizujućih ciljeva usmjerenih protiv državnih faktora uticati direktno ili indirektno, propagandnim metodama i sredstvima na ljudsku svijest i psihu kako bi se preduzele određene društveno devijantne i socijalno netolerantne aktivnosti. U kontekstu navedenog, kao rizično ponašanje na internetu ogledaju se sve slobodniji i otvoreni pozivi na razračunavanje sa državnim faktorima putem konvencionalnih sredstava u čijim pozivima posredstvom propagande jasno su poruke obojene govorom mržnje. Kao posledica ovakvih oblika zloupotrebe interneta pojavljuju se sve češće secesionistički, separatistički i teroristički akti, koji kako u svijetu, tako i kod nas predstavljaju ozbiljnu bezbjednosnu problematiku, a nemogućnošću kontrolisanja internet prostora bezbjednosni hazard od ovakvih pojava je sasvim izvijestan. Kao područje primjene interneta u oblasti terorizma koristi se odašiljanje podataka i informacija, teroristički sajtovi, finansiranje, rad u mreži, regrutovanje, prikupljanje podataka, itd.[1] Posebnost problematike zloupotrebe interneta ogleda se između ostalog i u sve češćoj pojavi rizika i prijetnji koje se odnose i na problematiku nasilničkog ponašanja koje internet kao prostor može da dozvoli u smislu kako uticaja i podstrekavanja na nasilničko ponašanje, tako i kao sredstvo putem kojeg se nasilničko ponašanje organizuje i priprema za realizaciju. U smislu nasilja posredstvom interneta karakteristično je međuvršnjačko nasilje. Međuvršnjačko nasilje putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijedjanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara. Svakako da je ovo jedan od segmenata koji kao skup rizičnog ponašanja mora da zabrine državu u smislu stvaranja bezbjednosnog koncepta, gdje su često mladi ljudi ugrožene grupe koje su obuhvaćene indukovanim rizičnim nasilničkim ponašanjem. Informacije i podaci dobiveni putem interneta, odnosno njegovom zloupotreboru mogu se iskoristiti u različite svrhe i ciljeve. U tom smislu, pored gore navedenih rizika i prijetnji, mogli bi kao dodatne rizike navesti još i : protivpravno korišćenje usluga i neovlašćeno pribavljanje informacija, kompjuterske krađe, kompjuterske prevare, kompjuterske sabotaže i kompjuterski terorizam i kriminal vezan za kompjuterske mreže. S tim u vezi, prema Evropskim standardima mogli bi da razlikujemo krivična djela sajber kriminaliteta kao: **1.Djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja, (proizvodnja, prodaja, uvoz, distribucija), programa, pasvorda;** **2.Djela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;** **3.Djela vezana za sadržaje, (dječja pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posjedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka);** **4.Djela vezana za kršenje autorskih i srodnih prava koja obuhvataju reprodukovanje i distribuciju neautorizovanih primjeraka i sredstva za efikasnu istragu i zaštitu.**

Zavisno od tipa počinjenih djela sajber kriminal može biti: **Politički** (*sajber špijunaža, haking, sajber sabotaža, sajber terorizam, sajber ratovanje*); **Ekonomski** (*sajber prevare, haking, krađa internet usluga i vremena, piratstvo softvera, mikročipova i baza podataka, sajber industrijska špijunaža, prevare na internet aukcijama - neisporučivanje prizvoda, udruživanje radi postizanja veće cijene,trgovina robom sa crnog tržišta*); **Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja** (*dječja pornografija, pedofilija, vjerske sekte,širenje rasističkih, nacističkih i sličnih ideja i stavova zloupotreba žena i djece*); **Manipulacija zabranjenim proizvodima, supstancama i robama** (*drogom, ljudskim organima i oružjem*); **Povrede sajber privatnosti** (*nadgledanje e-pošte, spam prislушкиvanje, snimanje "pričaonica", praćenje e-konferencija, nedozvoljeno kaćenje*).[15]

4.1. Odnos internet zavisnosti i kriminala

Internet kao globalna mreža predstavlja pravi izazov bezbjednosnih službi u domenu kontrole, nadzora i prevencije, jer je ova oblast veoma specifična i zahtijeva višestruke bezbjednosne napore kako bi se minimizirali rizici i prijetnje. Može se reći da se bezbjednosni problem na internetu najčešće zanemaruje, sve do onih momenata, kada on postane aktuelan, odnosno kada se desi nešto što predstavlja

inkriminisanu radnju, ili pak predstavlja svojevrsnu bezbjednosnu pojavu koja ima, ili može da ima negativne konotacije. Kvantitativna ekspanzija interneta manifestovana pojavom subjekata koji ga koriste i korisnika – zavisnika, svakako da predstavlja problematiku svojevrsnog cenzurisanja internet sadržaja, ali pored toga, dalekosežnije su posledice koje se pojavljuju njegovim uticajem na psiho-socijalne odluke njegovih konzumentata, koji često pribjegavaju vršenju kriminala, bez obzira da li to vrše putem interneta, ili je internet na direktni ili indirektni način uticao na njihovu odluku da izvrše neku aktivnost koja je pravno osuđujuća. Prethodno smo naveli koje kategorije lica su najčešće internet zavisnici i koje psiho-socijalne indikacije ova vrsta zavisnosti ostavlja na ta lica. Uzevši u obzir da internet zavisnost može u negativnom kontekstu da utiče na ljudsku psihu, gdje se čovjek poistovijeti sa slobodom interneta, svakako je za očekivati da na psihički labilnije osobe, kojima ova zavisnost produbljuje ionako nestabilno psihičko i duševno stanje, inicira odluku za vršenje određenih kriminalnih aktivnosti a zahvaljujući mogućnosti pristupa sadržajima koji su društveno neprihvatljivi ili su društveno osuđujući a pri tome su lako dostupni i necenzurisani. Tako je često u praksi bilo prilike da se za pedofiliju i širenje dječje pornografije putem interneta, osumnjiči lice, za kojeg su radne kolege, poznanici ili komšije najčešće imali riječi hvale, sa objašnjnjem da je to lice bilo mirno, tiho, povučeno itd. Međutim, u toku istrage se utvrđi da je upravo to lice latentni internet zavisnik sa asocijalnim, depresivnim i drugim degradirajućim faktorima ličnosti. Kako je već navedeno da internet zavisnost negativno utiče na psihičke i socijalne funkcije čovjeka, to svakako uzima za pravo da se reaguje u smislu redukcije vremena koje se provodi na internetu. Naime, činjenica je da se u ekstremnim situacijama sajber zavisnost ljudi manifestuje i u zanemarivanju porodice, profesionalnih obaveza, prijatelja čak i fizioloških potreba. Može se reći da su ove kategorije ljudi vrlo često kvalifikovane kao sajber proganjitelji. Sajber proganjanje prije svega spada u zloupotrebu interneta a odnosi se na interpersonalne odnose. Praktično govoreći, sajber proganjanje sadrži on-lajn uznemiravanje. Postupci koje karakterišemo kao on-lajn uznemiravanje preraštaju u sajber proganjanje kada se neželjena komunikacija ponavlja, bilo da je direktna ili indirektna, i kada se vrši u određenom vremenskom periodu, putem jednog ili više sredstava internet ili neke druge vrste elektronske komunikacije. On-lajn uznemiravanje može biti direktno ili indirektno. Direktno podrazumijeva prijetnje, zastrašujuće poruke upućene žrtvi putem e-maila ili nekim drugim vidom internet komunikacije, slanje zaraženih poruka ili kompjuterskih virusa. Indirektno on-lajn uznemiravanje uključuje, ali nije ograničeno samo na širenje glasina o žrtvi na različitim internet forumima, potpisivanje žrtve na neželjene on-lajn servise, slanje poruka drugima u žrtvino ime.[16] Kada je riječ o sajber proganjanju tu se razlikuju određeni tipovi proganjitelja:[17] Prije svega pojavljuje se: **1. Osvetnički tip**, (Najčešće zastrašuju žrtvu a proganjanje se vrši i van virtualne stvarnosti. Većina ih ima kriminalni dosije, te su im najbliža nasilnička krivična djela. Žrtve često dobijaju bizarre i nepovezane poruke, prijeteće multimedijalne poruke, npr. fotografije leševa, mrtvačke glave i sl.). **2. Romantični tip**, (Bore se za osjećanja i naklonost žrtve. Najčešće koriste e-mailove, sajtove za upoznavanje itd. Ovakav tip najčešće ima uvid u detalje iz žrtvinog života. Često se radi o bivšim partnerima, bivšim prijateljima žrtve i osobama koje su žrtvi nepoznate, a koje žele da ostvare intimnu vezu sa njom. Postupci proganjanja od strane bivših partnera kreću se od jednostavnih poruka koje imaju za cilj obnovu veze do surovih prijetnji. Kod onih koji teže započinjanju romantične veze sa žrtvom prijetnja postaje sve ozbiljnija i učestalija kada shvate da su odbijeni). **3. Strpljiv tip**, (U ovu grupu spadaju lica koja su najčešće usmjereni prema konstantnom dosađivanju i iritiranju žrtava. Ovaj tip ne želi da ostvari emotivnu vezu sa žrtvom ali želi duboko da je uznemiri. Strpljiv proganjitelj najučestalije upućuje prijetnje žrtvi). **4. Tip koji djeluje u grupi**, (Ovaj tip sajber proganjitelja djeluje u grupi. Karakteristični postupci proganjanja su: prijetnje multimedijalnim i drugim porukama, prijetnje identitetu žrtve. Ovaj tip najčešće ne uznemirava osobu izvan virtualnog svijeta. U okviru ovog tipa treba razlikovati učinioce korporacijskog proganjanja, pri čemu institucija preuzima odgovornost za proganjanje). Pored sajber proganjitelja, kao internet zavisnici u sukobu sa zakonom mogu da se pojave i lica sklona ispoljavanju agresivnog, manjakalnog ponašanja. Ono što posebno predstavlja rizik od uticaja zloupotrebe interneta a što se može prepisati licima koja su mlađe dobi a pri tome su internet zavisnici, jeste problematika nasilničkog ponašanja koje internet kao prostor može da dozvoli u smislu kako uticaja i podstrekavanja na nasilničko ponašanje, tako i kao sredstvo putem kojeg se nasilničko ponašanje organizuje i priprema za realizaciju. U smislu nasilja posredstvom interneta karakteristično je međuvršnjačko nasilje. Međuvršnjačko nasilje putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhodenje, vrijedjanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara. Svakako da je ovo jedan od segmenata koji kao skup rizičnog ponašanja mora da

zabrine državu u smislu stvaranja bezbjednosnog koncepta, gdje su često mladi ljudi ugrožene grupe koje su obuhvaćene indukovanim rizičnim nasilničkim ponašanjem. Prije svega ovdje se misli na lica koja koriste socijalne mreže i mreže za razna dopisivanja i druženja kao što su Facebook, Twooo, Badoo i druge. Tako je u Srbiji zabilježen slučaj svirepog ubistva maloljetnice od strane lica za koje se utvrdilo da je preko društvene mreže Facebook zavodio maloljetnice.[18]

Pored ovoga, javnost u BiH je uz nemirio i događaj kada se u Mostaru desilo ubistvo kojem je prethodio dogovor za fizički obračun putem Facebook-a.[19] Postoje mnogobrojni inkriminirani primjeri u praksi koji su se desili a da je prethodno slobodni prostor korištenja interneta i mogućnost korištenja lažnog identiteta pored nebrojeno provedenih sati za računarom, upravo psihički „okidač“ da osoba nekome ili nečemu nanese neko zlo ili štetu. Često su prisutne ucjene i razne prijetnje objavljuvanja kompromitujućih sadržaja neke osobe putem interneta ukoliko se ne plati određeni iznos novca ili se ne učini neka usluga itd. Pored ovakvih, postoje još i ekstremniji slučajevi. Naime, internet u današnje vrijeme služi kao veoma moćno sredstvo za teroriste, kao i za vršenje krivičnih djela, ali, isto tako, internet služi i kao sredstvo propagande, širenja nemoralnih sadržaja, raznih nacionalističkih, retrogradnih i drugih društveno i globalno neprihvatljivih ideja. Naime, internet danas, pored ostalog, može da posluži i služi za uputstvo kriminalcima kako da najbolje izvrše krivično djelo, odnosno kako da ne budu uhvaćeni, za širenje pornografije, za propagandu političkih ideja i programa uopšte, za vršenje kriminalnih i terorističkih akata (putem interneta), za propagiranje mržnje i nasilja, za pranje novca, itd. Prednost interneta, a koju veoma dobro koriste kriminalci i teroristi, jeste da na internetu praktično ne postoji mogućnost fizičkog ugrožavanja lica koje vrši nedozvoljene akte, pa je i mogućnost redukcije tih akata bitno smanjena.[20] Sve ove informacije su lako dostupne licima koja mnogo vremena provode na internetu. Tako je vrlo moguće na internetu pronaći informaciju kako napraviti ili aktivirati određeno minsko eksplozivno sredstvo, kako otuditi vozilo, kako neutralisati alarmne sisteme radi vršenja razbojništava ili provala, kako se regrutovati u terorističke grupe itd. Dakle, od najbagatelnijih i najbezazlenijih informacija (poput kupovine student-bubica), do informacija kako izvršiti najteže oblike krivičnih djela, sa uputstvima da se sakriju tragovi od organa gonjenja, danas su dostupni na internetu. Ako se kombinuje internet zavisnost i beskonačna dostupnost različitih informacija, bez izvjesne kontrole, nadzora ili čak represivne reakcije, ishodi mogu biti katastrofalni.

Na osnovu istraživanja koja su sprovedena kako u svijetu, tako i u regionu, može se zaključiti da je internet zavisnost veoma rasprostranjena. Osobe koje se kategorisu u ovu skupinu su socijalno otuđeni, nepovjerljivi, depresivni, povučeni u sebe, nezadovoljni realnim životom, iskompleksirani, isfrustrirani, afektivni, ukratko rečeno retrogradni i sa određenim psihičkim smetnjama i poremećajima. Ukoliko se kao takvi, nađu na meti određenih, za to namjenjenih internet sadržaja koji podržavaju društveno neprihvatljive aktivnosti, tako psihički nestabilni, odnosno, kao osobe labilni, vrlo lako mogu svoja nezadovoljstva i fantazije sprovesti u djelo, počevši od bezazlenih radji pa sve preko samoubistava, ubistava, silovanja, do na kraju krajeva, terorizma i drugog brutalnog kriminala.

UMJESTO ZAKLJUČKA

Zavisnost od interneta je društveni fenomen koji htjeli to priznati ili ne, uveliko postoji kako u svijetu, tako i kod nas. Pretpostavka je da samo postoje različiti nazivi ili mišljenja o pojmovnom definisanju, ali suština je približno ista. Jasno je da kvantitativno utrošeno internet vrijeme, kvalitativno utiče na osobu, njeno stanje, osjećanja, mišljenja, ponašanje i na kraju krajeva, odluke. Ovakva pojava zahtijeva multidisciplinarni pristup koji bi se ogledao kako u preventivnom djelovanju, tako i u kliničkim tretmanima lica, odnosno zavisnika. Kao najranjivija kategorija korisnika interneta, ujedno i kao osobe koje ga najviše koriste, jesu upravo djeца i omladina. U tom smislu potrebno je sagledavati dječje mentalno i fizičko zdravlje koje svakako prekomernom upotrebom interneta i zbog same inertnosti psihofizički razvoj djece i omladine vodi degradirajućim pravcem. Kao nazadnost i potencijalni bezbjednosni faktor kojim bi se trebali baviti, kada je ovaj fenomen u pitanju jeste sve veća pojava asocijalnosti i otuđenosti, nezadovoljstva i gomilanje bijesa kod djece i omladine, te kao takva, a podstaknuta nasiljem putem interneta koji je necenzurisan, svakako da predstavljaju izazov i rizik (u ekstremnim slučajevima i prijetnju), koji je moguć da se manifestuje različitim socijalnim devijacijama. Upravo u ovom segmentu, potrebno je pored pravosudnih institucija i organa gonjenja prije svega u preventivnom smislu, ali i represivnom na kraju krajeva, uključiti i stručnjake iz psihologije, psihijatrije,

teologije, vjerske predstavnike, stručnjake za socijalni rad i aktivnost djece i omladine, kao i druge vladine i nevladine organizacije i institucije kako bi se ovaj problem sa djecom preduprijedio i kako ne bi došlo do neželjenih posledica. Sinergijom ovih institucija i organizacija rezultiralo bi se pozitivnim formiranjem djece u psihološki-fizički-socijalno zdravu omladinu.[1] Sa aspekta bezbjednosti i kriminalistike, internet zavisnost bez sumnje predstavlja svojevrsnu prijetnju po društveno prihvatljive norme ponašanja.

Pored ponašanja koja se mogu okarakterisati kao adolescentska kriza, postoje brojni modaliteti ispoljavanja kriminala putem interneta koje je nemoguće sveukupno nabrojati iz razloga svakodnevnog modifikovanja i unapređivanja oblika kriminala. Kao najčešći su razne internet prevare, krađe identiteta, provlađivanje u tuđe računare i računarske sisteme, krađa podataka i informacija, „krađa vremena“, razne krađe internet usluga, internet piraterija, pornografija i pedofilija, računarska sabotaža, računarska diverzija, teroristički akt realizovan (samo) uz pomoć interneta, razni oblici informacionog ratovanja, itd. a što zahtijeva veliko poznavanje informaciono komunikacionih tehnologija i nesagleđivo vrijeme utrošeno na internetu. Na kraju, u smislu cjelokupne internet zavisnosti, potrebno je primijeniti sinergiju djelovanja svih institucija kako bi se internet zavisnik iz virtuelnog svijeta vratio u realni svijet, te se kтивno uključio u društveno-socijalne tokove gdje bi se ona druga „podvojena ličnost“ sa svim prljavštinama čovjekovog uma maksimalno minimizirala ili barem svela na prihvatljiv nivo.

U smislu bezbjednosti, ovo bi se trebalo shvatiti kao proces a ne kao stanje, koji bi podrazumijevao podvrgavanje posebnim određenim standardima koji bi se zahtijevali i koji bi bili obavezujući za sve internet korisnike. Usled navedenog, bezbjednost na internetu mora da bude optimalno rješenje između suprotstavljenih koncepata posmatranja interneta - s jedne strane, posmatranog kao „poslednje utočište slobode“ koje je determinisano konceptom neutralnosti mreže, odnosno uticaja formalnih ograničenja formalnih subjekata lokalne, nacionalne ili globalne zajednice, te, s druge strane, nastojanja upravo tih zajednica da na određeni način regulišu sve brojnije i frapantnije slučajevje kršenja bezbjednosti kojima se narušava lični, ali i nacionalni, pa i globalni integritet korisnika interneta.[20]

LITERATURA

- [1] BLAGOJEVIĆ, G.: „Bezbjednosni hazardi i legislativa zloupotrebe interneta“ Rizici i bezbjednosne prijetnje, Zbornik, 2015. god., str.327-328.
- [2] MILADINOVIC, A.: „Fejsbuk i kriminalitet“, Visoka škola unutrašnjih poslova Banja Luka, 2013.
- [3] GIDENS, E.: „Sociologija“, Ekonomski fakultet Beograd, 2001.
- [4] KOVAČEVIĆ-LJEPOJEVIĆ, M.: „Pojam i karakteristike internet zavisnosti“ Specijalna edukacija i rehabilitacija, Vol. 10, br. 4., 2011. god., str. 618.
- [5] BAI, Y., CHAO-CHENG, L., CHEN, J.: „Internet Addiction Disorder Among Clients“ Virtual Clinic, Psychiatric services, 52 (10), 2001. god., str. 1397.
- [6] DAVIS, R.A. : „A cognitive-behavioral model of pathological Internet use“. Computers in Human Behavior, 17 (1), 2001. god., str. 187–195.
- [7] YELLOWLEES, P., MARKS, S.: „Problematic Internet use or Internet addiction“? Computers in Human Behavior, 23 (3), 2007. god., str. 1450.
- [8] <http://www.internetoveruse.com/wp-content/uploads/Internet-Addiction-Test.pdf>. (20.02.2016.)
- [9] YOUNG, K. S.: „Internet Addiction: A new clinical phenomenon and its consequences“ American Behavioral Scientist, 48 (4), 2004. god., str.402-415.
- [10] HINIĆ, D., MIHAJLOVIĆ, G., ŠPIRIĆ, Ž., ĐUKIĆ-DEJANOVIĆ, S., JOVANOVIĆ, M. : „Excessive Internet use – addiction disorder or not“? Vojnosanitetski pregled, 65 (10), 2008. god., str. 763–767.
- [11] YOUNG, K., PISTNER, M., O'MARA, J., BUCHANAN, J.: „Cyber disorders: the mental health concern for the new millennium“ Cyber Psychology and Behavior, 3 (5), 2000. god., str. 475-479.
- [12] CHOU, C., CONDRON, L., BELLAND, J.: „A review of the research on internet addiction“ Educational Psychology Review, 17 (4), 2005. god., str. 363-388.
- [13] HINIĆ, D.: „Korisnički profili internet zavisnika u Srbiji“ Psihologija, 41 (4), 2008. god., str. 435-453.
- [14] KRAPAC, D. : „Kompjuterski kriminalitet“, Pravni fakultet, Zagreb, 1992.

- [15] TANILIR, N.M., TAHIROVIĆ, M.: „*Međunarodna bezbjednost i sajber opasnost*“, Monet., Vol. 34, Podgorica, 2013.god., str. 10-11.
- [16] ELLISON, L., AKDENIZ, Y. : „*Cyber-stalking:The regulation of harassment on the Internet*“, Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, 1998. god., str. 31.
- [17]<http://www.socioloskaluca.ac.me/PDF18/Vujovic,%20T.,%20Zavisnost%20od%20interneta%20i%20interpersonalno%20nasilje%20u%20sajber%20prostoru.pdf>. (26.02.2016.).
- [18] <http://www.klix.ba/vijesti/regija/tijanin-ubica-preko-facebooka-zavodio-maloljetnice-i-pozivao-naseks/140814007>. (26.02.2016.).
- [19] <http://tip.ba/2015/12/21/detalji-ubistva-dzani-sa-svojim-ubicom-susret-dogovorio-preko-facebooka/>. (26.02.2016.).
- [20] MILAŠINOVIC, R., MIJALKOVIĆ, S., AMIDŽIĆ, G.: „*Bezbednost i internet*“ Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Zbornik, Banja Luka, 2012. god., str. 34.

CYBER SIGURNOST U EU ZEMLJAMA

Perenda Halid

perenda.halid@gmail.com

Apstrakt: U ovome radu će biti obrađeni podaci iz istraživanja koje je izvršeno u svim EU zemljama sa više od 27.000 ispitanika. Ovi ispitanici su iz različitih socio-demografskih skupina a ispitani su svi relevantni podaci vezani za cyber kriminal.

Ključne riječi: cyber kriminal, EU istraživanje, statistički podaci.

UVOD

Cyber kriminal predstavlja problem koji ne poznae granice i sastoji se od kriminalnih aktivnosti koje su počinjene online koristeći elektronske komunikacione mreže i informacione sisteme a uključuje specifične vrste kriminalnih aktivnosti kao što su online prevare i iznude kao i objavljivanje ilegalnih sadržaja. Globalne računarske mreže stvorile su mogućnosti za nove pojavnje oblike kriminala. Pokazalo se kako nacionalna zakonodavstva više nisu dosta na za efikasno regulisanje sve većeg broja novih društvenih odnosa koji traže pravnu regulaciju.

Iako nije tačno poznato koliko cyber kriminal utječe na ekonomiju zemalja pretpostavlja se da se gubici mjeru u bilionima eura godišnje. Sa sve većim razvojem cyber kriminala svake godine Europska komisija je organizovala koordinirane policijske akcije zajedno sa svim europskim državama kako bi se smanjio ovaj utjecaj. Kada je riječ o zakonskoj regulativi u borbi protiv cyber kriminala ona podrazumjeva napade protiv informacioni sistema, dijeljenje uvredljivih materijala i dječje pornografije, kao i napade na online sigurnost i online prevare kao i krivotvorene. U našoj zemlji je još u 2012 godini prepoznata potreba da se agencije za sprovođenje zakona spreme da se efikasno i efektivno bore protiv svih oblika cyber kriminala. U današnjem okruženju ne postoji sistem koji je apsolutno siguran i otporan na cyber kriminal bilo da se radi o napadima sa interneta uz pomoć raznih malicioznih programa ili da se radi o ljudskom faktoru poput krakera, vandala, cyber terorista itd.

Pravni osnov za postupanje u oblasti cyber kriminala je ustanoavljen u našoj zemlji usvajanjem konvencije o visokotehnološkom kriminalu ili konvencije o kibernetičkom kriminalu.

U ovome radu će biti obrađeni podaci iz istraživanja koje je obavljeno u svih 28 zemalja Europske unije sa više od 27 hiljada ispitanika. Ovi ispitanici su iz različitih socijalnih i demografskih grupa. Nažalost u ovome istraživanju nije obuhvaćena Bosna i Hercegovina dok su istraživanjem obuhvaćeni naši susjedi kao što su Srbija i Makedonija.

1. KORIŠTENJE INTERNETA

Istraživanje je pokazalo da je korištenje interneta još uvijek veoma različito zavisno u kojoj zemlji se nalazimo. Iako većina građana 63% kaže da svakodnevno koristi internet tako imamo i procenat od 24% građana koji nikada nisu koristili internet. Za razliku od do sada uobičajenog načina korištenja interneta preko računara čak 92% ispitanika sve veći je broj korisnika interneta preko telefona oko 61% i preko tableta 30%. korištenje telefona i tableta za korištenje interneta je se drastično povećalo u odnosu na istraživanje iz 2013 godine. Više od pola korisnika interneta u EU kažu da koriste internet za pristupanje e-mailu 86%, čitaju novine online 63%, pristupaju socijalnim mrežama 60% i kupuju stvari i usluge online 57% ili obavljaju internet bankarstvo 54%. korištenje svih ovih servisa je se drastično povećalo od istraživanja u 2013 godini a nama posebno interesantni podaci su o korištenju interneta za internet bankarstvo kao i kupovinu stvari i usluga online.

Tokom korištenja interneta za online kupovinu ili bankarstvo dvije najveće brige korisnika su neovlašteno korištenje ličnih podataka 43% kao i sigurnost prilikom online plaćanja 42%. građani EU su sada mnogo više zabrinuti za svoju online sigurnost nego što je to bilo ranijih godina.

Tako uporedno sa rezultatima ovog istraživanja su interesantni podaci da ljudi mijenjaju svoje navike za razliku od istraživanja u 2013 godini: 61% ljudi je instaliralo antivirusni softver, 49% ljudi ne otvara e-mailove od nepoznatog pošiljaoca dok 38% korisnika ne žele da otkrivaju svoje prave podatke na web stranicama.

Malo povećanje je primijećeno kada je riječ o informiranost kada je riječ o cyber kriminalu. Tako imamo sljedeće podatke da tek oko 47% korisnika u EU se osjeća dovoljno dobro informisanim o cyber kriminalu. Internet korisnici su izrazili visok nivo zabrinutosti za svoju cyber sigurnost, tako da 89% korisnika ne želi davati svoje informacije online dok se 85% slaže da je povećan rizik da se postane jedna od žrtava cyber kriminala. Visok je nivo onih koji su zabrinuti za svoje informacije zbog toga što ih web stranice ne čuvaju dobro a to je čak 73% dok je 67% ljudi mišljenja da institucije ne ulažu dovoljno npora da sačuvaju lične podatke.

Dva od tri internet korisnika u EU zemljama su zabrinuti da se ne suoče sa krađom identiteta 68% dok je više od polovine građana zabrinuto da ne postanu žrtve internet bankovne prevare 63%. i ostale vrste prevare nisu ništa manje zastupljene pa su tako građani u strahu od hakovanja e-maila ili telefonskih poziva 57% kao i hakovanja njihovih računa na socijalnim mrežama 60%.

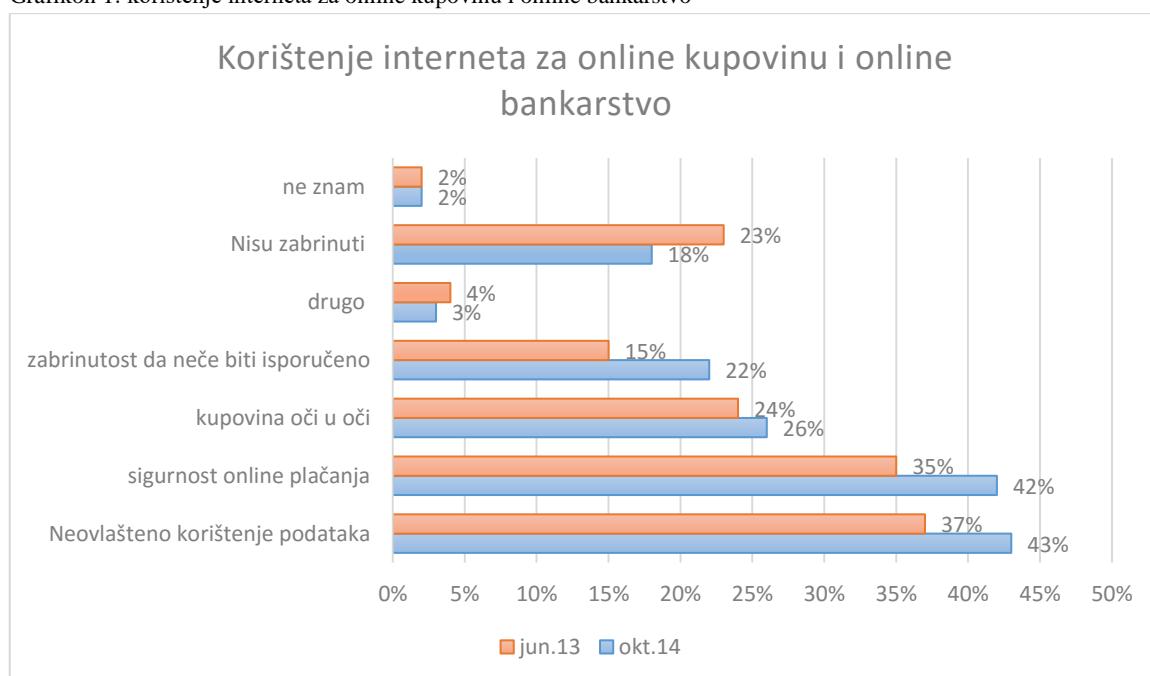
Veoma mali nivo potrebnih koraka se poduzima da se zaštite djeca dobi ispod 16 godina koja su online pa tako samo 22% roditelja prati korištenje interneta, govori o rizicima korištenja interneta sa svojom djecom 22%, ograničava vrijeme provedeno na internetu 18% i prilagođava sigurnosne postavke pretraživača tek 13%.

2. ZABRINUTOST ZA CYBER KRIMINAL

Kao što smo već ranije napomenuli ovo istraživanje je obuhvatilo i podatke o korištenju interneta za stvari kao što su online bankarstvo i online kupovina stvari i usluga. Internet korisnici su najviše zabrinuti kao što smo već spomenuli za neovlašteno korištenje njihovih podataka na internetu kao i sigurnost prilikom plaćanja računa online. Takođe jedan manji dio ljudi su zabrinuti da neće primiti stvari koje kupe online 22% dok je jedan od šest korisnika izjavio da nema briga kada su u pitanju online transakcije a to čini 18%.

Ono što je evidentno je da ljudi sada za razliku od istraživanja iz 2013 godine su mnogo više zabrinuti za njihovu online sigurnost. Ovo se posebno odnosi na neovlašteno korištenje njihovih podataka pa tako 43% ljudi su zabrinuti da će se njihovi podaci koristiti neovlašteno za razliku od istraživanja iz 2013 godine kada je ta brojka bila 37%. primjetno je povećanje zabrinutosti i za online plaćanja 42% na prema 35% kao i da neće dobiti plaćenu robu 22% na prema 15%.

Grafikon 1: korištenje interneta za online kupovinu i online bankarstvo



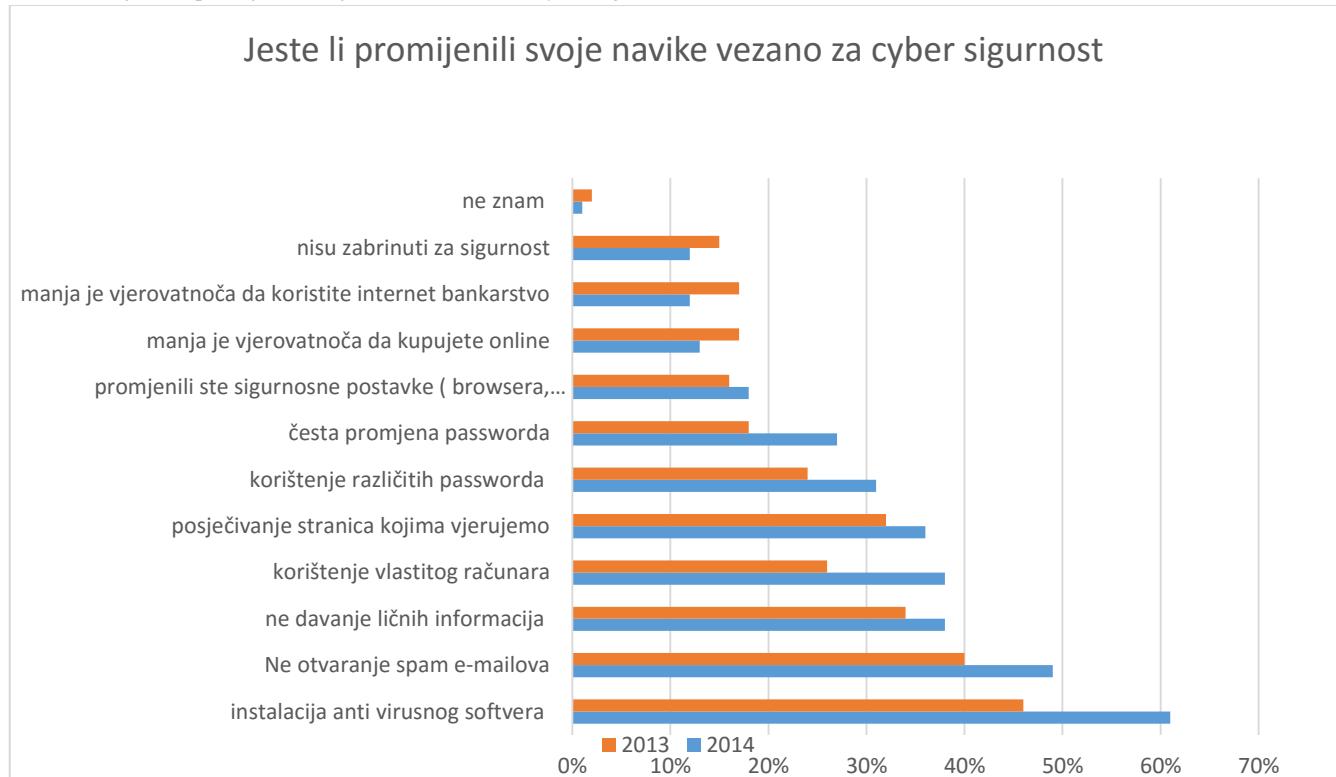
Izvor: Special Eurobarometer 423 cyber security

Zabrinutost korisnika kada je u pitanju cyber kriminal varira različito od zemalja u kojima se nalaze. Korisnici u Njemačkoj, Španiji i Luksemburgu su najviše zabrinuti zbog neovlaštenog korištenja ličnih podataka i to preko 50% dok su korisnici iz Irske najviše zabrinuti za sigurnost prilikom online plaćanja sa 53%.

3. CYBER KRIMINAL I UTJECAJ NA PONAŠANJE KORISNIKA

Nakon istraživanja iz 2013 godine korisnici su umnogome promijenili svoja pravila ponašanja na internetu. Akcije koje su najviše poduzimane da bi se zaštitili su instalacija anti virusnog softvera 61%, kao i ne otvaranje e-mailova koji dolaze od nepoznatih korisnika 49%. kada je riječ o drugim promjenama korisnici manje žele da dijele svoje privatne informacije na web stranicama 38% kao i trude se da koriste svoj lični računar i posjećuju stranice za koje znaju da su sigurne. O drugim akcijama kada je u pitanju zaštita sigurnosti na internetu najviše je spominjana promjena sigurnosnih postavki pretraživača 18%, dok je 13% korisnika sada manje sigurno u online kupovinu a 12% je otkazalo korištenje internet bankarstva. U istraživanju iz 2013 godine korisnici nisu bili pitani o čestim promjenama passworda i ova opcija je dodana tek u ovom istraživanju. U poređenju sa ranijim istraživanjem možemo vidjeti mnoge pozitivne pomake kao što su instalacija anti virusnog softvera, korištenje ličnog kompjutera za online bankarstvo i online plaćanje kao i korištenje različitih passworda za različite stranice. Činjenica je da su korisnici preuzeli dosta mjera kako bi se zaštitili od cyber kriminalaca i zabrinuti su za svoju online sigurnost.

Grafikon 2. jeste li promijenili svoje navike vezano za cyber sigurnost



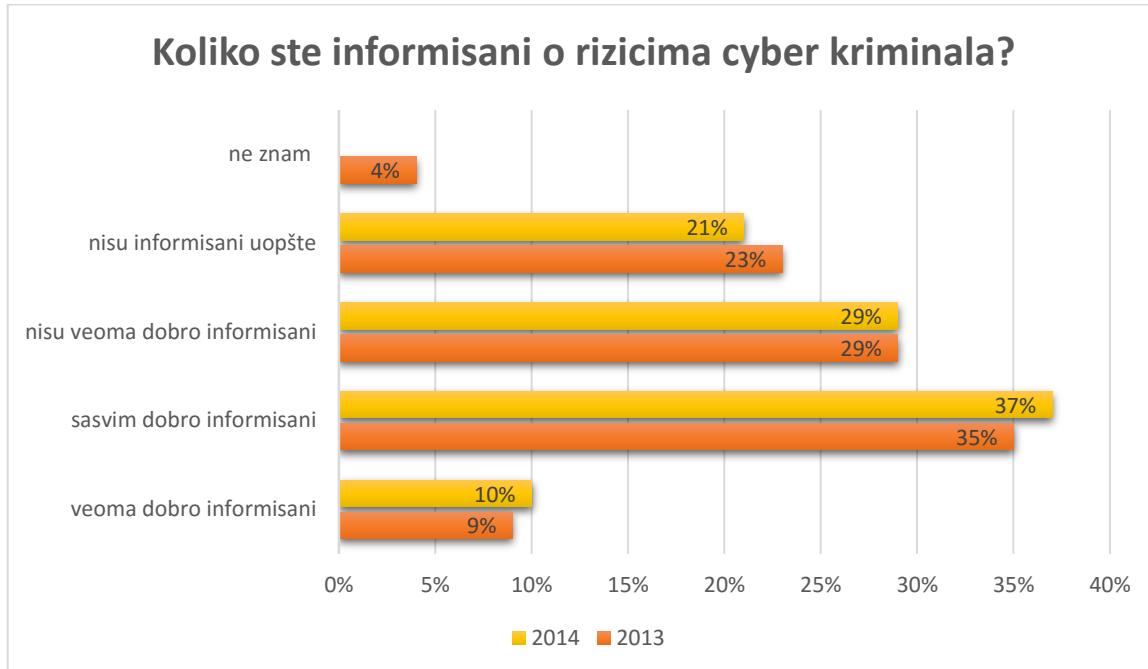
Izvor: Special Eurobarometer 423 cyber security

Gledajući pojedinačno korisnici su najčešće u mnogome promijenili svoje navike o korištenju interneta zbog zabrinutosti za svoju online sigurnost i to najviše u zemljama poput Švedske 96%, Holandija 98%, Danska 95% i Austrija 95%. najmanje promjene su uočene u zemljama poput Poljske, Rumunije kao i Ujedinjenog Kraljevstva 80%.

4. NIVO ZNANJA O CYBER KRIMINALU

Negdje oko polovina EU građana 47% kažu da su veoma dobro informisani o rizicima cyber kriminala, 10% se osjeća veoma dobro informisani po ovom pitanju dok je 37% donekle informisani . međutim imamo i veliki procenat onih koji se se ne osjećaju dovoljno informisanim 29% a 21% građana se izjašnjava kao da nisu uopšte informisani o rizicima cyber kriminala.

Grafikon 3: koliko ste informisani o rizicima cyber kriminala?



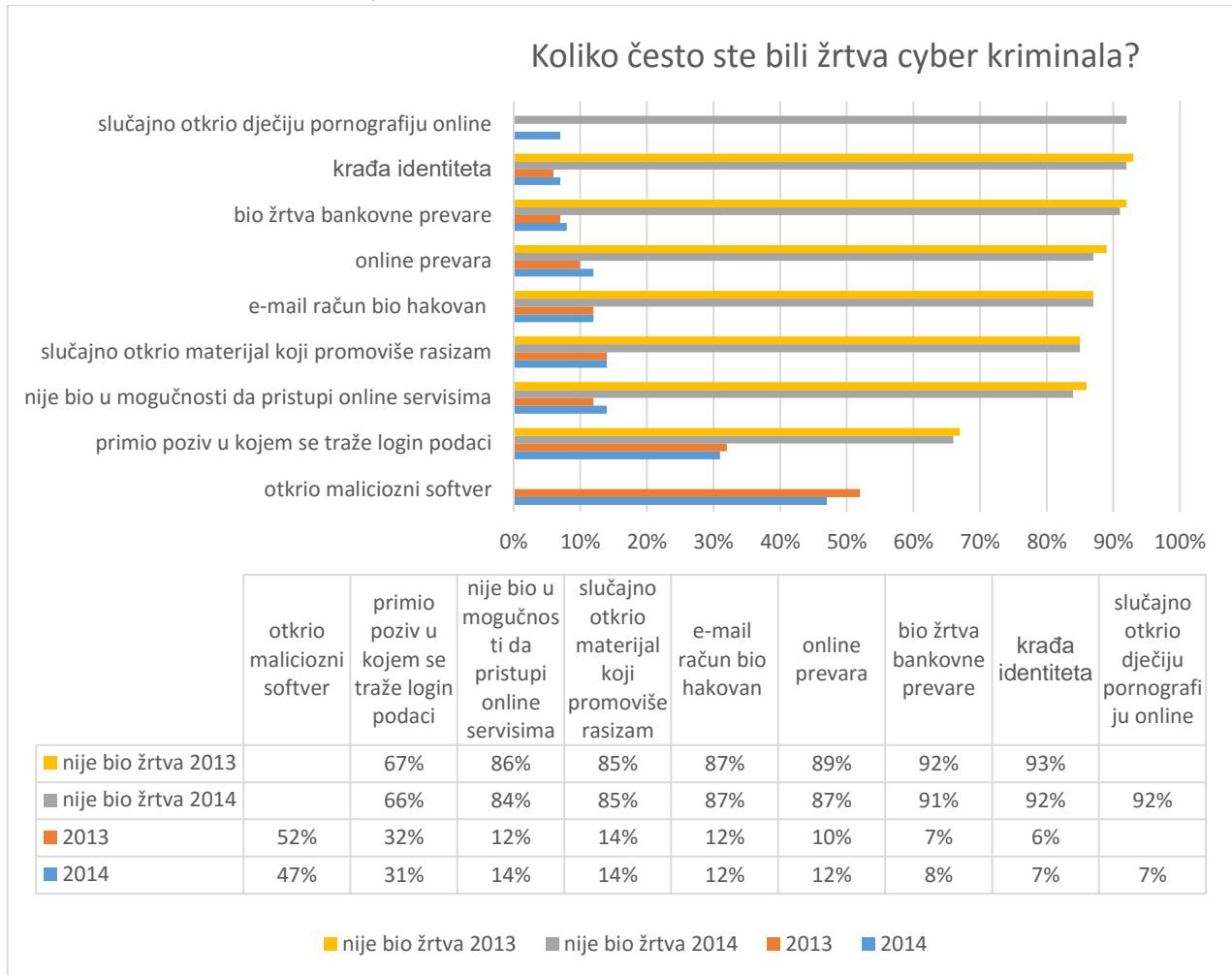
Izvor: Special Eurobarometer 423 cyber security

Kao i kod svakog drugog pitanja postoje razilaženja po pitanju informiranost o cyber kriminalu. Građani u bolje razvijenim zemljama poput danske 67%, Švedske 66% i UK 65% se bolje informisani o rizicima cyber kriminala nego slabije razvijene zemlje poput Rumunije 31% i Bugarske 34% gdje je zabilježen najveći broj odgovora da ljudi uopšte nisu informisani o rizicima cyber kriminala. Naravno ovakav odgovor nije uopšte začuđujući kada uzmemu u obzir broj korisnika interneta koji je u razvijenim zemljama skoro 100%. najviše poboljšanja je primijećeno u Austriji 14% kao i Portugalu 13% dok je u nekim zemljama zabilježen pad informisanosti o cyber kriminalu Luksemburg 10% pad informisanosti.

5. ZABRINUTOST I ISKUSTVA SA RAZNIM DJELIMA CYBER KRIMINALA

U ovome dijelu istraživanja ispitivani su stavovi jesu li korisnici bili žrtve cyber kriminala i kakvo je njihovo iskustvo prilikom toga. Kao što smo već ranije napomenuli najviše zabrinutosti je zbog krađe identiteta a nakon toga slijedi otkrivanje zlonamernog softvera na nekom od njihovih uređaja. Internet korisnici su takođe zabrinuti za mogućnost da budu žrtve online bankovne prevare.

Grafikon 4: koliko često ste bili žrtva cyber kriminala?

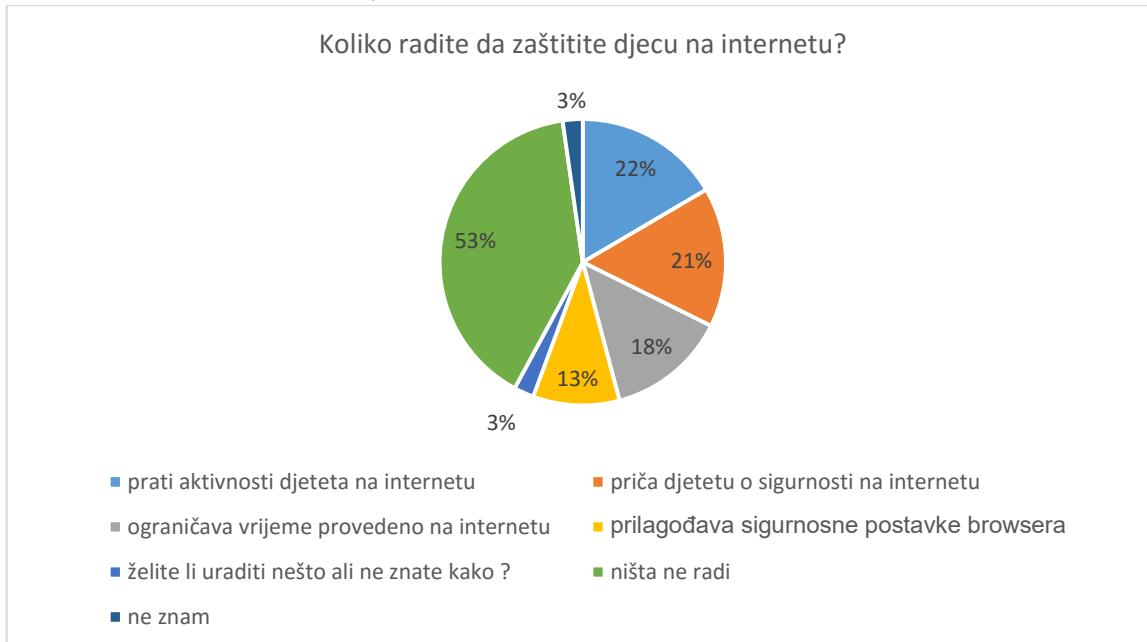


Izvor: Special Eurobarometer 423 cyber security

6. BORBA PROTIV CYBER KRIMINALA

Svi ispitani korisnici su takođe odgovarali na pitanje koliko i u kojoj mjeri su zaštitili svoje ukućane od cyber kriminala, sveukupno od deset korisnika internet njih četiri tj 38% pokušali su da zaštite svoju djecu ispod 16 godina starosti dok su online na neke od načina. Jedan od pet korisnika kažu da prate dječije aktivnosti na internetu(22%), dok sličan broj njih tvrdi da poduzima mjere da bi podučili djecu o opasnostima koje vrijebaju na internetu (21%) a 18% roditelja ograničava vrijeme provedeno na internetu. Veoma mali broj korisnika mijenja i prilagođava sigurnosne postavke internet pretraživača da bi zaštitio djecu tek 13%. Ono što je veoma važno napomenuti je i činjenica da je na ova pitanja odgovaralo oko 48% korisnika iz razloga što drugi nemaju djecu ispod 16 godina.

Grafikon 5: koliko radite da zaštitite djecu online?



Izvor: Special Eurobarometer 423 cyber security

Podaci koji su čudni je da se u razvijenijim zemljama poput Njemačke mnogo manje brine za sigurnost djece na internetu nego što je to u Hrvatskoj na primjer tj 52% na prema 26% u Njemačkoj. Veoma dobre rezultate postižu naši susjedi Hrvatska kada je u pitanju zaštita djece na internetu pa su tako u vrhu liste zajedno sa Luksemburgom, Francuskom itd.

Socio demografske varijacije pokazuju da prosječni korisnici interneta su oni koji se osjećaju veoma dobro informisanima o rizicima cyber kriminala i i čine sve da zaštite svoju djecu online. Tako npr 26% prosječnih korisnika interneta govori svojoj djeci o rizicima na internetu dok 22% korisnika koji manje koriste internet i 9% onih koji ne koriste internet. Većina korisnika interneta na pitanje koga bi pozvali da budu jedna od žrtava cyber kriminala su odgovorili sa policiju a tek zatim bi se obratili stranici na kojoj su bili izloženi cyber kriminalu a potom i davatelju internet usluga.

ZAKLJUČAK

U ovome izvještaju su ispitivani stavovi EU građana i njihova mišljenja o različitim oblicima cyber kriminala i uspoređivani su sa istraživanjem iz 2013 godine.

Mnogi od ispitanika su promijenili svoje mišljenje iz sigurnosnih razloga, i nerado otkrivaju svoje informacije na internet stranicama i ne otvaraju e-mailove od nepoznati osoba. Rezultati koji su predstavljeni u ovome istraživanju su većinom poboljšani u odnosu na istraživanje iz 2013 godine a naročito se razlikuju rezultati individualnih zemalja kao i različitih dobnih grupa i nivoa obrazovanja.

EU građani se osjećaju bolje informisanima o rizicima cyber kriminala nego što je to bio slučaj ranijih godina i većina korisnika se osjeća spremnim da se zaštiti od cyber kriminalaca. Skoro polovina ispitanika je otkrila neki od malicioznog softvera na njihovim uređajima. A skoro trećina njih tvrde da su primili spam e-mailove ili telefonske pozive. Manji je broj onih korisnika koji su bili žrtve online prevara, krađa identiteta kao i hakovanja e-mail računa ili računa na socijalnim mrežama.

Ispitivane grupe su izrazile veliku zabrinutost zbog cyber kriminala. Većina a se slaže sa činjenicom da je povećan rizik da se postane žrtva cyber kriminala i strahuju da njihovi lični podaci nisu sigurni na web stranicama kao ni u javnim institucijama.

LITERATURA

- [1] Special eurobarometer 423 cyber security report, October 2014
- [2] <http://ec.europa.eu/eurostat> datum pristupa 02.03.2016

ODREDNICE EKSTERNALIZIRANIH PROBLEMI ADOLESCENATA U VIRTUELНОM OKRUŽENJU

Mr Edina Heldić-Smailagić⁴

Visoka škola unutrašnjih poslova Banjaluka, edina_heldic@yahoo.com

Apstrakt: Svedoci smo vremena u kojem važno mjesto za komunikaciju, upoznavanje i formiranja odnosa sa drugima, kao i za izgrađivanje i stvaranje slike o sebi, predstavlja virtuelno okruženje ili virtualni svijet. Razvijanjem savremenih informacionih tehnologija razvijao se interes za upotrebu, ali i zloupotrebu dimenzija virtualnog svijeta, prvenstveno misleći i govoreći o ekspanziji popularnosti korištenja društvenih mreža (Facebook, Instagram, Twitter...). Koliko god virtualni svijet putem nedirektnе komunikacije nudio brže načine povezivanja, on u sebi nosi izvjesnu težinu, koja se ogleda u nekontroli ponašajnih aspekata ličnosti. Društvene mreže obiluju raznim oblicima indirektnе agresivnosti, ali je u nekim prilikama i sredstvo putem kojeg se pozivaju i organizuju adolescenti da eksternalizuju svoje negativne emocije prema društvu ili pojedincima. Veliki broj adolescanata je ovisan od korištenja Interneta, al najviše kada se govori o korištenju društvenih mreža, na kojoj ispoljavaju često agresivno i delinkventno ponašanje, koje ne percipiraju dovoljno ozbiljno u odnosu na to isto ponašanje u stvarnom okruženju. Istraživanja su pokazala da čak pojedinci koji su agresivni na socijalnim mrežama takvi nisu u stvarnom životu. Uvodni dio rada će sadržavati opšte odrednice o adolescenciji kao najosjetljivijem razdoblju razvoja ličnosti, kao i eksternaliziranim problemima koji često prate ovaj turbulentan i dinamičan period života svake osobe. Drugi dio rada će govoriti o nekim teorijskim odrednicama koji sagledavaju svijet socijalne patologije, u ovom slučaju patološkim oblicima ponašanja koji se pojavljuju u virtuelnom okruženju.

Ključne riječi: eksternalizirani problemi, agresivno ponašanje, adolescencija, virtuelno i stvarno okruženje, percepcija, društvene mreže, etiologija

UVODNA RAZMATRANJA

Adolescencija je izuzetno osjetljivo doba za svakog pojedinca, u kojem se očekuje nagli prelaz na veći stepen emocionalnog, kognitivnog i socijalnog razvoja. Taj prijelaz od djetinjstva ka odraslomu dobu predstavlja jedan buran, nestabilan i dinamičan period, kojeg ipak većina prebrodi bez značajnih emocionalnih problema. Pored tjelesnih promjena ovaj prijelaz je potaknut sve važnijom i snažnijom ulogom vršnjaka i novootkrivenom kognitivnom sposobnošću koja omogućuju adolescentu da razmišlja o budućim događajima i da proširi spoznaju o sebi, kako bi pronašao odgovor na pitanje „ko sam ja“. Adolescent se susreće sa zadatkom postizanja identiteta, suočen sa nakupljenim snagama i slabostima iz prošlosti- povjerenjem, autonomijom, inicijativom i produktivnošću, na pozitivnoj strani, odnosno nepovjerenjem, sramom, sumnjom, krivnjom i ineferiornošću, na negativnoj (Wenar, 2003). Potraga za identitetom je najčešće praćena dubljim odnosima sa vršnjacima i nešto manje stabilnim odnosima s roditeljima. Za adolescente je jako važan odnos sa vršnjacima, odnosno za njega je primaran njegov status u grupi i on nastoji da bude priznat od strane svojih vršnjaka. Zbog toga je jedan od najvećih pretnji u adolescenciji upravo vezan za vršnjake. Adolescenti se vrednuju u odnosu na vršnjake i nema sumnje da najveći dio novih vrijednosti prihvataju od vršnjaka i njihovih idola, često pogrešno izabranih. Težnja za popularnošću je jedna od „zvijezda vodilja“ adolescenata na putu ka odraslomu dobu. Upravo ta neodoljiva želja za prihvatanjem od strane drugih i težnja da se zauzme neki važan položaj u vršnjačkoj grupi, a s druge strane potraga za samim sobom i društvene obaveze koje pritišću, čine adolesceniju izuzetno plodnim tlo za nastajanje niza socijalno neprihvatljivih ponašanja i poremećaja. Među njima značajno mjesto zauzima agresivno i antisocijalno ponašanje, ili drugim riječima napisano, eksternalizirani problemi, koji adolescenti ispoljavaju u primarnoj zajednici, a zatim i u širem okruženju, unutar koje značajno, ako ne i najznačajnije mjesto, zauzima virtualni svijet, odnosno lični prostor u internet zajednici.

⁴ Visoka škola unutrašnjih poslova Banjaluka, edina_heldic@yahoo.com, stručni saradnik za opšteobrazovnu grupu predmeta

Eksternalizirani problemi su se počeli pojavljivati ili vezati za virtuelno okruženje, pogotovo ako se uzme u obzir da je zajedno s razvojem i ekspanzijom računarske tehnologije internet postao standradni način komunikacije adolescenata. Povezanost društvenih mreža i eksternaliziranih problema, u kontekstu agresivnih oblika ponašanja na internetu, prevashodno se može posmatrati kroz prijetnje, vređanje, ponižavanje, zlostavljanje, uhođenje, iritiranje, lažno predstavljanje i mnoge druge oblike negativnog ponašanja. Povezanost ostalih oblika agresivnog i delinkventnog ponašanja i društvenih mreža se ogleda u činjenici da su problematičnim adolescentima društvene mreže sredstvo za podstrekavanje, vrbovanje i omasovljavanje saputnika na delinkventnom putu. Ovi negativni oblici ponašanja su posebno značajni, s obzirom na to da oni ne pogađaju samo žrtvu, već ima uticaj i na druge korisnike društvene mreže, što je nekad i cilj nasilnika. Prijetnje su svakako najučestaliji i najkonretniji oblik nasilja u virtuelnom okruženju, on se realizuje od strane nasilnika prema žrtvi, ali tako da sama prijetnja bude vidljiva i cijeloj društvenoj mreži. Česte su i prijetnje u međusobnoj komunikaciji. Fizičkim obračunima, vandalizmu i destruktivnosti često prethodi formiranje grupe na društvenoj mreži u kojim se adolescenti internauti dogovoraju oko realizacije agresivnog čina prema pojedincu, grupi ili imovini.

1. EKSTERNALIZIRANI PROBLEMI KOD ADOLESCENATA

Posljednjih decenija agresivno i delinkventno ponašanje je u konstantnom porastu. Takvi negativni obrasci ponašanja od strane adolescenata podrazumijevaju stalni rad javnih i društvenih institucija, koji u BiH ne mogu adekvatno da odgovore zbog povećanog obima socijalno neprihvatljivih ponašanja, a s druge strane, malog broja edukovanih i obrazovanih zaposlenika u ovom polju rada.

Agresivnost kao ponašanje predstavlja širok pojam u kojem je veliki broj autora našao svoje uporište za istraživački rad. S tim u vezi je i veliki broj određenja agresivnosti. Agresivnost je ponašanje u čijoj je pozadina namjera da se drugoj osobi nanese šteta ili uništi neki objekt (Bartol, 1995). Ovakva definicija ima niz implikacija (Moeller, 2001): agresivno ponašanje uvijek ima namjeru da nanese štetu, ukoliko se to desi nemamjerno to se ne može nazvati agresivnim ponašanjem (upravo ovo otežava situaciju u zakonodovstvu kada se radi o prijetnjama i ostalim oblicima negativnih oblika ponašanja na društvenim mrežama, odnosno u tome kako dokazati nečiju namjeru); druga implikacija se odnosi na to da agresivnost podrazumijeva ne samo fizičko oštećenje, nego i duševno (agresivnim ponašanjem se smatra i kada neki adolescent pričajuci ružne stvari želi da nanese bol drugom, što je izuzetno često na virtuelnim mrežama); i treća implikacija je da agresivno ponašanje može biti usmjereno ne samo na ljude, nego i na životinje i objekte.

Agresivno ponašanje adolescenata se može sagledati iz više uglova, ali se što se tiče psihološkog ugla gledanja statističkim pristupom iz opisa problematičnih oblika ponašanja djece i mladih izvedeni su dva široko shvaćena sindroma ponašanja: eksternalizirajući i internalizirajući sindromi (Achenbach, 1993). Dok internalizirajući sindrom predstavlja pretjerano kontrolisane oblike ponašanja, eksternalizirajući sindrom se odnosi na hiperaktivne, delinkventne i agresivne oblike ponašanja. Eksternalizirani problemi uključuju sljedeće oblike ponašanja: agresivno ponašanje (tjelesne obračune, destruktivnost, neposluh, prkosno ponašanje, prijetnje drugima i ometanje nastave u školi) i delinkventno ponašanje (bježanje od kuće, podmetanje požara, krađe, izostajanje s nastave, zloupotrebu alkohola i droga, te vandalizam) (Esseu i Conradt, 2006).

Najčešći oblik eksternaliziranih problema u virtuelnom okruženju su prijetnje, ali ne treba isključiti i ostale oblike koji su indirektno povezani sa dimenzijama virtuelnog svijeta. S obzirom da adolescenti veliku važnost daju društvenim mrežama, i da na osnovu aktivnosti unutar virtelnog okruženja grade i stvaraju svoj identitet, ne bi se trebalo zanemariti važnost društvenih mreža u ranom prepoznavanju razvoja agresivnog ponašanja. Putem virtuelne komunikacije adolescenti dogovaraju fizičke obračune, destruktivne radnje, djele informacije o dostupnosti droga, pripremaju vandalske činove. Virtuelno okruženje problematičnim adolescentima nudi širok dijapazon mogućnosti da ispolje sve frustracije, kao i da saznaju i pokažu sve što u realnom okruženju ne bi mogli, uslijed neadekvatne socijalizacije, straha, tjeskobe i drugih socijalno-psiholoških faktora. Kao prikriveni internauti se često sukobljavaju sa drugima putem prijetnji, zlostavljanja, ponižavanja, ometanja, uhođenja i ostalim oblicima agresivnog ponašanja.

Adolescenti 21. vijeka imaju potrebu da djele svoju intimu sa ostatkom svijeta upravo putem društvenih mreža, te nerijetko nekom agresivnom ili delinkventnom obliku ponašanja prethodi objavljen sadržaj od strane adolescenata na društvenoj mreži. Stoga su virtualne mreže o svijetu dobar prediktor za eksternalizirane problem, ali i značajan faktor kada je riječ o prepoznavanju i sprečavanju adolescenta u njegovim namjerama.

Agresivnost se može podjeliti na više tipova i podtipova, kada je riječ o njegovom pojavljivanju u virtualnom svijetu. Postoje otvoreni oblici agresije, kada djeca otvorenog asocijalnog ponašanja reaguju na neku situaciju razdražljivije, osjetljivije i burnije, u odnosu na djecu prikrivene agresivnosti. U ovom slučaju misle se na pretnje, omalovažavanja, ponižavanja vršnjaka putem virtualne komunikacije koja se često odvija vrlo transparentno i jasno, putem njihovih istinskih profila na društvenim mrežama, ili kroz formiranje društvenih grupa u kojim se negativno percipiraju vršnjaci. Adolescenti otvorenog asocijalnog ponašanja druge adolescente pozivaju na linč i direktni sukob sa pojedincima, koje su označili kao metu svog "asocijalnog poduhvata". Neki adolescenti se u virtualnoj stvarnosti odlučuju za prikrivene oblike agresivnosti, odnosno nastoje da putem lažnih profila ili lažnog predstavljanja nanesu štetu svojim vršnjacima.

Eksternalizirane probleme adolescenata u virtuelnom svijetu možemo sagledati i kroz prizmu reaktivne i proaktivne agresivnosti. Reaktivna agresivnost je agresivno djelo koja predstavlja reakciju na neki događaj ili osobu. S obzirom da je zasnovano na percepciji adolescenta često bude praćeno subjektivnošću i pretjeranim agresivnim reakcijama. Vanjski podražaj izaziva veliku količinu bijesa, koji se udružuje s impulsivnošću, slabom sposobnošću usmjeravanja ponašanja, slabo razvijenim sposobnostima savladavanja i neprimjerenom obradom socijalnih informacija. Zbog neprimjerene obrade socijalnih informacija vjerovatno je da osoba o kojoj se radi očekuje negativan ishod, pokazuje fiziološku uzbudjenost i reaguje agresivno (Conradt i Essau, 2006). Virtuelno okruženje, prvenstveno zbog anonimnosti s jedne strane, a s druge strane zbog mogućnosti uticaja na druge korisnike unutar mreža, omogućava adolescentima da na lak i brz način eksternaliziju svoj nakupljene frustracije u vezi sa nekim događajem ili osobom. Adolescenti koriste društvene mreže kao sredstvo osvete. Reaktivni agresivni adolescenti često budu percipirani kao osobe koje i same zavređuju nasilje (Crick i Dodge, 1996). U odnosu na proaktivno agresivne adolescente, koje odlikuje samopouzdanje i miran stav, reaktivni su dosta opasniji kada je riječ o njihovom djelovanju i aktivnostima u virtuelnom svijetu. Reaktivno agresivni adolescent nisu omiljeni među vršnjacima u realnom okruženju. Obično su to adolescenti koji su bili izloženi fizičkom zlostavljanju, socijalnim problemima i koji dolaze iz nestabilnih porodica i kao piuni takvog realnog okruženja imaju potrebu da u virtualnom okruženju stvore identitet i formiraju sliku "snage, moći i dominacije". Sve u okviru društvenih mreža shvataju isuviše lično i važno, na njih iznose svoja lična uvjerenja (često i vrlo pogrešna), stvaraju lažnu sliku kako bi se uklopili među svijet svojih vršnjaka. S tim u vezi je i sljedeći oblik agresivnosti, a to je relacijska agresivnost. Relacijska agresivnost je ponašanje koje šteti drugima zbog uništavanja veza, prijateljstava, pripadnosti skupini ili osjećaja prihvaćenosti, ili se takvim uništenjem prijeti (Crick, 1996). Relacijski agresivni adolescent se u odnosima s vršnjacima osjećaju nesrećnima i očajnim, usamljenim neprihvaćenim, i upravo ih to navodi da se osvete vršnjacima korištenjem oblika relacijske agresivnosti. Oni se osjećaju bolje nakon što uzrokuju isključivanje drugih vršnjaka iz grupe (Crick i Grotjeter, 1995, prema Conradt i Essau, 2006). Relacijska agresivnost, odnosno narušavanje prijateljskih odnosa u virtualnom i stvarnom okruženju je više vezan za djevojke, jer djevojke prijateljske odnose više vrednuju u odnosu na mladiće. Na društvenim mrežama adolescenti ostavljaju podatke o svojim prijateljima, važnim i značajnim osobama u svom životu, a upravo to mogućava drugima da koristeći oblike ove agresivnosti naškode osobi. I ako se uvijek apeluje da društvene mreže, odnosno profili ne treba da sadrže lične i intimne podatke ili slike zbog mogućih zlopotpotreba, adolescenti se nerijetko oglušavaju na sva upozorenja.

Imajući u vidu prethodno navedeno, možemo navesti sljedeće modalitete ispoljavanja sindroma eksternaliziranih problema na društvenim mrežama:

- Krađa profila;
- Ucenjivanje i iznuđivanje; seksting
- Vršnjačko nasilje i drugi oblici elektronskog nasilja ili korištenjem mogućnosti društvenih mreža;
- Narušavanje privatnosti;
- Narušavanje javnog reda i mira;
- Širenje zabranjenog sadržaja i propagiranje zabranjenih ideja;
- Govor mržnje.

Krađa profila je jedan oblik krađe (kompromitacije profila) identiteta. Svako nedozvoljeno posjedovanja autentifikacionih i identifikacionih podataka tuđeg profila, bez obzira na realizovanu nedozvoljenu aktivnost, smatra se kompromitacijom profila, a samim tim i kompromitacijom identiteta vlasnika tog profila na društvenim mrežama (Miladinović, 2013). Pošto smo već ustanovili da adolescenti na profilu ostavljaju mnoštvo ličnih informacija, koje se vežu za identitet njegovih prijatelja, njegovu komunikaciju s prijateljima, pridruženosti i posjećenost određenim grupama i stranicama, krađa profila predstavlja najdrastičniji oblik narušavanja tuđe privatnosti, i kao takav može ozbiljno narušiti duševno zdravlje žrtve, što je i implikacija agresivnog ponašanja po nekim autorima. Kompromitacijom profila, odnosno korištenjem istog u tuđe ime, može trajno narušiti odnose sa drugim korisnicima, u ovom slučaju prijatelja te osobe. Ovakav vid agresivnog ponašanja možemo podvesti pod relacijsku agresivnost, jer to je i obično cilj adolescenta kada izvrši ovaj prestup u virtuelnom okruženju. Cilj se zasniva na zlonamjernoj aktivnosti u svrhu povređivanja druge osobe. U vezi sa ovim oblikom agresivnog ponašanja je i ucenjivanje i iznuđivanje. Adolescenti znaju važnost virtuelnog svijeta za svoju populaciju, s jedne strane, a s druge strane znaju koristiti sve pogodnosti i mogućnosti interneta. Važnost stvaranja i formiranja slike o sebi, odnosno ugleda u virtuelnom okruženju je velikom broju adolescenata primarno, pa stoga ucenjivači smatraju da će objavljanjem kompromitujućeg sadržaja, koji su dobili ili putem komunikacije na internetu, ili sa samih profila osoba, uspjeti u svojoj namjeri. Ovakav vid ponašanja je oblik instrumentalne agresivnosti, čak i proaktivne, gdje ucenjivači vođeni krajnjim ciljem se ponašaju beskrupulozno, a žrtve, najčešće mlađi adolescenti, pristaju na uslove učjene, jer im je u tom periodu jako važna percepcija drugih o njima.

Društvene mreže su prvi izbor adolescentima kada je u pitanju vršnjačko nasilje i to iz više razloga. Prvi razlog je da društvene mreže omogućavaju anonimnost korisnika, dok sama žrtva nasilja ne može da pobjegne i da se zaštići. Druga bitna stavka je masovnost. U želji da nanese duševnu bol nasilniku je važno da to vidi što više ljudi. To se uglavnom odnosi na postavljanje uvredljivih, ponižavajućih, negativnih implikacija vezanih za tu osobu, bilo da se radi o tekstu, slici ili video materijalu. Lažno preslatvaljanje je takođe oblik vršnjačkog nasilja, koji se načešće kreiraju na ime žrtve, te se na navedenom profilu objavljuju razni za žrtvu kompromitirajući sadržaji, te se zatim učine dostupnim za sve druge internaute.

Poseban oblik vršnjačkog nasilja na društvenim mrežama je postavljanje seksualno inkriminišućih i ponižavajućih fotografija, video snimaka ili drugog sadražaja na profilu. U vezi sa navedenim je i tzv. online seksualno napastovanje, koje se sastoji u konstatnom i kontinuiranom slanju poruka, fotografija i snimaka, te postavljanju komentara i sličnih aktivnosti koje imaju određenu seksualnu pozadinu ili kontekst (Miladinović, 2013).

Virtuelno okruženje, odnosno društvene mreže, su zbog svoje masovnosti vrlo popularne kada se radi o formiranju hejt grupe. Hejt grupe propagiraju mržnju, netrpeljivost ili neku drugu vrstu negativne emocije prema određenoj osobi iz vršnjačke skupine. Činjenica da su članovi te grupe osobe iz neposredne okoline, čine žrtvu još više ugroženom, te ona najčešće izbjegava školu, internet i povlači se u sebe. Pokazalo se da su ovom obliku vršnjačkog nasilja više sklone djevojčice, kao i korisnici koji imaju manje od 13 godina. Formiranje hejt grupe je u poveznici sa govorom mržnje, samo što je u ovom slučaju „žrtva“ višebrojna. Najčešće se odnose na vjerski, nacionalni ili seksualni identitet pojedinaca, koji su svojim izborom privukli pažnju problematičnim adolescentima.

Eksternalizirani problemi u virtuelnom okruženju su izuzetno opasni, jer za razliku od realnog okruženja sadrže sljedeće odrednice:

- Agresivni adolescenti koriste pogodnosti korištenja društvenih mreža jer znaju da za razliku od realnog okruženja, virtuelni svijet nudi zaštitu putem anonimnosti, a s druge strane, relevantne institucije, pa i zakonodavstvo nije pronašlo adekvatan odgovor na sve veći broj socijalno neprihvatljivih oblika ponašanja na internetu;
- Agresivni adolescenti biraju društvene mreže kao sredstvo nanošenja bola drugoj osobi zbog masovnosti korištenja društvenih mreža, i što obično sama žrtva i posmatrači agresivnog čina pripadaju istoj vršnjačkoj skupini;
- Za razliku od realnog okruženja gdje se agresivni akt može zaustaviti, sadržaj koji aludira na vršnjačko nasilje nikad ne prestaje, čak se kompromitirajući sadržaj jako brzo širi na internetu i često žrtva osjeća posljedice jako dugo i nakon samog napada. Najčešće i sama žrtva odgovara na isti način nasilniku, te se se krug vršnjačkog nasilja samo i dalje širi.

Povezanost realnog i virtuelnog okruženja i eksternaliziranih problema adolescenata je najviše očita kada se radi o narušavanju javnog reda i mira kroz sljedeće tri situacije: zakazivanje tuča između maloljetnika, kroz podstrekavanje nasilja na sportskim priredbama i kroz demonstracije inicirane ili posredovane putem društvenih mreža (Miladinović, 2013). Zakazivanje tuča putem društvenih mreža je česta pojava, koja u nekim slučajevima završava s teškim tjelesnim ozljedama. Prate je formiranje hejt grupa koji svojim sadržajima vređaju drugu skupinu maloljetnika, koja odgovara na njihove prozivke i samim tim učestvuje u organizovanju masovne tuče. Po ovom principu se dogovaraju tuče nakon utakmica i pripremaju adolescenti za nerede na sportskim priredbama.

2. ETIOLOGIJA NASILJA NA INTERNETU

U posljednjih pedeset godina razvijen je velik broj teorijskih koncepata diskursa koji su pokušali da sagledaju i objasne porast agresivnih oblika ponašanja među adolescentima. Uzroke sve učestalijih primjera eksternaliziranih problema možemo tražiti u širem spektru koji podrazumijeva niz endogenih i egzogenih faktora, koji najčešće djeluju udruženo, pa će samim tim najbolji odgovor na pitanje etiologije virtelnog nasilja dati integrativne teorije, odnosno modeli, koje će se u sebi da sadrže elemente kognitivnih teorija, teorija socijalnog učenja i socijalne povezanosti, te teorije koje naglašavaju intrapersonalne karakteristike. Faktori rizici koji podstiču, razvijaju ili dovode direktno do eksternaliziranih problema se obično nalaze u sljedećim skupinama: porodično okruženje (interakcija roditelj-dijete), pripadnost skupinama vršnjaka sa odstupajućim ponašanjem, masovni mediji, personalne karakteristike, kao i kulturni milje kojem pripada adolescent. U psihološke osobine koje imaju centralnu ulogu, odnosno koje favorizuju ulazak osobe u svijet socijalne patologije, prema nekim autorima, spadaju motivacija, emocionalna labilnost, agresivnost i intelektualne sposobnosti (Milosavljević, 2004). Među konstrukte koji najviše doprinose razvoju eksternaliziranih problema se ubrajaju osobine ličnosti, a naročito dimenzija emotivne stabilnosti, odnosno nestabilnosti (Heldić-Smailagić, 2012).

Dva su široka modela opisala sljed i razvoj agresivnih oblika ponašanja. Prvi je Patersonov model koji je označen kao razvojni, jer u sebi sadrži opisana sva zbivanja koja po ovom autoru vode antisocijalnim sklonostima. Ključna je pretpostavka da se temelji budućeg ponašanja stvaraju kod kuće, te da su čanovi porodice jako važni u stvaranju budućeg antisocijalnog ponašanja. Slabe porodične vještine roditelja i stresne okolnosti u porodici vode ka stvaranju antisocijalnog i neprilagodenog djeteta s niskim samopoštovanjem (koje će pokušavati izgraditi u virtuelnom svijetu). U školskoj dobi takvo dijete će biti odbačeno od strane vršnjaka i roditelja, te će uslijed toga imati loš akademski uspjeh i nizak nivo motiva za postignućem. U trećoj fazi će se pridružiti nekoj devijantnoj grupi i krenuće naginjati delinkventom ponašanju, u koje se ubrajaju i socijalno neprihvatljiva ponašanja u virtuelnom okruženju.

Drugi model je model višestrukih rizičnih i zaštitnih faktora, koji je dao Carr (1999), kada je objašnjavao ponašajne probleme. Svi faktori se djeli na predisponirajuće, precipitirajuće i održavajuće faktore, koji se nadalje djeli na lične i okolinske faktore. Predisponirajući faktori uključuju faktore koji stvaraju psihološku ranjivost za razvoj agresivnog ponašanja, a to su u ovom slučaju niska inteligencija, težak temperament, eksternalni lokus kontrole, rani oblici agresivnog ponašanja, nedostatak discipline od strane

roditelja, slaba rana intelektualna stimulacija, lose socijalne vještine roditelja i razna druga traumatska iskustva za dijete.

Ono što predstavlja "okidač" za eksternalizirane probleme kod adolescenata, odnosno precipitirajući faktori za ponašajne problem predstavljaju sljedeći faktori: stresne situacije, uključivanje u devijantne grupe, zlostavljanje od strane vršnjaka ili drugih, razvod roditelja, gubitak prijateljskih veza i nezainteresovanost roditelja. U održavajuće faktore eksternaliziranih problema Carr ubraja: slabe socijalne vještine, nedostatak adekvatnog modela za stvaranje veza, nezreli mehanizmi odbrane, disfunkcionalne strategije u rješavanju problema, slaba samoefikasnost, dezorganizovana porodica, eksternalni lokus kontrole kod roditelja, loša komunikacija s roditeljima, negativan atribucijski stil, nedosljedna disciplina roditelja i nadzor i drugo.

U lične zaštitne faktore Carr je svrstao: dobro zdravlje, visoka inteligencija, lak temperament, samopouzdanje, internalni lokus kontrole, visoka samoefikasnost, optimistični atribucijski stil, zdravi mehanizmi odbrane i funkcionalne strategije za rješavanje problema. U okolinske zaštitne faktore je svrstao zdrave porodične odnose, povezanost roditelja s djetetom, kvalitetnu kominaciju s roditeljima, visok stepen samopoštovanja i efikasnosti kod oba roditelja, njihov optimistični atribucioni stil i internalni lokus kontrole.

Što se tiče prevencije većina autora su saglasni da u ovaj problem treba uključiti i porodicu i školske institucije. Nastavnici i roditelji bi po ovakvom uglu gledanja trebali da nekoliko sati sedmično provedu s učenicima, odnosno djecom, razvijajući njihove kognitivne sposobnosti, odnosno da ih nauče kako da kontrolišu i iskazuju svoje emocije, te kako da uspješno rješe probleme u vezi sa svojim identitetom (Daniel J. Flannery i saradnici, prema Gullota i Adams, 2005). Sa ovakvim programima bi trebalo krenuti što ranije i na taj način bi se prevazišle sve moguće razvojne poteškoće adolescenije.

ZAKLJUČAK

Zbog osjetljivosti razvojnog perioda u kojem se nalaze adolescent, virtuelno okruženje, a naročito društvene mreže su mjesto na kojima oni provode mnogo slobodnog vremena komunicirajući s vršnjacima, gradeći veze i odnose, kao i formirajući sliku o sebi i položaj "u svijetu vršnjaka". Društvene mreže i internet omogućavaju dosta pogodnosti s jedne strane, ali s druge strane nose sa sobom izvjesne opasnosti i probleme. Ti problemi se mogu sagledati kroz prizmu eksternaliziranih problema kod adolescenata, odnosno pojavu agresivnog i delinkventnog ponašanja na društvenoj mreži, ili u poveznici sa agresivnim ponašanjem u stvarnoj dimenziji. Na društvenim mrežama se najčešće pojavljuju sljedeći oblici negativnog ponašanja: krađa profila; ucjenjivanje i iznuđivanje; seksting; vršnjačko nasilje i drugi oblici elektronskog nasilja ili korištenjem mogućnosti društvenih mreža; narušavanje privatnosti; narušavanje javnog reda i mira; širenje zabranjenog sadržaja i propagiranje zabranjenih ideja i govor mržnje. Kada je riječ o agresivnom ponašanju, a naročito vršnjačkom nasilju, govorimo o multidimenzionalnom etiološkom pristupu. Od integrativnih modela koje najviše doprinose sagledavanju ovog problema potrebno je istaći Patersonov razvojni model i Carrov model višestrukih rizičnih i zaštitnih faktora.

LITERATURA

- [1] Achenbach, T.M. (1991): Manual for the Youth Self-Report and 1991 profile. Burlington: University of Vermont Department of Psychiatry.
- [2] Achenbach, T.M. (1993): Taxonomy and comorbidity of conduct problems: Evidence from empirically based approaches. Development and Psychopathology, 5, 51-61
- [3] Carr, A. (1999): Child and Adolescent Clinical Psychology, a Contextual Approach. London and New York: Taylor and Francis Group, Routledge
- [4] Crick, N.R. (1996): the role of relational aggression, overt aggression, and prosocial behavior in the prediction of children's future social adjustment. Child development, 67, 1003-1104
- [5] Bartol, C.R. (1995): Criminal behavior: A psychosocial approach. Englewood Cliffs, NJ: Prentice Hall
- [6] Essau, C.A., Conradt, J. (2006): Agresivnost u djece i mladeži. Jastrebarsko: Naklada Slap
- [7] Gullota, T.P., Adams, G.R. (2005): Handbook of adolescent behavioral problems: evidence-based approaches to prevention and treatment. NJ: the Child and Family Agency of Southeastern Connecticut
- [8] Helić-Smailagić, E. (2012): Eksternalizirani problemi kod adolescenata. Banjaluka: Minsitastvo nauke i prosvjete.

- [9] Miladinović, A. (2013): Fejsbuk i kriminalitet. Banjaluka: Internacionalna asocijacija kriminalista
- [10] Milosavljević, B. (2004): Socijalna patologija. Banjaluka: Filozofski fakultet Banjaluka
- [11] Moeller, T.G. (2001): Youth aggression and violence. Hillsdale, NJ: Lawrence Erlbaum Associates.
- [12] Wenar, C. (2003): Razvojna psihopatologija i psihijatrija. Jastrebarsko: Naklada Slap

KAKO SE ZAŠTITI OD ZLONAMJERNOG SOFTWAREA I NARUŠAVANJA SIGURNOSTI KORISNIČKIH PODATAKA

Jasmin Kahriman

Buroj International Group, Sarajevo, Bosna i Hercegovina, jasmin.kahriman@outlook.com

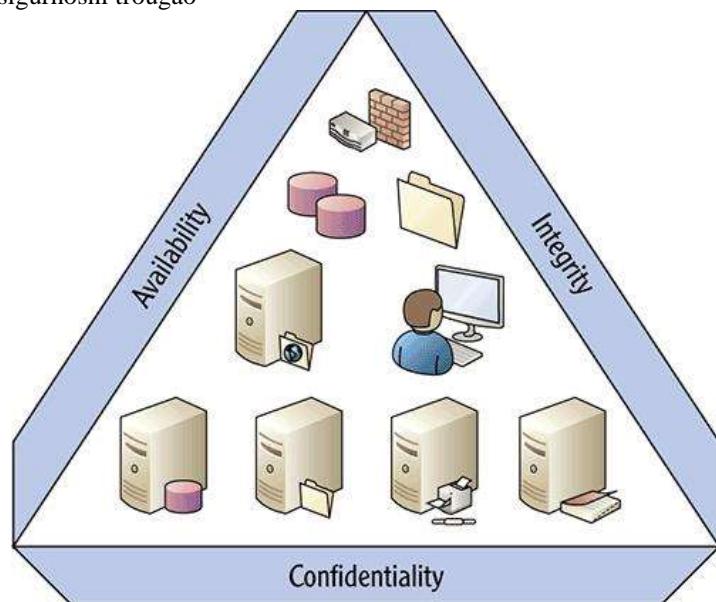
Apstrakt: Jedan od glavnih zadataka krajnjih korisnika i poslovnih lica je implementacija sigurnosnih mehanizama zaštite korisničkih podataka, čime se smanjuje rizik napada i zloupotrebe podataka i informacija od strane zlonamjenih osoba. Povjerljivost, integritet i dostupnost podataka su glavne tačke, zadaci na koje se IT stručnjaci trebaju fokusirati kako bi imali zdravo radno okruženje, koje prije svega uključuje zdrav informacioni sistem. Postoje razni preduslovi koje je potrebno ispuniti kako bi se smanjio rizik napada, a neki od njih su: up-to-date operativni sistemi, edukacija zaposlenika, jake i sigurne korisničke šifre, antivirusna rješenja i pametne računarske mreže, sa mehanizmima detaljne kontrole mrežnog saobraćaja.

Ključne riječi: sigurnost, antivirusi, edukacija, hakerski napad, zaštita

1. CIA/AIC TRIANGLE (SIGURNOSNI TROUGAO)

Jedan od osnovnih problema sa kojim se korisnici na Internetu susreću je narušavanje CIA/AIC sigurnosti. Ne, ne radi se o Centralnoj obavještajoj agenciji (Central Intelligence Agency), nego o sigurnosnom trouglu koji uključuje tri sigurnosna principa, koja je potrebno očuvati, C - confidentiality (povjerljivost), I - integrity (integritet) i A - availability (dostupnost). Povjerljivost podataka podrazumijeva da samo autorizovani korisnici mogu pristupiti podacima, a način kako povećati povjerljivost podataka je implementacijom multifactor autentifikacije i enkripcije podataka. S druge strane, integritet podataka podrazumijeva da samo autorizovani korisnici mogu manipulisati podacima (vršiti izmjene nad njima), a način na koji se može sačuvati integritet podataka je definisanje dozvola nad podacima (permissions) i provjera podataka koristeći HASH algoritmom. Podaci trebaju biti dostupni kada god korisnici imaju potrebu da ima pristupe, dostupnost podataka se povećava redovnim održavanjem informacionih sistema, koji uključuju hardware, operativne sisteme i software.

Slika 1. CIA/AIC sigurnosni trougao



Izvor: www.safaribooksonline.com

2. KAKO ZAŠTITI PODATKE

Jedan od najvećih problema sa kojim se korisnici susreću je zlonamjerni software, a kao posljedica toga i zloupotrebjeni korisnički računi (Facebook, Twitter, E-mail i sl.), te ukradeni podaci. Posljedica navedenog problema leži u (ne)znaju krajnjih korisnika. Ukoliko se korisnici pridržavaju osnovnih propisa, smanjiti će rizik napada, krađe podataka i ličnih autentifikacijskih i autorizacijskih informacija.

Postoji nekoliko mehanizama čijom implemtacijom se postiže veća sigurnost, o kojima će biti više informacija u narednim podpoglavlјima.

2.1 Up-to date operativni sistem

Jedno od osnovih pravila je koristiti novije operativne sisteme, koji pružaju bolju sigurnost, veću produktivnost i na kraju novo korisničko iskustvo. Navikavanje na novi dizajn, ne treba da bude prepreka, nego korak naprijed. Ipak je mnogo važnije imati sigurnije nego "ljepše" korisničko iskustvo, tkz. user experience, koji je individualna stvar. Svaki Windows proizvod ima životni ciklus. Svaki životni ciklus počinje kada se proizvod objavi i završava se kada se podrška za njega ukine. Poznavanje ključnih datuma u ovom životnom ciklusu pomaže da krajnji korisnici ili IT stručnjaci donesu kvalifikovane odluke o tome kada izvršiti nadogradnju ili napravite druge promjene na softveru. Iz upotrebe isključiti korištenje Windows XP (istekla podrška) i Windows VISTA (nestabilan) osim ako je neophodan za poslovne potrebe. Više informacija o životnom ciklusu pronaći na linku: <http://windows.microsoft.com/sr-latn-rs/windows/lifecycle>.

Tabela 1: Životni ciklus klijentskih operativnih sistema

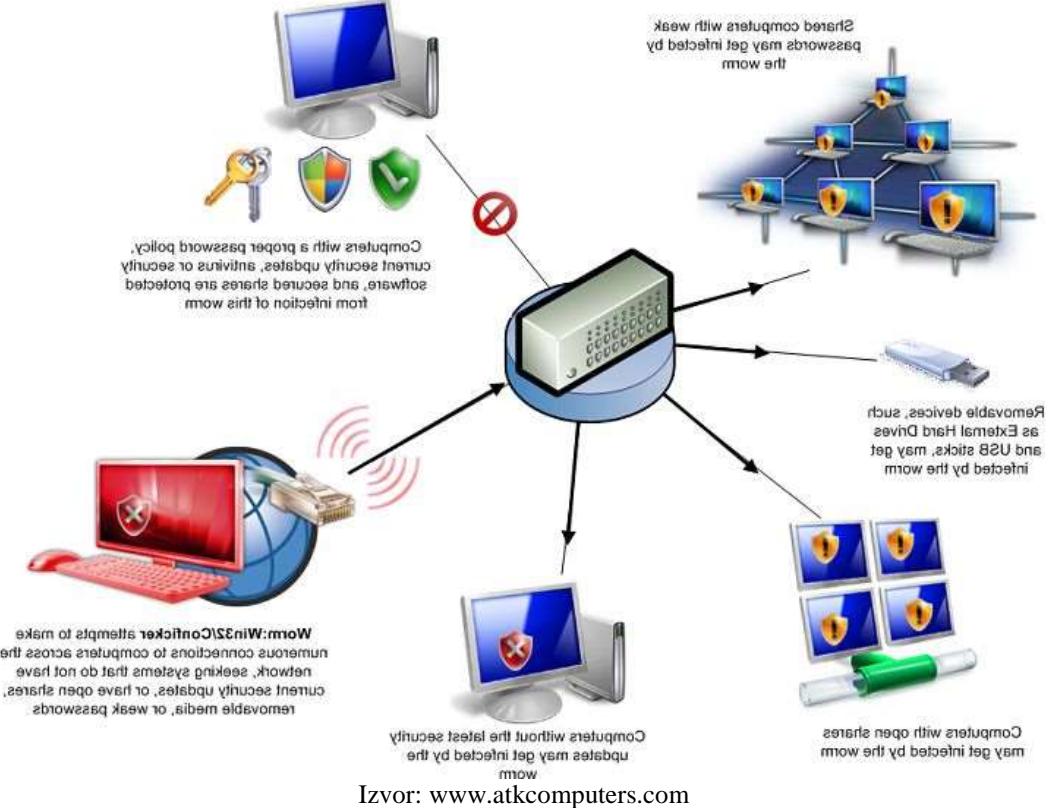
Klijentski operativni sistemi	Najnovija ispravka ili servisni paket	Kraj glavne podrške	Kraj proširene podrške
Windows XP	Servisni paket 3	14.04.2009.	08.04.2014.
Windows VISTA	Servisni paket 2	10.04.2012.	11.04.2017.
Windows 7*	Servisni paket 1	13.01.2015.	14.01.2020
Windows 8	Windows 8.1	09.01.2018.	10.01.2023.
Windows 10	Nedostupno	13.10.2020	14.10. 2025.

Tabela 2: Povlačenje iz prodaje

Klijentski operativni sistemi i ispravke	Datum opšte dosutnosti	Povlačenje software is maloprodaje	Povlačenje računara sa unaprijed instaliranim operativnim sistemom Windows iz prodaje
Windows XP	31.12.2001.	30.06.2008.	22.10.2010.
Windows VISTA	30.01.2007.	22.10.2010.	22.10.2011.
Windows 7 Home Basic, Home Premium, Ultimate	22.10.2009.	31.10.2013.	31.10.2014.
Windows 7 Professional	22.10.2009.	31.10.2013.	31.10.2016.
Windows 8	26.10.2012.	31.10.2014.	30.06.2016.
Windows 8.1	18.10.2013.	01.09.2015.	31.10.2016.
Windows 10	29.07.2015.	Nedostupno	Nedostupno

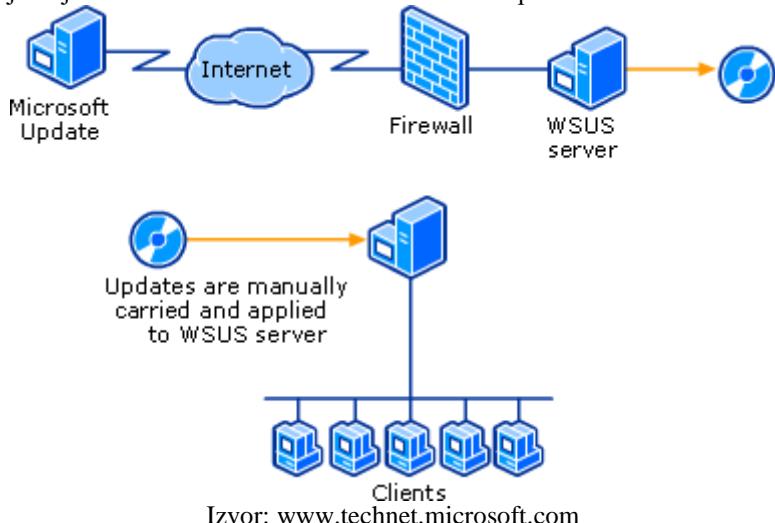
Mnogi korisnici izbjegavaju korištenje Windows update, što predstavlja veliki nedostatak. 2010. godine zabilježen je slučaj u jednoj od državnih institucija, gdje je kompletna služba (20 PCs), bila zaražena crvom "Conficker", koji se uspješno izvršavao na operativnim sistemima koji nisu imali sigurnosnu zakrpnu. Crv je zaguošio mrežu, usporio računare i onemogućio rad službe sa strankama. Uklanjanje zlonamjernog crva sa računara bio je kompleksan posao, koji je trajao više od dva dana. Jedna od njegovih osobina je multipliciranje na sve računare koji su na mreži, što je zahtjevalo isključenje svih računara sa mreže, pojedinačno skeniranje sa više antivirusnih alata, instalacija update koji su bili neophodni za onemogućavanje ponovnog vraćanja Conficker crva, te u dosta slučajeva preinstalacija operativnog sistema, koji se oštetoio uslijed uklanjanja Conficker.

Slika 2. Conficker - crv koji se širi mrežom



U mnogo slučajeva update mogu da prouzrokuju probleme, te onesposobe određene funkcionalnosti operativnog sistema i aplikacija. Neki od problema sa kojima se korisnici susreću uslijed instalacije neadekvatnog update je prestanak rada hardware (mrežna ili audio kartica, prestanak rada miša i sl.), prestanak rada Outlooka, koja uključuje nemogućnost slanja ili primanja elektronske pošte i sl. Preporuka je aktivirati "System Restore", kako bi se kreirali Checkpoints prije i nakon svakog update. Ukoliko se desi da update nije kompatibilan sa trenutnom konfiguracijom, potrebno je ili uraditi System Restore ili ukloniti update. U poslovnim okruženjima implementirati WSUS (Windows Server Update Services).

Slika 3. WSUS rješenje za automatizovanu kontrolu Microsoft update



2.2 Edukacija krajnjih korisnika

Najranjivija sigurnosna tačka su ljudi. Social Engineering je hakerska metoda, na osnovu koje hakeri grade povjerenje prema žrtvi, te isto povjerenje prekrše zbog lične koristi i štete korisnika. Zamislite da konkurentna kompanija želi doći do informacijama o novim projektima, podacima ili izvornom kodu. To

je sve moguće, ukoliko se izgradi povjerenje između dvije osobe, tu se rodi ljubav, i podaci lagano procure, bez osjećaja da je žrtva učinila grešku. Upravo na tome je baziran Social Engineering.

Slika 3. Social engineering tehnike obmanjivanja



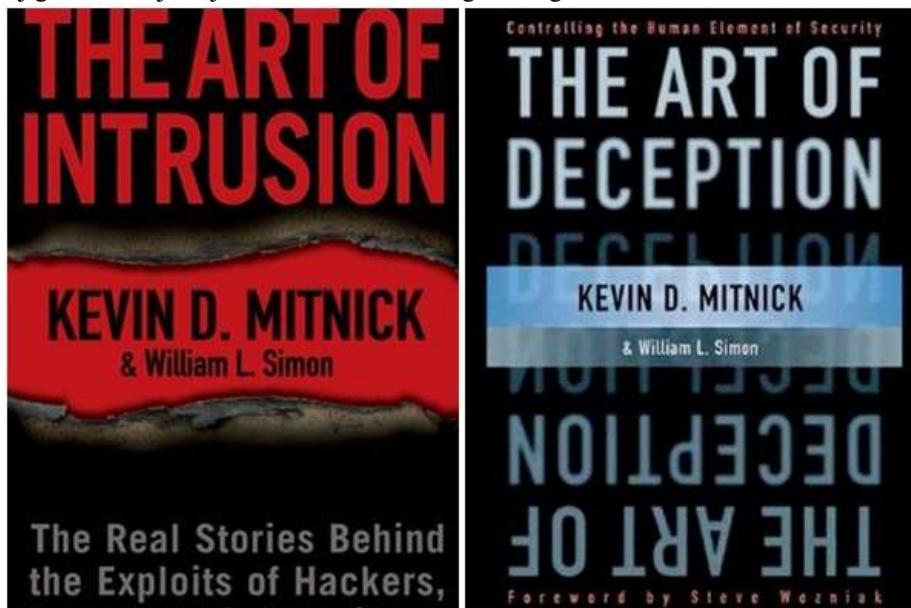
Izvor: www.securitylab.ru

Potrebno je kreirati poslovnu etiku, klasifikaciju informacija i podataka i normi po kojima se zaposlenici trebaju ponašati. Poslovne informacije trebaju ostati u kompaniji, a ne izvan nje. Potrebno je educirati korisnike o Social Engineeringu, sigurnom surfanju (phishing), zlonamjernom software i naučiti ih da primjete problem, prije nego bude kasno. Edukaciju trebaju voditi IT stručnjaci koji posjeduju znanje o pomenutoj oblasti.

Na tržištu Bosne i Hercegovine dostupne su dvije knjige koje se mogu iskoristiti u cilju povećanja znanja iz oblasti social engineering:

- "The art of deception", Kevin Mitnick & William Simon, 2002. godina
- "The Art of Intrusion", Kevin Mitnick, 2005. godina

Slika 4. Knjige o obmanjivanju metodom „Social Engineering“



Izvor: www.wired.com

Ukoliko se Social Engineering metoda napada ukombinuje sa Phishing napadom, povećava se mogućnost krađe podataka. Poznavanje osnovnih informacija o oba napada, krajnji korisnici smanjuju mogućnost da budu potencijalne žrtve. Phishing je metoda napada gdje hakeri lažiraju informacije na web stranicama i predstavljaju ih drugačijim potencijalnoj žrtvi. Haker klonira određene web stranice (društive mreže, prijava na banku ili treće sajtove), te istu web stranicu preusmjeri na računar žrtve. Žrtva pokuša da se prijavi na Facebook sa validnim, autentifikacijskim i autorizacijskim informacijama. Ukoliko je žrtva bila prijavljena na web sajt, nakon ponovnog upisivanja u lažni web sajt, biti će redirektana na pravu stranicu Facebook, i neće primjetiti nikakve promjene. Ukoliko žrtva nije bila prijavljena na web sajt, dobiti će

grešku, da pokuša kasnije. S druge strane, haker je dobio validne informacije i pristupio korisničkim računima žrtve. Krajnji korisnici moraju biti oprezni kakvim web sajтовимa pristupaju, malo više pažnje i rizik napada je smanjen.

Slika 5. Phishing napad



Izvor: www.thegreenlanterns.wordpress.com

2.3 Korisničke šifre

Dvije kardinalne sigurnosne greške su korištenje slabih šifri i korištenje istih šifri na više korisničkih računa. Unutar kompanije je potrebno kreirati sigurnosnu polisu koja uključuje definisanje korisničkih šifri na minimalno 8 karaktera, uključujući velika i mala slova, brojeve i interpukcijske znakove. Jedno od pravila koje se može primjeniti je mjenjanje šifri nakon 90 dana, korištenja, sa polisom da korisnici ne mogu koristiti ranije korištene šifre. Nikada ne koristiti istu šifru na više korisničkih računa. Ukoliko zlonamjerna osoba zloupotrijebi jedan korisnički račun, velika mogućnost je da će istu šifru probati i na drugim računima, prije nego što krajnji korisnici primjete. Ukoliko se unutar kompanija nalazi Active Directory infrastruktura, potrebno je kreirati grupne polise za definisanje korisničkih šifri. Nadogradnjom infrastrukture na Windows 10, smanjuje se mogućnost zloupotrebe domenskih korisničkih informacija, obzirom da nova tehnologija, tzv. Credential Guard, čuva domenske kredencijale od napada.

Slika 6. Najgore (najnesigurnije) šifre korištene 2015. godine

WORST PASSWORDS OF 2015		
RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	↑ ↗
4	qwerty	↑ ↗
5	12345	↓ ↘
6	123456789	Unchanged
7	football	↑ ↗
8	1234	↓ ↘
9	1234567	↓ ↗
10	baseball	↓ ↘

Izvor: www.prweb.co

2.4 Antivirusi, spyware, adblock

Postoji razlika između virusa i malware. Virus predstavlja dio koda koji se kopira na računar, izvršava i na kraju uništava naš sistem, aplikacije ili podatke. Malware čine trojanci, spyware, adware, ransomare, worms i virusi. Potrebna je korisnička intervencija da se računar zaradi, tj. korisnik klikne na link ili otvori file unutar kojeg je integriran malware, što rezultuje aktiviranjem zlonamernog software. Sigurnosni eksperti kažu da je nemoguće samo sa jednim antivirusnim rješenjem biti zaštićen i ukloniti zlonamjeri software sa računara. Iz tog razloga je preporuka pored Antivirusa instalirati i Antimalware. Ukoliko se radi o besplatnim antivirusima, preporukuje Avira FreeAntivir ili Avast, a ukoliko korisnici odluče na kupovinu licenciranog antivirusa, nećen pogriješiti sa kupovinom NOD32 (godišnja licenca cca 50.00 KM). Što se tiče malware rješenja, preporuka je instalirati AntiSpyware ili Malwarebytes. Nakon instalacije Antivirus i AntiSpyware, potrebno ih je konfigurisati na High Protection, i kreirati automatizovano skeiranje hard diska po unaprijed definisanom vremenenskog razdoblju. Preporuka je jednom sedmično. Svi virusi su malware, ali malware nisu svi virusi.

Slika 7. Antivirusna rješenja



Izvor: www.racunalo.com

Kako izbjjeći reklame? Po statistici o korištenju brosvera (<http://www.sitepoint.com/>), već duži period, Google Chrome je na prvom mjestu (Decembar 2015, 53.71%). Krjanji korisnici neće pogriješiti ukoliko instaliraju Google Chrome ili Mozilla Firefox. Preporuka je instalirati AdBlock Plus koji će onemogućiti izvršavanje dosadnih reklama i HTTPS Everywhere koji surfanje čini sigurnijim, tj. pokreće web stranice kroz HTTP Secure protokol.

Slika 8. Zaštita od dosadnih reklama



Izvor: socialmouths.com

2.5 Zaštita računarskih mreža

Računarske mreže su složena i kompleksna tema, na koju su napisani tomovi knjiga. Kompletan protok mrežnog saobraćaja se odvija kroz računarsku mrežu, i od velike važnosti je nadgledati i analizirati protok dolaznog i odlaznog saobraćaja. Implementacijom pametne računarske smanjuje se rizik napada, a koja uključuje upravljive switcheve, routere sa ugrađenim sigurnosnim mehanizmima, firewalle koji omogućavaju implementaciju pravila za protok mrežnog saobraćaja, te IDS i IPS sisteme za zaštitu od hakerskih napada. Neadekvatni mrežni uređaji i loša konfiguracija, mogu koštati kompaniju mnogo novca, i mnogo izgubljenog vremena (downtime).

Sigurna mrežna komunikacija podrazumijeva:

- Povjerljivost
- Integritet podataka
- Provjera autentičnosti krajnjih tačaka
- Operaciona bezbjednost

"Najsigurniji računar je onaj koji je isključen iz mreže i struje i zaključan u ormaru".

VRŠNJAČKO NASILJE NA INTERNETU

Mr. sci Musić Nijaz

Apstrakt: Sa historijskog aspekta, nasilje u svakom svom obliku je sve prisutnija pojava sa kojom se susreće društvena zajednica.. Percepcija društva je da je nasilje svakodnevno u porastu, uključujući i nasilje među vršnjacima i nasilje u školama, međutim, za sada nema sistematskog pristupa kada je u pitanju praćenja ove pojave, zbog čega ne možemo sa sigurnošću tvrditi kakvi su trendovi. Nasilje u školama nije pojava novijeg doba. Prije više generacija nasilje među vršnjacima je predstavljalo odmjeravanje snaga među pojedinim učenicima. Međutim, danas kada govorimo o oblicima vršnjačkog nasilja, više je nego očigledno da su ti oblici agresivnog ponašanja odavno izgubili obilježe bezazlenog dječjeg dokazivanja, s obzirom na to da je pojava recidivizma sve izraženija. Međutim, jednotreba imati u vidu,a to je da su zajedno sa tehnološkim napretkom, odnosno sve bržim razvojem informaciono-komunikacione tehnologije, kao što su računari, mobilni telefoni i internet već odavno postali sastavni i gotovo neizbjeglan dio naše svakodnevnice. Svakako da nagli razvoj informacionih tehnologija i sve rasprostranjenija primjena i korištenje računara i mobilnih telefona ima jako veliki uticaj i na nasilje.Nasilje putem interneta opšti je pojam za svaku komunikacionu aktivnost putem interneta, koja se može smatrati štetnom kako za pojedinca tako i za opšte dobro, a u svijetu je poznato kao cyberbullying, što u doslovnom prijevodu znači vršnjačko nasilje na internetu.Ako još uzmemo u obzir činjenica kako veliki broj djece i njihovih roditelja nije svjestan opasnosti do kojih može dovesti neprimjereno i nekontrolisano korištenje računara i interneta, onda je to još razlog više za poduzimanjem konkretnih mjera na prevenciji i suzbijanju ove društveno neprihvatljive pojave.

Ključne riječi: Maloljetnici, informacione tehnologije, bullying, cyberbullying, IP adresa.

UVOD -VRŠNJAČKO NASILJE-BULLYING

Potrebno je s posebnim oprezom govoriti o vršnjakom nasilju, kako ga ne bismo učinili jedinom temom o mladima i za mlade. Postoji nekoliko definicija vršnjakog nasilja, ali je svima zajedničko da govore o namjernom povredjivanju, o učestalom ponavljanju nasilja, o neproporcionalnom odnosu snaga, odnosno o namjernom i svjesnom postupanju da se kod žrtve izazove psihička i fizička bol. Nasiljem među djecom i mladima smatra se svako namjerno fizičko i psihičko nasilno ponašanje usmjereni prema djeci i mladima od strane njihovih vršnjaka učinjeno s ciljem povrijedjivanja, a koje se ovisno o mjestu izvršenja, može razlikovati po obliku, težini, intenzitetu i vremenskom trajanju i koje uključuje ponavljanje istog obrasca i odražava neravnopravan odnos snaga, a koje za posljedicu ima ugrožavanje zdravlja, razvoja i dostojanstva ličnosti žrtve.

Međutim, sve češće se javlja i nasilje kojem su djeca izložena putem interneta ili SMS poruka prijetećeg, uvredljivog ili provokativnog sadržaja.⁵ Ove činjenice govore da savremeno društvo donosi promjene u svim sferama života i da se nasilje i njegovi pojavnji oblici mijenjaju. Stoga, društvo ima veliku odgovornost i obavezu da prati i reaguje na sve oblike nasilja koji od pojedinanih slučajeva vrlo brzo prerastu u pojavu koju najprije prepoznaju mlađi. Zato je neophodno biti u stalnom kontaktu s djecom i slušati ih jer oni najbolje poznaju svoje vršnjake i njihov način razmišljanja i reagovanja. Primjera radi vrlo često djeca znaju za simuliranje vršnjake tuče koja se snima mobilnim telefonom a zatim "pušta" na internet strancama dostupnim svima kao što je You tube. Ova pojava govori o odnosu djece prema nasilju i o tome da je postalo „trend“ ponašati se agresivno, a svjedoci smo da je ovo vrijeme pripadanja grupi po svaku cijenu. O nasilju se mnogo govori i piše. Ono je udarna vijest, pa se smatra da ga ima više nego ranije. Koliko su te procjene tačne, teško je reći bez pravih i detaljnih istraživanja. O vršnjačkom nasilju se sve više govori što je dobro jer ga je lakše uočiti, prepoznati, spriječiti. Loša strana čestog pokretanja ove teme je stvaranje neadekvatne slike o djeci koja se generalno predstavljaju kao agresivna i sklona nasilju, te se kao takva i etiketiraju u jednoj sredini.

Suzbijanje svih oblika nasilja zahtijeva aktivno uključivanje svih u proces edukacije i prevencije koji će početi od učenika, nastavnika i roditelja. Ono što se ne smije zaboraviti jeste da je agresivnost osobina

⁵Dorić, M. (2009). Bulling kao vrsta socijalnog nasilja. Subotić, D. (Ur.), Politička revija, 145–164, Beograd: Institut za političke studije.

koja se razvija u ranom djetinjstvu pa ju je potrebno prepoznati još u najranijoj fazi i pravilno na nju reagovati. U našoj sredini važno je raditi na nekonfliktnoj komunikaciji koja može u mnogome biti ključ za spriječavanje nasilja.

Ovdje prije svega mislim na prevenciju ne samo vršnjakog nasilja na internetu, već nasilja uopšte, pa i maloljetnike delikvencije, te edukacije djece, nastavnika i roditelja o problemu vršnjakog nasilja i to bi bio jedan je od osnovnih oblika borbe protiv ovog društveno neprihvatljivog ponašanja. Državna strategija za borbu protiv nasilja nad djecom, 2007-2010⁶, obavezuje na uspostavljanje planova i programa na svim nivoima, od lokalne zajednice, entiteta i države, sa ciljem unapređenja aktivnosti na zaštitu djece od svakog oblika nasilja bez obzira da li se ono dešava u školi, porodici ili na ulici.

1. VRŠNJAČKO NASILJE NA INTERNETU- CYBERBULLYING

Cyberbullying ili nasilje na internetu je savremeni, moderni oblik vršnjačkog nasilja koji se realizuje pomoću sredstava masovne komunikacije koju koriste učenici, u prvom redu preko interneta i mobilnih telefona, u cilju ponižavanja, diskreditacije, omalovažavanja i na druge načine nanošenja štete drugima. Internet omogućava pristup mnogobrojnim korisnim informacijama i razmjenu iskustava između korisnika kad su u pitanju različite teme i različite oblasti života, od naučnostručnih istraživanja koja se provode diljem cijelog svijeta pa sve do razmijene iskustava korisnika o određenim proizvodima ili razmijene kulinarskih recepata za domaćinstvo. Djeca danas već od ranog uzrasta koriste internet, te na zabavan i zanimljiv način uče o tome kako koristiti informacione tehnologije.

Kao glavne odlike ovog oblika manifestovanja vršnjačkog nasilja su anonimnost nasilnika, širok sadržaj nasilja, specifični oblici ispoljavanja nasilnih sadržaja, brzo širenje sadržaja, dostupnost nasilnog sadržaja velikom broju lica, konstantnost i kontinuiranost ispoljavanja nasilja, sredina unutar koje se nasilje realizuje. Za razliku od klasičnog oblika ispoljavanja vršnjačkog nasilja, kod elektronskog vršnjačkog nasilja anonimnost nasilnika je najčešće zagarantovana, odnosno veoma teško je otkriti identitet nasilnika, uslijed čega nasilnik, znajući da je mogućnost njegovog otkrivanja, a samim tim i sankcionisanja, relativno mala, najčešće intenzivira nasilničke aktivnosti. Posljedica ovoga svakako je tendencija kvantitativnog, ali i kvalitativnog povećanja konkretnih oblika ispoljavanja elektronskog vršnjačkog nasilja. Naravno, činjenica je da se nasilnici i sami otkriju, kao i da nasilje preko interneta čine otkrivajući vlastiti identitet na početku ispoljavanja nasilnih sadržaja, ali je ovo rjeđe, što svakako nameće i potrebu revizije uobičenih biopsihosocijalnih karakteristika nasilnika, prihvaćenih analizom nasilnika koji vršeklasično vršnjačko nasilje

1.2. Istraživanja i podaci o vršnjačkom nasilju

Iako je provedeno malo istraživanja na temu međuvršnjačkog nasilja putem interneta, rezultati su vrlo zanimljivi. U jednom istraživanju koje je provedeno u Njemačkoj, čak 18 % djece u dobi od 12 do 14 godina bilo je žrtva nekog od oblika nasilja preko interneta, a 11 % njih izjasnilo se kao "internet nasilnici". Od djece koja su bila izložena učestalom nasilju na internetu, njih 62 % izjavilo je kako je nasilnik bio njima poznata osoba ili čak kolega iz razreda. Uz to, djevojčice su češće žrtve, ali i češći nasilnici na internetu od dječaka.

Istraživanje u SAD-u, koje je uključivalo djecu u dobi od 10 do 17 godina koja se redovnob koriste internetom, pokazalo je da je 19 % njih bilo izloženo seksualno neprimjerenum porukama. Od izložene djece, njih 25 % pokazivalo je veći stepen stresa nakon toga. Najveći stres bio je prisutan kod mlađe djece (dobi od 10 do 13 godina), kod djece koja su se koristila računalom izvan vlastitoga doma, djece koja su dobivala agresivne poruke seksualnog sadržaja, te u slučajevima kad je druga osoba pokušala dijete nagovoriti na susret.

Čini se da, što je dječja aktivnost na internetu više istraživačka, veća je vjerojatnost izlaganja nepoželjnom seksualnom sadržaju. Većina nepoželjnih izlaganja dogodila se dok su se djeца koristila računarom kod kuće, a 7 % djece susrelo se s porukama koristeći se računaram u školi.

⁶Državna strategija za borbu protiv nasilja nad djecom 2007 - 2010, („Službeni glasnik BiH”, broj: 46/07)

Djeca čiji roditelji nemaju pristup njihovim e-mailovima češće su primila poruke sa seksualnim sadržajima (32 % prema 20 % djece koji se koriste adresom roditelja za dopisivanje). Naime, pokazalo se da 49 % djece izjavljuje da roditelji nemaju pristup njihovoj pošti, a kod 16 % njih da „možda imaju“, što upućuje na smanjenu mogućnost nadzora sadržaja koji dijete prima putem e-mailova. Roditelji imaju pristup e-mailovima kod 22 % djece.

Trećina ove djece (33 %) nije nikome povjerila svoje iskustvo dobivanja poruka sa seksualnim sadržajima. A oni koji su se povjerili, najčešće su to učinili: priateljima (52 %), roditeljima (17 %), a 4 % djece reklo je nekoj drugoj odrasloj osobi, najčešće profesoru u školi. Djevojčice češće odmah obrišu ili zatvore pristigle poruke od dječaka (53 % prema 24 %).

Dječaci češće odu na ponuđene internetske stranice (20% prema 5%). Jedna četvrtina djece koja su bila izložena porukama sa seksualnim sadržajima izjavljuje da su imala uznenemirujuću emocionalnu reakciju, češće djevojčice (47 %, dječaci – 19 %) i mlađa djeca. Internetski bullying uključuje populaciju koja je većim dijelom srednja klasa, djecu najčešće poznatu kao “dobru” ili “one od kojih bismo najmanje očekivali” zlostavljanje ili ponižavanje drugih. Internet izaziva neobuzданo ponašanje dijelom i zbog činjenice da je riječ o “sivom području” društvene interakcije.

Stručnjaci ističu da internet eliminiše društvene kočnice. Dopušta djeci da govore i čine stvari koje ne bi mogli napraviti u interakciji “licem u lice”, i ona imaju osjećaj da neće morati odgovarati za takva ponašanja na način na koji bi inače odgovarali za, primjerice, javno izrečene riječi. To im daje lažan osjećaj sigurnosti i moći.⁷

S pravom možemo konstatovati da u današnje vrijeme djeca mnogo više vremena provode na internetu i za računaram nego u igri u prirodi i na otvorenom u društvu svojih vršnjaka. Odrastanje u ovom virtuelnom svijetu umnogome se razlikuje od načina odrastanja koji poznaju i koji su živjeli roditelji djece. Zbog takvog načina odgoja i vaspitanja djece postaje pravi izazov za roditelje koji su često nepripremljeni za sve izazove kojima su njihova djeca, iako nedorasla, itekako izložena na internetu. U situacijama kada dijete zatreba neke informacije, posebno ako se one odnose na učenje i razvijanje kreativnosti, internet predstavlja idealan medij. Upravo zbog toga roditelji ne mogu i ne treba da brane djeci pristup internetu. Za djecu i mlade internet je uglavnom veoma pozitivan, kreativan i produktivan medij, koji, između ostalog, koriste i u razvoju svog vlastitog identiteta. Djeci i mladima veoma je važno da putem interneta i raznih socijalnih mreža budu povezani sa svojim vršnjacima, da sa njima razmjenjuju iskustva, stavove, da pripadaju grupama koje okupljaju vršnjake istih ili sličnih interesovanja i slično. Ovakva komunikacija svakako da na određen način podržava socijalizaciju kod mlađih, međutim, stručnjaci koji rade sa djecom primjećuju da veliki broj djece koja u razredu nemaju nikakvu komunikaciju ili čak i ne razgovaraju, imaju veoma intenzivnu komunikaciju putem informatičkih sredstava. Iako internet pruža brzu dostupnost različitim i zanimljivim informacijama, kao i komunikaciju s velikim brojem ljudi, potrebno je biti svjestan i opasnosti koje može predstavljati. Glavni rizici upotrebe interneta za djecu su: izloženost uznenemirujućim, agresivnim ili nepristojnim e-mail porukama, direktna komunikacija s osobom koja traži neprimjerene odnose, izlaganje seksualnim sadržajima, pretjerana izolovanost djeteta koja je posljedica prečestog/dugotrajnog korištenja računara/interneta i sl. Djeca ne shvataju ozbiljno mogućnosti zloupotrebe interneta, kao ni potencijalne posljedice, a opet, spremna su da učestvuju u „igram“ i „šalamu“ koje su usmjerene prema drugoj djeci, ne shvatajući da mogu da dovedu do povrijeđenih osjećanja, narušenog samopouzdanja, ozbiljnih trauma, pa i do dramatičnih posljedica.⁸ Sindrom vršnjačkog nasilja na internetu i nasilja putem mobilnih telefona – tzv. „sajber buling“ (cyber bulling) širi se velikom brzinom na internetu. Fizičko i psihičko nasilje dobilo je novi oblik s kojim se susreću djeca i maloljetnici.⁹

Za razliku od „običnog bulinga“, koji se dešava u školi ili na ulici, zbog mogućnosti koje pruža internet, žrtva sajber bulinga može da doživi nepriyatnosti bilo kad i od bilo kuda, potpuno neočekivano i potpuno nepripremljena, tokom bilo kojeg doba dana ili noći, jer nasilnik, skrivajući se iza anonimnosti koju pruža

⁷Popović-Ćitić, B. (2009) Vršnjačko nasilje u sajber prostoru, Petrušić, N. (Ur.), Temida, 43–61, Beograd: Viktimološko društvo Srbije i Prometej;

⁸<http://www.poliklinika-djeca.hr>. pristup stranici izvršen 13.02.2016.godine;

⁹Procjena je, koju je iznio Asošijeted Pres, da je u SAD od 2003. godine najmanje 12 osoba starosti od 11–18 godina izvršilo samoubistvo uslijed izloženosti nekoj vrsti nasilja na internetu.

internet, često bude nepoznat i teško se otkriva njegov identitet. Vršnjačko nasilje na internetu podrazumijeva slanje poruka putem interneta ili mobilnog telefona sa ciljem da se povrijedi ili uznemiri neko dijete. Nasilje se manifestuje kroz tekstualne ili video-poruke, fotografije ili pozive kojima se šire nasilni i uvredljivi komentari o vršnjaku. Nasilje putem interneta može uključivati bilo kakav oblik višestruko slanih poruka internetom ili mobilnim telefonom čiji je cilj povrijediti, uznemiriti ili na bilo koji drugi način oštetiti dijete, mlade ili odrasle koji se ne mogu zaštititi od takvih postupaka. Može biti u obliku tekstualnih ili video poruka, fotografija ili poziva, a nasilje se sve češće odnosi na nekoliko oblika komunikacije, uključujući zvuk, slike, animacije i fotografije. Nasilje pitem interneta uključuje podsticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijedanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara. Može uključivati slanje okrutnih, zlobnih, katkad i prijetećih poruka, kao i kreiranje internet stranica koje sadržavaju priče, crteže, slike i šale na nečiji račun. Takvo se nasilje, nadalje, odnosi i na slanje fotografija svojih kolega te traženje ostalih da ih procjenjuju po određenim karakteristikama, odnosno da glasaju za osobu koja je, na primjer, najružnija, najnepopularnija ili najdeblja u školi. Djeca ponekad na određenoj popularnoj internet stranici traže od ostalih da navedu osobu koju najviše mrze te da o njoj napišu nekoliko riječi, a sve s ciljem da žrtvu osramote pred što većim brojem ljudi. Nasilje na internetu podrazumjeva „ulazak/provaljivanje“ u tuđe e-mail adrese te slanje zlobnih i neugodnih sadržaja drugima. Pored ovoga, vršnjačko nasiljem putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, vrijedanje te nesavjestan pristup štetnim materijalima. Sve češće se i na YouTube-u pojavljuju snimci fizičkog nasilja nad vršnjakom, sa velikim brojem pregleda i brojnim, često neprimjerenum komentarima koji sekundarno viktimizuju žrtvu kojoj se nasilje dogodilo. Društvene mreže se takođe koriste kao sredstvo za širenje nasilja, jer omogućavaju da u kratkom periodu veliki broj ljudi komentariše, vrijeda ili vidi fotografiju ili komentar. Konflikti koji ovako započinju uglavnom se završavaju fizičkim sukobima. Jedan od takvih novijih primjera jeste da djeca u tuđe ime otvaraju tzv. blogove ili profile na društvenim stranicama kao što je Facebook, Netlog, i slično. Zatim na tim stranicama iznesu nekoliko istinitih detalja o navodnom vlasniku bloga, odnosno profila kako bi podaci bili uvjerljivi onima koji poznaju tu osobu. Nakon toga navode ružne detalje ili na primjer napišu da „vlasnik bloga ili profila“ nudi seksualne usluge ili prodaje narkotička sredstva, te uz to navede tačan broj telefona i adresu. Dijete na čije ime je otvoren blog ili profil ne može izbrisati stranicu niti lažne podatke, jer mu je za to potrebna šifra koju ima samo onaj ko je zapravo i kreirao lažni blog, odnosno profil.¹⁰

Takođe, zabilježen je jedan primjer u Austriji gdje su vršnjaci jednog dječaka starosne dobi 12 godina, na jednoj Internet stranici prozvali islamskim teroristom, za drugog su proširili „vijest“ da je homoseksualac... Slična iskustva imala su i maloljetna lica iz Sarajeva. Jedan slučaj 2008. godine zabilježen je u Goraždu, kada se jedna učenica obratila supruzi svog razrednog starješine i predstavila se kao njegova ljubavnica, naravno sve ovo je uradila sa lažnog facebook profila kojeg je koristila i u komunikaciji sa drugim učenicima.

Ovakve prijave još uvijek izazivaju jedan vid zbuđenosti kod pripadnika policije, koji, očigledno nenaviknuti na ovakav vid nasilja odnosno zlostavljanja jer nisu imali priliku da se sa njim susretnu, često ne znaju kako da reaguju i kako da ovakve pojave okvalifikuju. Ovo je često posljedica činjenice da veliki broj odraslih ne koristi internet na način da otvaraju profile i blogove na internetu, pa im je teško i objasniti o čemu se zapravo radi.

Postoje specifičnosti nasilja putem interneta koje ga razlikuju od fizičkog nasilja u neposrednom odnosu, a to su:

- može biti prisutno 24 sata, svih sedam dana u sedmici;
- izloženost i kod kuće i na mjestima koja su ranije bila sigurna za dijete;

¹⁰Olweusova knjiga „Bullying at School“ prevedena je na hrvatski pod naslovom „Nasilje među djecom u školi“ (Olweus, 1998).

- publika i svjedoci mogu biti mnogobrojni i brzo se povećavaju;
- anonimnost pojačava osjećaj nesigurnosti kod žrtve;
- zlostavljanje putem interneta može biti prisutno među vršnjacima, ali mete mogu biti i odrasli, kao na primjer profesori i učitelji;
- bez fizičkog kontakta sa žrtvom i publikom, djeca i mladi teže vide i razumiju štetu koju njihove riječi mogu nanijeti, ponekad i poruke koje se šalju iz šale mogu povrijediti, premda nisu imale namjeru zlostavljati nekoga.

To su samo neki od mnogih primjera nasilja na internetu. Međutim, ono što mnoga djeca, mladi, a ni odrasli ne znaju jeste da se takvi događaji mogu i trebaju prijaviti provajderu, koji onda spornu stranicu ukloni s interneta, te se na taj način zaustavi nasilje, omalovažavanje i izrugivanje maloljetnog lica koje može da ima nesagledive posljedice.

2. PROVIDER I IP ADRESA

Svakom računaru s internetom, provider dodjeljuje poseban identifikacijski broj, tzv. IP adresu. Iz nje se može vidjeti gdje se nalazio određeni računar i koji provider koristi za spajanje na internet. Računaru se nasumično dodijeli nova IP adresa svaki put kad se spoji na internet. Računar providera bilježe koja se IP adresa dodijelila kojem računaru i u koje vrijeme. Statistike web stranica bilježe IP adrese računala koja su posjetila tu stranicu, a to znači da i vlasnik (administrator) internetske stranice i provider mogu znati vrijeme kad je neki računar pristupilo određenoj stranici, kao i gdje se ono nalazi. Provideri i administratori internetskih stranica zakonom su obvezani držati u tajnosti privatne podatke posjetitelja stranica. To pogotovo vrijedi za stranice na kojima su e-mail, chat, forum ili blog. Privatni podaci su ime i prezime, adresa, broj telefona, e-mail adresa, lozinka, te broj kreditne kartice, ali i IP adresa, s obzirom na to da se iz nje mogu saznati ostali podaci.

Međutim, ako se iz nekog razloga protiv posjetitelja stranice podnese prijava policiji, administrator stranice i provider obvezni su sarađivati sa policijom i omogućiti im uvid u svoje statistike kako bi mogli identificirati i pronaći počinitelja, te poduzeti zakonom propisane mjere s ciljem sankcionisanja počinitelja.

2.1. Prevencija

Još jedan oblik nasilja među vršnjacima koji nam donosi moderno doba tehnologije jeste i nasilje putem mobilnih telefona¹¹. Ovaj oblik nasilja uključuje bilo kakav oblik poruke zbog koje se osoba osjeća neugodno ili joj se na taj način prijeti – može biti tekstualna, video poruka, fotografija, poziv – odnosno, bilo kakva višestruko slana poruka kojoj je cilj uvrijediti, zaprijetiti, odnosno nanijeti bilo kakvu štetu maloljetnom vlasniku mobilnog telefona. Mogućnost da se izbjegnu ovakva nasilna ponašanja, s obzirom na to da se na internetu može dogoditi bilo kad i bilo gdje, veoma je mala. Pošto nasilnik može ostati anoniman, velikom broju djece upravo ta činjenica služi kao podsticaj da se nasilno ponašaju, iako u stvarnom svijetu vrlo vjerojatno ne bi bila nasilna. Zbog moguće anonimnosti internet može djelovati tako da se lakše otpuste kočnice neprihvatljivog ponašanja. Nasilnik dobije na hrabrosti jer se ne mora direktno suočiti sa žrtvom i dobija lažni utisak da je u potpunosti anoniman. Budući da nemaju direktnog kontakta sa žrtvom ili publikom, mladim nasilnicima je teže vidjeti i razumjeti štetu koju mogu prouzrokovati ovakvim oblikom nasilja. Često nemaju ni predstavu o tome da je takvo ponašanje prouzrokovalo štetu i kakve su sve posljedice takvog ponašanja. Upravo ova moguća anonimnost nasilnika pruža im lažan osjećaj da su sigurni i moćni, kao i osjećaj da to i dalje mogu nekažnjeno činiti.

Danas je među mladima, a kako se čini i među odraslima, uvriježeno mišljenje da nasilje putem interneta može proći nekažnjeno i da odrasli, a ni djeca ne mogu učiniti ništa da bi se taj vid nasilja zaustavio. Posljedice nasilja preko interneta često mogu biti i ozbiljnije od posljedica nasilja u stvarnim situacijama. Nasilje preko interneta često je mnogo šire od onog na školskom igralištu, u razredu, ispred zgrade i dostupnije mnogo većoj publici. Uz to, kod nasilja na internetu postoji snaga pisane riječi, jer žrtva može

¹¹Ured UNICEF-a za Hrvatsku, str. 16, <http://www.unicef.hr> pristup stranici izvršen 11.02.2016.godine;

svaki put ponovno da pročita šta je nasilnik o njoj napisao, a u verbalnom obliku uvrede se lako mogu zaboraviti. Pisana riječ djeluje konkretnije i realnije od izgovorene. Veliki broj korisnika kompjutera i interneta upravo su djeca, a samim tim i moguća grupa koja će se suočiti s ovim problemom. Žrtvi je u ovakvim situacijama još teže, jer može više puta pročitati šta je nasilnik o njoj napisao, pri čemu je publika koja svjedoči nasilju često mnogo šira nego kod drugih oblika vršnjačkog nasilja. Zbog svega navedenog, posljedice nasilja preko interneta katkad mogu biti i ozbiljnije od posljedica nasilja u stvarnim situacijama. Način da se počne rješavati problem jeste odgovornost čitave šire zajednice. Vršnjačko nasilje, kao i nasilje putem interneta kod maloljetnika nije problemsamo škole, niti samo roditelja. To je problem koji se rješava na multidisciplinarnom nivou na kojem treba da su uključeni roditelji, škola, služba socijalnog staranja odnosno centar za socijalni rad, policija i lokalna zajednica. Ne rješava se problem tako da se dijete uputi pedagogu, psihologu ili direktoru školu, te mu se, eventualno, izrekne neka kazna u školi za neprimjereno ponašanje. Samo zajedničkim naporima cijele školske zajednice, i nastavnika i roditelja i učenika, kao i centra za socijalni rad, te policije, problem "bullynga" i „cyberbullynga“ je moguće svesti na najmanju moguću mjeru. Prepuštanje tereta odgovornosti i djelovanja samo jednom učesniku, bilo da se radi o školi, policiji ili centru za socijalni rad, neće dati očekivane rezultate, niti će doprinijeti smanjivanju vršnjačkog nasilja među djecom i mladima u obrazovnom sistemu. Sveobuhvatna i kvalitetna zaštita djece podrazumijeva zajednički rad svih nadležnih institucija i tijela. Kada govorimo o vršnjačkom nasilju putem interneta, ova vrsta problema je relativno nova, nepoznata, i nažalost vrlo često neopravdano zanemarivana. Jedna od najvažnijih stvari u sprečavanju ovih dešavanja i pomaganju djeci da u savremenoj digitalnoj eri budu sigurna i zaštićena jeste da se i sami roditelji informišu o takvom obliku zloupotrebe interneta i načinima zaštite djece. Iako je dijete u kući za računaram, u svojoj ili dnevnoj sobi, to u današnje vrijeme nikako ne znači da nije u opasnosti. I roditelje i djecu neophodno je konstantno upozoravati na moguće opasnosti koje korištenje interneta može prouzrokovati, te i roditelje i djecu upoznati sa sigurnim načinima korištenja interneta. Djeca više nemaju tu sigurnost da mogu otići kući i skloniti se od nasilja. Danas, kada djeca i mlađi provode toliko vremena ispred računara, djeca lakše postaju metom nasilja putem interneta i izložena su mu toliko dugo koliko su na internetu.

ZAKLJUČAK

Vršnjačko nasilje je veoma složena pojava, koja je u poslednje vrijeme uzela jako veliki zamah, ali joj se i uprkos tome još uvijek ne pridaje dovoljno značaja. Vršnjačko nasilje predstavlja veoma, posmatrano iz perspektive žrtve predstavlja uznemirujuće iskustvo koje traje i po nekoliko godina. Ono može da dovede do psihičkih poteškoća kod maloljetnika različitog uzrasta, a posebnu pažnju potrebno je posvetiti maloljetničkom vršnjačkom nasilju putem interneta. Većina roditelja i njihova djeca nisu ni svjesna opasnosti koja vreba sa interneta. Još veći problem predstavlja činjenica da veliki broj roditelja uopšte ne koristi računar, te da nisu dovoljno upoznati sa društvenim mrežama, opasnostima kojima djeca mogu biti izložena na internetu te rizicima njegovog korištenja. Oni su vrlo često u zabludi da su djeca bezbjednija dok sjede kod kuće za računaram, nego dok provode vrijeme na ulici. Nažalost, situacija je sasvim drugačija, jer se još uvijek nije izgradio potpuno efikasan sistem zaštite djece na internetu. Zabранa pristupa internetu od strane roditelja najčešće će samo proizvesti kontra efekat, jer u današnjem svijetu informacionih-tehnologija internetu se može pristupiti bilo gdje i bilo kada. Nekad je dovoljno da dijete ode kod druge, u internet klub ili bilo koji kafić odakle prosječnim mobilnim telefonom može pristupiti internetu bez ikakve mogućnosti kontrole nad sadržajima kojima je izloženo.

U komunikacijskom smislu internet je veoma moćan vid komunikacije, ali treba napomenuti da je on ipak samo alat u rukama onih koji ga koriste. Potrebno je znati da internet, u zavisnosti od načina na koji se koristi, takve posljedice i proizvodi. Pravilnom edukacijom kao i adekvatnim preventivnim programima djeca se mogu zaštiti od opasnosti koje vrebaju sa interneta.

LITERATURA

- [1] Đorić, M. (2009). Bulling kao vrsta socijalnog nasilja. Subotić, D. (Ur.), Politička revija, 145–164, Beograd: Institut za političke studije.

- [2] Državna strategija za borbu protiv nasilja nad djecom 2007 - 2010, („Službeni glasnik BiH”, broj: 46/07).
- [3] Popović-Ćitić, B. (2009) Vršnjačko nasilje u sajber prostoru, Petrušić, N. (Ur.), Temida, 43–61, Beograd: Viktimološko društvo Srbije i Prometej;
- [4] <http://www.poliklinika-djeca.hr/>, pristup stranici izvršen 13.02.2016.godine;
- [5] U.S. Department of justice, (2008): Child abduction response plan, Federal Bureau of Investigation, Virginia.
- [6] Ured UNICEF-a za Hrvatsku, str. 16,<http://www.unicef.hr/> pristup stranici izvršen 11.02.2016.godine;
- [7] Olweusova knjiga „Bullying at School” prevedena je na hrvatski pod naslovom „Nasilje među djecom u školi” (Olweus, 1998).

NASILJE NA FEJSBUKU

“VIOLENCE ON FACEBOOK”

Prof. dr Mile Matijević,

Fakultet pravnih nauka Univerziteta za poslovne studije Banja Luka

Aleksandar Miladinović, mr

Visoka škola unutrašnjih poslova Banja Luka

Apstrakt: Imajući u vidu da se za nasilje smatra da je imanentno ljudskoj egzistenciji, razumljivo je da se ono inkorporiralo i u savremene tehnološke inovacije. U tom pogledu, primarno se nasilje može posmatrati kroz internet, a u ovoj internet (virtualnoj) realnosti, nasilje pored toga što egzistira, ono doživljava svoju kvalitativnu nadgradnju, u smislu da sama egzistencija u virtuelnom okruženju podrazumijeva izloženost određenom stepenu (virtuelnog) nasilja. Iako navedeno na prvi pogled djeluje bezazleno, treba imati u vidu inkorporiranost virtuelnog i realnog okruženja, a sledstveno tome i interakciju virtuelnog nasilja na konkretnog pojedinca. U tom kontekstu, u radu se percipiraju fenomenološki obrasci određenih nasilničkih aktivnosti i nasilnih sadržaja koje se konkretizuju na trenutno najmasovnijoj društvenoj mreži na Fejsbuku, poput elektronskog vršnjačkog nasilja na Fejsbuku, govora mržnje na Fejsbuku, uticaja ovog nasilja na korisnike Fejsbuka i na realno okruženje...

Ključne riječi: Fejsbuk, internet nasilje, internet okruženje, interakcija, vršnjačko nasilje, govor mržnje.

Abstract: Bearing in mind that the violence is that it is inherent to the current human existence, it is understandable that it is incorporated and the modern technological innovation. In this regard, primarily the violence can be viewed through the internet and in the internet (virtual) reality, violence, despite the fact that it exists, it is experiencing a qualitative upgrade in the sense that the very existence of the virtual environment involves exposure to a certain degree (virtual) violence. Although listed at first sight look harmless, one should bear in mind the incorporation of virtual and real environments, and consequently the interaction of virtual violence to a particular individual. In this context, the paper perceived phenomenological patterns of certain violent actions and violent content that is concretized in the currently most massive social networks on Facebook, such as electronic bullying on Facebook, hate speech on Facebook, the impact of this violence on the users of Facebook and the real environment. ..

Keywords: Facebook, internet violence, internet environment, interaction, bullying, hate speech.

UVODNA RAZMATRANJA

Za nasilje se često kaže da je opšta i najvažnija karakteristika prošlog vijeka, zbog čega bi XX vijek, smatraju neki, trebalo nazvati "vijekom nasilja". Nasilje postaje simbol, sastavni dio životnog stila, filozofija mladih ljudi. Ono figurira i funkcioniše kao sredstvo najraznovrsnijih oblika društvene moći, prvenstveno posmatrano sa pozicije mas-medija (Turjačanin, 2001: 200).

Ukoliko pođemo od maksime da živimo u vremenu nasilja i nasilju vremena (Koković, 2001: 9), a imajući u vidu mnogobrojne karakteristike interneta i kao medija, i kao okruženja, ali i kao lokacije, te populacije internauta, razumljivo je da je internet i poligon za ispoljavanje raznih oblika nasilja, koje je uglavnom verbalnog karaktera, ali ne treba zapostaviti ni njegove implikacije koje (može da) ima i u stvarnom okruženju.

U tom pogledu ni društvene mreže nisu izuzetak. Društvene mreže su poslednjih nekoliko godina jedna od najpopularnijih, ako ne i najpopularnija usluga na internetu. međutim, kvalitativna i kvantitativna ekspanzija društvenih mreža svakako da ima i svoju "tamnu stranu". Naime, uporedo sa ekspanzijom društvenih mreža, primjetna je i ekspanzija kriminalnih aktivnosti na društvenim mrežama ili prema korisnicima društvenih mreža. Navedenom je razlog, prije svega, masovnost korisnika društvenih mreža, ali isto tako i needukovanost korisnika o bezbjednosnim rizicima na društvenim mrežama, vlastita pasivizacija mogućnosti zaštite, virtuelni aspekt okruženja u kojem egzistiraju ove mreže...

Usljed navedenog, razni se oblici kriminaliteta i drugih kriminogenih i asocijalnih pojava, kao i sami akteri navedenih aktivnosti, "preseljavaju" u okruženje društvenih mreža, s obzirom na to da im navedeno okruženje omogućava da gotovo cijelokupne faze kriminalne aktivnosti (planiranje, pripremanje, vrbovanje žrtava, obezbjeđenje sredstava, sama realizacija, pribavljanje koristi) realizuju "iz sobe", odnosno korišćenjem usluga interneta preko društvenih mreža, znajući da je mogućnost otkrivanja njihovog identiteta minimalna.

To je uslovilo ekspanziju klasičnih kriminalnih aktivnosti (prevare, krađe, razni oblici nasilja, antiestablišmentsko djelovanje, terorizam), ali, isto tako, i savremenih oblika kriminalnih aktivnosti (krađe identiteta, krađe vremena, internet piraterije, internet nasilja). U tom kontekstu, kao najučestaliji, ali naravno ne i jedini oblici kriminalnih aktivnosti na društvenim mrežama se posmatraju prevare, krađe identiteta, piraterija, pornografija, pedofilija, terorizam, vršnjačko nasilje, govor mržnje, te razni oblici antiestablišmentskog djelovanja korišćenjem društvenih mreža (Miladinović, Petričević, 2012: 257).

Oblici nasilja na internetu¹², a pogotovo na Fejsbuku su razni i uslovljeni su mnogobrojnim mogućnostima koje sam Fejsbuk pruža korisnicima u okviru kojih se nalaze i nasilnici (korisnici koji produkuju nasilje), ali i žrtve (korisnici prema kojima je usmjereno nasilje). Naravno, pored navedenog, ispoljavanje raznih oblika nasilja može da se posmatra i u širem okruženju interneta, pa i u okviru realnog okruženja, ukoliko se ima u vidu da nasilje na Fejsbuku (može da) ima određene implikacije i na realno okruženje, odnosno na ljude koji nisu korisnici Fejsbuka, pa čak ni internauti.

Nasilje na Fejsbuku je posebno značajno, s obzirom na to da ne pogađa samo žrtvu koja je (najčešće) korisnik Fejsbuka, već ima uticaj i na druge korisnike Fejsbuka, što je nerijetko i cilj nasilnika. Naravno, razumljivo je da je cilj nasilnika da uvrede i ponižavanje žrtve koja je korisnik Fejsbuka predstavi što većoj populaciji, ali u ovom kontekstu treba diferencirati i sekundarni karakter ovog cilja, a to je da razni oblici prijetnje kod većine korisnika mogu da izazovu suprotnu reakciju prema nasilniku, što može da bude viktogenog karaktera. Međutim, mnogo goru "reakciju" korisnika Fejsbuka na konstantne i kontinuirane oblike nasilja prema žrtvi ili prema žrtvama, bez obzira na to da li su one korisnici Fejsbuka ili ne, izaziva upravo odsustvo reakcije od strane korisnika, pa čak i od strane administratora, pa i relevantnih subjekata društva (poput policije ili drugih formalnih i neformalnih subjekata u društvu), čime se na Fejsbuku smatra dopuštenim takvo stanje nasilja, odnosno nasilje se posmatra kao dopušteni, pa čak i podrazumijevani oblik komunikacije između korisnika Fejsbuka, što svakako kod većeg dijela populacije Fejsbuka stvara osjećaj nespokojsstva, nesigurnosti, nelagode, pa čak i straha od potencijalnih oblika nasilja usmjerenih i ka njima.

1. NASILNIČKE AKTIVNOSTI I NASILNIČKI SADRŽAJI NA FEJSBUKU

Povezanost Fejsbuka sa nasiljem, u kontekstu internet nasilja, treba se prevashodno posmatrati kroz prijetnje i vrijeđanje, ponižavanje i zlostavljanje, omalovažavanje i slične negativne aktivnosti koje se od strane drugih korisnika produkuju prema konkretnim korisnicima Fejsbuka, prema određenoj populaciji korisnika Fejsbuka, prema svim korisnicima Fejsbuka, prema internautima ili prema određenoj populaciji društva, čiji su pojedini članovi i korisnici Fejsbuka.

Konkretni i sigurno najučestaliji oblici ispoljavanja nasilja na Fejsbuku su svakako mnogobrojni oblici ispoljavanja raznih prijetnji, uvreda, ponižavanje i zlostavljanje, ali pod nasiljem u ovom širem kontekstu treba posmatrati i razne oblike omalovažavanja i degradiranja, maltretiranja, uhođenja, iritiranja, lažnog predstavljanja i mnogobrojne druge oblike negativnog ponašanja prema žrtvi sa ciljem da se žrtva povrijedi, uvrijedi, da ima konstantan osjećaj nespokojsstva, straha, ugroženosti... Izuzev prijetnji i uvreda, koje imaju direktni kriminalni kontekst, bez obzira na to da li se realizuju na Fejsbuku, u okviru interneta ili u stvarnom okruženju, za ostale oblike nasilja, bez obzira na okruženje u kojem se izvodi, ne može se tvrditi da su a priori kriminalnog konteksta, s tim što, naravno, ne treba bespogovorno negirati potencijalnu kriminogenost, pa i viktogenost.

Stoga bi se moglo reći da su ovi oblici nasilja na Fejsbuku bezazleniji, te predstavljaju svojevrsno šikaniranje žrtve kojima se primarno izaziva iritacija, diferentnost, rezignacija, frustriranost, ali, naravno, navedeno može da izazove i samo osjećanje nespokojsstva i nesigurnosti, pa i straha. U tom slučaju, za ove oblike nasilja, posmatrajući navedeno kroz šikaniranje korisnika, ne bi se moglo tvrditi da su bezazleni, bez obzira na to što se dešavaju u Fejsbuk okruženju. U tom kontekstu bi trebalo i navesti da će i blaži oblici šikaniranja i drugi bezazleniji oblici nasilja na Fejsbuku, ukoliko se blagovremeno i

¹² Nasilje na internetu, odnosno u okviru internet okruženja naziva se raznim imenima, poput sajber nasilje, digitalno nasilje, internet nasilje, on-lajn nasilje, elektronsko nasilje, virtuelno nasilje, sajberbuling (*Cyber-bulling*)... Iako ovi pojmovi nisu sinonimi, najčešće se i u stručnoj i u opštoj javnosti koriste kao takvi kako bi se njima označilo nasilje koje se dešava u internet okruženju.

adekvatno ne preduprijede ili ne sankcionišu, svakako vremenom dobiti i kvalitativnije i kvantitativnije razmjere.

Naravno, na Fejsbuku se kao primarni pojavljuju prijetnje i vrijedanje kao konkretni oblici nasilja prema drugim korisnicima, dok su ostali oblici sekundarnog karaktera i teško ih je diferencirati kao samostalne, s obzirom na to da su ili prateća pojava primarnih nasilnih aktivnosti na Fejsbuku ili se oni sami međusobno prepliću. Naravno, to ne umanjuje njihov kriminogeni aspekt prema potencijalnim ili konkretnim žrtvama.

Producovanje nasilja na Fejsbuku može da se posmatra kroz nasilne aktivnosti i nasilne sadržaje. Nasilne aktivnosti nasilnika na Fejsbuku podrazumijevaju takve aktivnosti korisnika Fejsbuka kojima on izaziva nespokojstvo, nesigurnost, pa i strah kod drugih korisnika, dok bi se pod nasilnim sadržajima podrazumijevalo postavljanje sadržaja na profil korisnika ili u okviru grupe ili stranice koje imaju nasilni karakter, odnosno kod drugih korisnika izazivaju nespokojstvo, nesigurnost, strah... Nasilne aktivnosti nasilnika predstavljaju praćenje drugih korisnika, dosađivanje drugim korisnicima, iritiranje drugih korisnika, lažno predstavljanje... Nasilnim sadržajima nasilnika bi mogli okarakterisati gotovo svi sadržaji koje oni postavljaju na svoj profil ili u okviru grupe ili stranice, a za koje znaju (ili im je to i cilj) da izazivaju osjećaj nespokojstva, nesigurnosti i straha prema žrtvi, odnosno kod žrtve. To mogu da budu objavljeni prijeteći ili uvredljivi statusi na profilu žrtve ili u okviru grupe, objavljeni ili podijeljeni tekstualni, muzički, video ili slični sadržaji, kvizovi ili slične aplikacije koje svojim performansama, dizajnom, načinom funkcionisanja ili sličnim kontekstom aludiraju na okolnosti koje kod žrtve izazivaju strah, nespokojstvo ili nesigurnost... Takođe, pod nasilnim sadržajima treba podrazumijevati i postavljanje fotografija neprimjernog sadržaja na profil nasilnika ili žrtve ili činjenje određenih kompromitujućih fotografija javnim u okviru Fejsbuka... Naravno, mnogobrojne su i druge mogućnosti nasilnih sadržaja, pa i nasilnih aktivnosti na Fejsbuku od strane nasilnika prema žrtvi, ali su navedeni najučestaliji, a među njima su svakako najkonkretniji oblici nasilja prijetnje i vrijedanje (Miladinović, 2013: 160).

2. OBLICI ISPOLJAVANJA NASILJA NA FEJSBUKU

Prijetnje su svakako najučestaliji i najkonkretniji oblik nasilja na Fejsbuku. Ovaj oblik nasilja se najčešće realizuje od strane nasilnika prema žrtvi, ali tako da sama prijetnja bude vidljiva i cijeloj Fejsbuk zajednici, uslijed čega se prijetnje najčešće postavljaju na profil žrtve ili na profil nasilnika, ali sa jasnom aluzijom ko je žrtva. Prijetnje se najčešće postavljaju sa pravog profila nasilnika, mada ne mora da bude slučaj, pogotovo ukoliko nasilnik želi da ostane anoniman. Međutim, anonimnost nasilnika svakako i umanjuje efekat koji žrtva osjeća, čega su svjesni i nasilnici, te najčešće prijetnje i realizuju sa vlastitim, pravim profila, pogotovo ukoliko su svjesni male mogućnosti sankcionisanja takvog ponašanja. Pored objavljuvanja prijetnji na profilu, česte su i prijetnje u međusobnoj komunikaciji korisnika (u okviru četa ili preko poruka na Fejsbuku) koje svakako ne treba zanemarivati, iako je razumljivo da su ove prijetnje najčešće latentne, pogotovo ukoliko se sama prijetnja ne realizuje. Prijetnje mogu da se objavljuju i u okviru grupe i stranica.

Dok su prijetnje apstraktnejše (naravno, ne zapostavljajući ni prijetnje gdje se žrtvi direktno prijeti tjelesnim povredama, smrću, trovanjem, paljenjem imovine...), uvrede preko Fejsbuka, kao jedan od oblika ispoljavanja nasilja na Fejsbuku daleko su konkretnije i najčešće aludiraju na određenu karakteristiku žrtve, bez obzira na to da li se ona posmatra u fizičkom, intelektualnom, duhovnom, religijskom, nacionalnom, geografskom, polnom, seksualnom, starosnom, porodičnom, profesionalnom, kulturološkom ili nekom drugom segmentu. Najčešće ta karakteristika žrtve nije opštepoznata, odnosno nije poznata u okruženju u kojem sama žrtva egzistira, a javno objavljuvanje navedenog (korišćenjem Fejsbuka) u širem društvenom kontekstu predstavlja uvodu za žrtvu ili sama žrtva smatra da navedeno predstavlja uvodu ili kod nje izaziva osjećaj straha, nespokojstva, nesigurnosti, ali i sramote i stida. Naravno, uvrede se najčešće realizuju postavljanjem uvredljivih poruka na profil nasilnika ili žrtve ili u okviru grupe, ali nisu za zapostavljanje ni fotografije i video-snimci uvredljivog karaktera. Štaviše, uslijed svog komunikaciono-distributivnog karaktera u odnosu na poruke, fotografije i video-snimci (na kojima se, uglavnom, nalazi žrtva u kompromitujućem kontekstu) svakako su opasniji i nasilniji sadržaj za širenje i nanošenje uvreda od poruka i sličnih sadržaja. Uvrede su sredstvo ponižavanja, omalovažavanja i degradiranja ličnosti žrtve, koja je korisnik (ali i ne mora da bude) Fejsbuka. Upravo je cilj vrijedjanja ponižavanje i omalovažavanje žrtve.

Za razliku od uvreda, koje su, iako upućene žrtvi, namijenjene širem društvenom ambijentu kakav je i Fejsbuk, ali i van njega, dotle se maltretiranje i zlostavljanje žrtava radi sa namjerom da se prema žrtvi izraze ta negativna osjećanja, bez namjere (odnosno, ona nije primarna) da se i šira Fejsbuk zajednica ili čak zajednica van Fejsbuka upozna sa navedenim. Usljed navedenog, ovaj oblik nasilja na Fejsbuku, iako je nesumnjivo prisutan, svakako da se ne ispoljava u velikoj mjeri, odnosno nije evidentan, imajući u vidu da se nasilne aktivnosti i nasilni sadržaj najčešće odvija jednosmjerno (od nasilnika ka žrtvi) ili dvosmjerno (i nasilnik i žrtva jedno prema drugom produkuju nasilne aktivnosti i nasilni sadržaj), dok treći korisnici Fejsbuka, pogotovo šira Fejsbuk zajednica nije upoznata sa navedenim.

Uhođenje predstavlja poseban, specifičan oblik nasilja na Fejsbuku koji se najčešće realizuje između korisnika koji su bili ili su još uvijek u određenim odnosima koji imaju (ili su imali) karakter bliskosti, odnosno određene povezanosti i uslovjenosti (u vezi, u braku, u porodici, na poslu...). Uhođenje korisnika korišćenjem Fejsbuka podrazumijeva da je i sam nasilnik (koji vrši uhođenje) na Fejsbuku, odnosno ima pristup Fejsbuku preko kreiranog lažnog ili čak i pravog profila. Najčešće je i prijatelj sa žrtvom, uz znanje ili čak i neznanje žrtve, a moguće je da je prijateljstvo "sklopljeno" i na prevaru, odnosno da žrtva nije upoznata sa pravim identitetom nasilnika koji je prati, odnosno nije upoznata sa pravim namjerama. Kao što se u realnom svijetu uhođenje sastoji u praćenju kretanja žrtve, tako se i na Fejsbuku prati "kretanje" žrtve kroz njene aktivnosti koje ima, te se u tom kontekstu, žrtva "prati" sa kim ostvaruje komunikaciju i sadržaj komunikacije, koje sadržaje dijeli sa interneta, koje sadržaje lajkuje, kojih stranica ili grupa je (aktivni) član, kakve statuse objavljuje...

Naravno, za sve navedene aktivnosti bi se teško moglo reći da su nedozvoljene, imajući u vidu da većina korisnika, svjesno ili nesvesno, ponekad ostvaruje uvid u sadržaje drugih korisnika. Međutim, kriminogeni kontekst navedenih aktivnosti, koje im daju atribut nasilnosti kroz šikaniranje, ali i kroz daleko nebezazleniji kontekst, konkretizuje se prilikom daljih aktivnosti samog nasilnika koji će takav sadržaj zloupotrijebiti radi realizacije vlastitih aktivnosti i ciljeva. Naime, cilj nasilnika nije samo uvid u aktivnosti žrtve, već upravo prikupljanje "sadržaja" kojim će prema žrtvi konkretizovati određenu aktivnost koja će kod nje same izazvati osjećaj uznemirenosti, nesigurnosti, pa i straha. Taj osjećaj može da bude rezultat kako upoznatosti nasilnika sa određenim aktivnostima žrtve, tako i sistematicnosti nasilnika u prikupljanju sadržaja i kontrolisanju žrtvinih aktivnosti. Naravno, ovdje se polazi od toga da žrtvine aktivnosti nisu, same po sebi, kompromitujuće po nju samu, ali osjećaj konstantnog i kontinuiranog "praćenja" njenih aktivnosti na Fejsbuku, pa i na internetu, te korišćenje tih saznanja u određene, nelukrativne svrhe svakako da ne izaziva pozitivne efekte korišćenja Fejsbuka i interneta kod žrtve.

Kao što je već navedeno, uhođenju na internetu najviše pribjegavaju nasilnici koji su u određenoj vezi ili odnosu sa žrtvom (bivši ili sadašnji supružnici, bivši ili aktuelni momak i djevojka), međutim, primjetno je da sve više poslodavci kontrolišu vlastite radnike u pogledu njihovih aktivnosti na Fejsbuku, kako za vrijeme radnog vremena, tako i van radnog vremena. Iako ova aktivnost sama po sebi nema karakter dopuštene, pa ni etične, sve više poslodavaca narušava privatnost vlastitih radnika kontrolišući njihove aktivnosti na Fejsbuku, njihovu posjećenost Fejsbuka, produktivnost na radu u kontekstu korišćenja Fejsbuka u toku radnog vremena, a pogotovo komentare u pogledu ocjenjivanja samog poslodavca, prizvodnog procesa, usluga ili proizvoda poslodavca, uslova u kojima se izvodi proizvodni proces, radnih uslova... Iz ovog je vidljivo da ovaj trend korporativnog uhođenja na internetu nije mimošao ni Fejsbuk. Štaviše, s obzirom na mogućnosti koje im Fejsbuk pruža, poslodavci se sve više odlučuju na uhođenje radnika samo preko ove društvene mreže, zanemarujući mogućnosti koje im pružaju ostale usluge na internetu. Poseban problem ovako posmatranog korporativnog uhođenja preko Fejsbuka ne odnosi se samo na neetičnost i nedozvoljenost navedenog usljed narušavanja njihove privatnosti, već upravo na zloupotrebu informacija i podataka do kojih se dođe uvidom u žrtvine podatke i informacije, odnosno objavljeni ili postavljeni sadržaj na profilu ili u okviru grupe i stranice. Naime, Fejsbuk omogućava nasilnicima da saznaju kada je žrtva koristila Fejsbuk, u kom periodu, koliko dugo, na koji način ga je koristila i slično, što mogu da iskoriste kako bi, eventualno, ukazali na pad produktivnosti rada žrtve usljed (prekomernog ili nedozvoljenog) korišćenja Fejsbuka za vrijeme radnog vremena ili sa radnog mjesta.¹³ S obzirom na karakteristike korporativnog uhođenja na Fejsbuku, neminovno se nameće i

¹³ Međutim, činjenica je da se otkazi na Fejsbuku mogu posmatrati i u okviru komentara koje postavljaju radnici, a tiču se njihovog zaposlenja, radnog mjeseta, usluga koje pružaju, proizvoda, međuličnih odnosa, atmosfere na poslu... Na primjer, konobarica iz

zaključak da ono predstavlja svojevrsni mobing radnika¹⁴, koji, doduše, još uvijek nije etabliran kao takav u radnim odnosima, odnosno u odnosima poslodavca i radnika, ali će, svakako, i uslijed kvantitativnosti, ali i uslijed kvalitativnosti, svoju afirmaciju ubrzo doživjeti i u radnim sporovima.¹⁵

3. FENOMENOLOGIJA NASILJA NA FEJSBUKU

Na Fejsbuku je nasilje najčešće usmjereno ka drugim korisnicima Fejsbuka, bez obzira na to da li je u pitanju pojedinačna žrtva ili više korisnika Fejsbuka. Međutim, primjetno je da se sve više Fejsbuk koristi i za ispoljavanje nasilnih akata prema određenoj društvenoj, formalnoj ili neformalnoj populaciji čiji su pojedini članovi, pretpostavlja se, i korisnici Fejsbuka. Za razliku od prvog slučaja, gdje je Fejsbuk najčešće primarna ili čak i jedina "lokacija" preko koje se nasilje realizuje, u ovom drugom slučaju Fejsbuk predstavlja "sredstvo" preko kojeg se maksimizira nasilje koje je već etabirano u društvu, pa se i na ovaj način želi nastaviti. Jasno je da i ovdje Fejsbuk može da ima primarnu ulogu u realizaciji nasilja, ali je ipak pretpostavka da će mu ta uloga biti sekundarnog karaktera, s obzirom na to da će samo nasilje, podrazumijevajući pod navedenim i akte fizičkog nasilja, svakako biti i učestalije i konkretnije i ekstremnije i većeg obima u stvarnom okruženju. Međutim, dok bi ovi oblici nasilja, podrazumijevajući pod navedenim nasiljem i upotrebu fizičkog nasilja, bili svakako opasniji i direktniji, odnosno konkretni i u realnom okruženju, ne treba zapostaviti jednu opasnost koje nosi sa sobom "nastavljanje", odnosno produbljivanje nasilja i preko Fejsbuka. Naime, širenjem ili propagiranjem nasilja kod dijela korisnika Fejsbuka takođe se može ispoljiti saglasnost, pa i volja za vršenjem fizičkog nasilja prema žrtvama, a imajući u vidu rasprostranjenost populacije korisnika Fejsbuka, nije teško pretpostaviti kolike bi to imalo posljedice (Miladinović, 2013: 168).

U ovom kontekstu, ali i kao specifični oblici nasilja korišćenjem mogućnosti Fejsbuka, primarno, ali ne i jedino mogu da se posmatraju vršnjačko nasilje, govor mržnje, bogohuljenje, zakazivanje narušavanja javnog reda i mira...

Jedan od najučestalijih oblika kriminogenog ponašanja na društvenim mrežama je vršnjačko nasilje. Ovaj oblik elektronskog nasilja usmjeren ka mlađim korisnicima društvenih mreža posebno je poguban, pogotovo u odnosu na klasične oblike ispoljavanja vršnjačkog nasilja, s obzirom na to da su žrtve ovom

Sjeverne Karoline je otpuštena zato što je na Fejsbuku kritikovala mušterije koje su tri sata provele u piceriji i ostavile joj napojnicu od (samo) pet dolara. Konobarica je navela da je zbog siće morala da radi prekovremeno. Picerija ju je otpustila zato što je kritikovala mušterije i predstavila piceriju u lošem svjetlu. Zabilježen je i slučaj iz SAD-a gde je jedna kancelarijska službenica na svom profilu kritikovala svog šefa, zaboravljajući da joj je na listi prijatelja i da može da pročita njen komentar. Nekoliko minuta kasnije dobila je otkaz, takođe, putem Fejsbuka!

¹⁴ U kontekstu ovakvo predstavljenog korporativnog uhodenja na Fejsbuku, ne treba izvlačiti zaključak o dozvoljenosti korišćenja Fejsbuka u radno vrijeme ili na radnom mjestu ili preko određenog vremena. Naravno, ukoliko pravila poslodavca podrazumijevaju nemogućnost korišćenja Fejsbuka u toku radnog vremena ili sa radnog mjesta ili van određenog perioda, svakako da navedeno predstavlja kršenje discipline od strane radnika koje se može sankcionisati. Međutim, utvrđivanje disciplinske odgovornosti svakako ne podrazumijeva uhođenje radnika preko Fejsbuka, pogotovo imajući u vidu mnogobrojne druge mehanizme i načine utvrđivanja korišćenja Fejsbuka sa radnog mjesta ili u toku radnog vremena (preko fajrvola, na primjer).

¹⁵ U tom kontekstu, treba navesti da je Illinois druga država u SAD koja je zabranila poslodavcima da od zaposlenih i kandidata za posao traže podatke potrebne za pristup njihovim nalozima na društvenim mrežama. S obzirom na razvoj društvenih mreža, zakon treba da zaštitи pravo na privatnost zaposlenih. Merilend je prva država i za sada jedina koja je zakonski zabranila poslodavcima da od zaposlenih i kandidata za posao traže lozinke za naloge na društvenim mrežama. Druga države u SAD za sada razmatraju mogućnost donošenja sličnih zakonskih odredaba koje bi zabranile ovakvu praksu poslodavaca u SAD zahvaljujući kojoj se oni koji konkurišu za poslove često izbacuju sa liste kandidata. Problem je dostigao takve razmjere da nije rijetko da oni koji tragaju za poslom privremeno deaktiviraju svoj profil i druge naloge na društvenim mrežama sve dok ne pronađu posao, poslije čega ih ponovo aktiviraju. Jedan od predlagajućih zakona je ilustrativno objasnio ovaj problem: "Poslodavcima svakako nije dozvoljeno da traže od zaposlenog ključeve od kuće kako bi mogli da je prouštuju tamo, tako da vjerujem da ista očekivanja u vezi s privatnošću i ličnim prostorom treba da budu proširena i na naloge na društvenim mrežama!". Nadalje se dodaje da poslodavcima nije dozvoljeno da postavljaju pitanja zaposlenima ili kandidatima za posao o godinama, polu, rasi ili seksualnoj orientaciji, a sve ove informacije mogu se otkriti na društvenim mrežama. Prema podacima koji su objavljeni prilikom potpisivanja zakona, 75% poslodavaca pregleda profile kandidata za posao, a trećina njih odbija njihove prijave zbog onoga što otkriju o njima tokom pregleda njihovih profila na društvenim mrežama. Kazne za pokušaj pristupanja podacima koji su zaštićeni podešavanjem privatnosti naloga iznosiće najmanje 100 do 300 dolara, ali mogu biti i veće od toga. www.informacija.rs/Drustvene-mreze/Illinois-Poslodavcima-zabranjeno-da-traže-lozinke-Facebook-naloga-zaposlenih.html.

Pored Illinoisa i Merilenda, krajem 2012. godine i Mičigen je donio zakon za zaštitu privatnosti na internetu, kojim se zabranjuje zaposlenima i obrazovnim institucijama da od pojedinaca zahtijevaju omogućavanje pristupa (dakle, da se traže identifikacioni i autentifikacioni podaci) ili posmatranje sadržaja (nadgledanje) na ličnim nalozima na internetu. Takođe, slični zakoni su u pripremi i u Delaveru i u Kaliforniji. www.bug.hr/vijesti/kad-sef-iste-lozinku/120836.aspx.

nasilju izložene konstantno i kontinuirano, bez obzira na to da li su korisnici društvene mreže ili ne. Drugim riječima, žrtva vršnjačkog nasilja na društvenim mrežama može da se postane čak i ukoliko ona sama nije korisnik društvenih mreža, pa ni interneta. Uzrok ovome je što nasilnički sadržaj (bez obzira na to o kakvoj vrsti sadržaja se radi) dolazi do drugih korisnika društvenih mreža koji poznaju žrtvu ili su iz njenog životnog okruženja, a čega je svjesna i sama žrtva, uslijed čega dolazi do njene reakcije u vidu pasivizacije i drugih posljedica koje vršnjačko nasilje nanosi samoj žrtvi (Matijević, Miladinović, Petričević, 2011).

S obzirom na to da su mlađi korisnici interneta (iz kojeg se "crpe" žrtve vršnjačkog nasilja, ali najčešće i sami nasilnici) uglavnom korisnici Fejsbuka, dok ostale društvene mreže rjeđe koriste, oblici elektronskog nasilja na društvenim mrežama se najučestalije i ispoljavaju na ovoj društvenoj mreži. Pored toga, Fejsbuk okruženje nasilniku omogućava anonimnost djelovanja i mnoštvo mogućnosti, dok žrtvi onemogućava bijeg i (efikasnu) zaštitu, a isto tako, i masovnost korisnika Fejsbuka, pogotovo vršnjačke populacije, kao i brzina širenja određenih sadržaja na Fejsbuku među korisnicima i lokalna fokusiranost i koncentrisanost korisnika, svakako da omogućavaju ekspanziju nasilnih sadržaja i aktivnosti vršnjačkog nasilja na Fejsbuku.

Kada su u pitanju faktori koji omogućavaju vršnjačko nasilje na Fejsbuku kao poseban oblik elektronskog vršnjačkog nasilja, činjenica je da samo Fejsbuk okruženje doprinosi tome. U tom kontekstu, pored formiranja grupe i anonimnosti korisnika koje omogućavaju lažni profili, što je već obrađeno, neophodno je da se obrati pažnja na sadržaje koji se postavljaju na novostima, zatim na mogućnost postavljanja aplikacija, na "lajkovanje"... Takođe, u kontekstu realizacije elektronskog vršnjačkog nasilja na Fejsbuku neizostavno je da se pomene i "tagovanje" žrtve neprimjerenum fotografijama ili drugim sadržajem, zatim mogućnosti koje omogućavaju tzv. "alatni profili", "hejterske" grupe i aktivnosti, postavljanje seksualno inkriminišućeg i ponižavajućeg sadržaja (seksting), seksualno napastovanje (grumming) (Miladinović, 2013)...

Ono što elektronsko vršnjačko nasilje preko Fejsbuka čini posebno pogubnim za žrtvu jeste masovnost korisnika, kao i lokalna fokusiranost većine korisnika Fejsbuka, a pogotovo nasilnika, pasivnih subjekata (posmatrača) i žrtve. Masovnost korisnika Fejsbuka je pogotovo velika među vršnjačkom populacijom. Ukoliko se tome doda da većina korisnika, pogotovo među ovom populacijom, za prijatelje ima korisnike iz lokalne sredine, jasno je da se nasilni sadržaj svakako veoma brzo širi u okviru sredine iz koje su, najčešće, i nasilnik i žrtva, kao i pasivni posmatrači.

Govor mržnje svakako nije nepoznanica na internetu, pa čak ni u konvencionalnim medijima, ali je svakako punu negativnu afirmaciju pronašao na društvenim mrežama, a pogotovo na Fejsbuku. To mu omogućava, prije svega, anonimnost subjekta, kao i fokusiranost ka što većoj populaciji, ali isto tako, i distanciranost od pasivnog subjekta, odnosno subjekta kojem je sam govor mržnje upućen. Naime, pored krađa profila i raznih oblika ispoljavanja prevarnih aktivnosti na društvenim mrežama, posebno su učestali razni oblici ispoljavanja nasilja, prije svega elektronskog nasilja, kroz govor mržnje. S obzirom na masovnost korisnika, kao i heterogenost korisnika u smislu pripadnosti određenim neformalnim društvenim grupama (nacionalnoj, vjerskoj, regionalnoj, lokalnoj, polnoj, obrazovnoj, seksualnoj, manjinskoj), a pogotovo s obzirom na mogućnost anonimnog djelovanja, preko društvenih mreža se sve više ispoljavaju razni oblici elektronskog nasilja koji se najčešće ispoljavaju kroz govor mržnje koji se ogleda u prijetnjama, ponižavanju, maltretiranju, ismijavanju i na druge slične degradirajuće načine. Karakteristika ovog oblika ispoljavanja govora mržnje jeste da se on najčešće realizuje prema određenoj populaciji korisnika društvenih mreža, najčešće manjinskoj (nacionalnoj, vjerskoj, seksualnoj) populaciji u određenom društvu, dok se rjeđe ispoljava prema konkretnom korisniku, iako ni navedeno ne izostaje, pogotovo kada su u pitanju korisnici društvenih mreža koji su u određenoj zajednici poznatiji, odnosno u određenom društvu imaju konkretnu formalnu ili neformalnu ulogu.

Ono što je karakteristično za govor mržnje na Fejsbuku je što on nije upućen konkretnom korisniku Fejsbuka, odnosno konkretnim (imenom i prezimenom identifikovanim) korisnicima Fejsbuka, već što se odnosi, odnosno upućen je korisnicima Fejsbuka sa određenim nacionalnim, vjerskim, seksualnim, polnim, regionalnim, starosnim, fizičkim, medicinskim, obrazovnim, profesionalnim ili sličnim karakteristikama. Naravno, činjenica je da se govor mržnje bazira, prije svega, na vjerskom, nacionalnom i seksualnom identitetu, uslijed čega su ovakvi ispadli i najčešći. Pored toga što govor mržnje na Fejsbuku podrazumijeva kreiranje grupa koje samim imenom ili sadržajem asociraju ili impliciraju na govor mržnje prema određenoj individualizovanoj grupi korisnika, česti su i slučajevi poimeničnog prozivanja korisnika Fejsbuka koji pripadaju grupi koja je meta napada govora mržnje. Iako je navedeno samo po

sebi neprijatno, nije i najgore, pogotovo što navedeno može da kod ostalih korisnika Fejsbuka stvori (ili afirmaše već postojeću) atmosferu linča, što (može da) rezultira i preduzimanjem konkretnih fizičkih aktivnosti prema metama govora mržnje. Ovdje se vidi jedna povezanost samog govora mržnje na Fejsbuku sa potencijalnim fizičkim ugrožavanjem određenih pripadnika konkretne (manjinske) populacije u zajednici, jer govor mržnje, sam po sebi neprijatan za pasivnog subjekta, najčešće, ukoliko se ne predupređuje, potencira i fizičko ugrožavanje pasivnih subjekata u vidu fizičkih napada na njih, ponižavanja, omalovažavanja i slično. Usljed navedenog, govor mržnje na Fejsbuku, iako često kreiran od strane bezazlenih korisnika, ne treba bezazleno posmatrati, upravo usljud efekta koji izaziva među drugim korisnicima, te na njega treba adekvatno reagovati, i od strane administratora na Fejsbuku, ali i od strane formalnih, pa i neformalnih subjekata u društvu (Miladinović, Petričević, Salamadija, 2013: 399). Usko povezano sa govorom mržnje, odnosno kao jedan vid ispoljavanja govora mržnje javlja se i blasfemija, odnosno blasfemično djelovanje (ispadi) na Fejsbuku.

4. INTERAKCIJA NASILJA NA FEJSBUKU NA REALNO OKRUŽENJE

Posmatrajući podjelu internet nasilja na dva glavna vida ispoljavanja ovog nasilja, mogu da se izvedu i određene paralele sa ispoljavanjem ovog nasilja i na Fejsbuku, te se i nasilje preko Fejsbuka može posmatrati u kontekstu direktnih i indirektnih oblika ispoljavanja nasilja na internetu.

Direktни oblici ispoljavanja nasilja na Fejsbuku bi podrazumijevali one oblike nasilja gdje nasilnik direktno, koristeći se mnogobrojnim mogućnostima Fejsbuka, a primarno preko svog profila kreiranog pod tačnim identifikacionim podacima, plasira razne nasilne aktivnosti. U ovom slučaju, nasilnik nema namjeru prikrivanja identiteta, već nasilje produkuje sa pravog profila ili iz grupe ili stranice kreirane na osnovu pravog profila. U ovom slučaju će se najčešće raditi o bezazlenijim oblicima nasilja, kao i o oblicima nasilja usmјerenog ka konkretnoj ličnosti, odnosno korisniku profila, mada nije za prenebregavanje ni činjenica da se preko autentičnog profila može plasirati i nasilje koje se sigurno ne bi moglo okarakterisati kao bezazleno, pa čak i ono nasilje koje ima implikacije na realno okruženje u vidu ispoljavanja nasilnih sadržaja.

Indirektni oblik ispoljavanja nasilja na Fejsbuku podrazumijeva prethodnu kompromitaciju profila korisnika ili kreiranje lažnog profila, pa se, pod plaštom anonimnosti ili pseudonimnosti ili lažnog identiteta, prema drugom korisniku ili prema drugim korisnicima produkuje nasilje. U ovom slučaju će se najčešće raditi o masovnim oblicima ispoljavanja nasilja, odnosno o nasilju koje je usmјereno ka određenoj populaciji korisnika ili prema više korisnika, s tim što se, naravno, može desiti da se realizuje i prema konkretnom korisniku, iz razloga kako on ne bi otkrio ko prema njemu primjenjuje nasilje. Naravno, u svrhe masovnog nasilja na Fejsbuku, odnosno produkovanja masovnih nasilnih sadržaja i aktivnosti, nasilnici najčešće kreiraju grupe preko lažnih ili kompromitovanih profila, te u okviru tako kreiranih grupa propagiraju nasilje, koje, naravno, ima implikacije i van grupe, a nerijetko i van samog Fejsbuka.

Naravno, ovu podjelu nasilja na Fejsbuku treba posmatrati uslovno, imajući u vidu njihovu potencijalnu isprepletenost, kao i nekonstantnost.

Neophodno je osvrnuti se na jednu specifičnost, odnosno kauzalitet nasilja na Fejsbuku sa pretpostavljenim, odnosno potencijalnim nasiljem u stvarnom okruženju, koje može da rezultira i primjenom fizičkog nasilja prema žrtvi (ali i prema nasilniku), čiji ishod može da bude i smrtni. Naime, samo nasilje na Fejsbuku, pored toga što izaziva nespokojstvo, nesigurnost i strah kod korisnika Fejsbuka koji je žrtva tog nasilja, može da podstakne lančanu reakciju u vidu drugih korisnika Fejsbuka koji takvo ponašanje prema žrtvi smatraju prihvatljivim, podrazumijevanim, pa čak i zahtijevanim, usljud čega mogu posegnuti za aktima fizičkog nasilja u stvarnom okruženju, smatrajući da se to od njih, kao korisnika Fejsbuka koji su učestvovali u određenoj komunikaciji, odnosno do kojih je došao nasilni sadržaj ili nasilna aktivnost, i očekuje.

Isto tako, nasilne aktivnosti na Fejsbuku mogu od nasilnika u virtuelnom okruženju da stvore žrtvu u realnom okruženju, imajući u vidu da žrtva virtuelnog nasilja, u cilju da nasilje prekine, može da posegne

za primjenom fizičkog nasilja u stvarnom okruženju, gdje se uviđa kriminološko-victimološka povezanost stvarnog i virtuelnog okruženja po pitanju ispoljavanja kriminogenih aktivnosti.¹⁶

ZAKLJUČNA RAZMATRANJA

Fejsbuk je koncipiran sa humanom idejom da omogući (kvalitativno i kvantitativno) produbljivanje komunikacije između članova cjelokupne populacije na planeti, te da samu komunikaciju podigne na viši nivo interakcije ljudi, za šta se može reći da je uglavnom i ostvario, pogotovo ukoliko se imaju u vidu koncepti "nove društvenosti" i "mrežnog identiteta" koji se, najčešće, vezuju za komunikaciju preko Fejsbuka po kojoj je ova društvena mreža, uglavnom, i poznata. Međutim, afirmisanjem povezivanja, Fejsbuk je i (nesvjesno) pokazao "mračnu stranu" koja se ogleda u cijelom nizu bezbjednosnih incidenata u okviru ove društvene mreže ili korišćenjem ove društvene mreže ili koji su na neki drugi način povezani sa ovom društvenom mrežom. Štaviše, uslijed mnogobrojnih etioloških, ali i victimoloških faktora, može se reći da je Fejsbuk omogućio ili u izvjesnoj mjeri doprinio i rekonceptualizaciji mnogobrojnih fenomenoloških obrazaca kriminalnog ponašanja i na internetu (savremenih), ali i uopšte (tradicionalnih), imajući u vidu međusobnu povezanost i interakciju realnog i internet okruženja. Naravno, ovu "drugu stranu medalje" Fejsbuka ne treba posmatrati samo kroz ispoljavanje kriminalnih aktivnosti, već i kroz cjelokupan niz drugih bezbjednosnih incidenata, kao i kroz nepodrazumijevano, neželjeno, neprihvatljivo i slično ponašanje internauta na Fejsbuku koji uglavnom imaju konkretizaciju tokom komunikacije. Djelimično uslijed navedenog, tvrdi se da je čak Fejsbuk, težeći da poveže ljudi, doveo do paradoksa, s obzirom na to da ljudi jesu povezani, ali da mnogo manje komuniciraju (što je suština povezivanja između ljudi), odnosno težeći društvenosti doveo je do otuđenosti ljudi, što je takođe surrogat ideje vodilje koncepta Fejsbuka.

Fejsbuk se čini kao paradigm svih negativnosti na mnogobrojnim društvenim mrežama, dok se neke vežu isključivo za njega, uslijed čega se može reći da je, pored toga što je ubjedljivo najpopularnija društvena mreža na internetu, svakako i najomraženija, najogovaranija, najnapadanija... Imajući u vidu kvalitativni i kvantitativni opseg mnogobrojnih nepodrazumijevanih aktivnosti koje se realizuju u Fejsbuk okruženju, pomoću mogućnosti Fejsbuka ili korišćenjem samog Fejsbuka čini se da ovi mnogobrojni napadi svakako nisu neargumentovani, međutim, time se ne bi trebao nipođostavati značaj i uloga Fejsbuka koju on ima u okviru interneta, a pogotovo u okviru internautske populacije, dok se, isto tako, ne bi sam Fejsbuk trebao okrivljivati, bar ne primarno, a pogotovo ne isključivo za kvalitativnu i kvantitativnu ekspanziju, pa i skoncentrisanost, odnosno fokusiranost mnogobrojnih negativnosti ka ovom okruženju.

LITERATURA

- [1] Bodiroga – Vukobrat, N., Martinović, A. (2009). *Izazovi novih tehnologija na radnom mjestu (posebnosti pravnih rješenja)*. Rijeka: Zbornik Pravnog fakulteta;
- [2] Koković, D. (2001). *Nasilje sportske publike*. Banja Luka, Defendologija centar;
- [3] Matijević, M., Miladinović, A., Petričević, V. (2011). *Vršnjačko nasilje na Fejsbuku*, Banja Luka: Panevropski univerzitet Apeiron;
- [4] Miladinović, A. (2013). *Fejsbuk i kriminalitet*. Banja Luka: Internacionalna asocijacija kriminalista;
- [5] Miladinović, A., Petričević, V. (2012). *Kriminogeni aspekt društvenih mreža*. Banja Luka: Visoka škola unutrašnjih poslova;
- [6] Miladinović, A., Petričević, V. (2013). *Elektronsko vršnjačko nasilje*. Banja Luka: Visoka škola unutrašnjih poslova;
- [7] Miladinović, A., Petričević, V., Salamadija, M. (2013). *Govor mržnje na Fejsbuku i na Wikipediji*. Banja Luka: Evropski defendologija centar;

¹⁶ Ilustrativan primjer navedenog je slučaj sedamnaestogodišnjeg Denijela Kanona iz Liverpula koji je, uslijed svađe koju je imao sa školskim drugom preko Fejsbuka, njega sačekao nekoliko dana potom, te se potukao sa njim i odgrizao mu uho. Izričući presudu, sudija je o ovom slučaju rekao da "zbog Fejsbuka ljudi postaju sve agresivniji i nasilniji uslijed čega korisnici u porukama i komentarima često govore stvari koje se ne bi usudili reći drugima u lice, a agresija i svađe sa Fejsbuka i drugih usluga lako se mogu prenijeti u stvarno okruženje." www.tehnologija.me/strasno-odgrizao-mu-uvo-nakon-svade-na-facebook-u.

[8] Turjačanin, M. (2001). *Teze o nasilju*. Banja Luka: Defendologija centar

Internet izvori

- [1] www.bug.hr/vijesti/kad-sef-iste-lozinku/120836.aspx;
- [2] www.informacija.rs/Drustvene-mreze/Illinois-Poslodavcima-zabranjeno-da-traze-lozinke-Facebook-nalog-a-zaposlenih.html;
- [3] www.tehnologija.me/strasno-odgrizao-mu-uvr-nakon-svade-na-facebook-u.

CYBER TERORIZAM - TERORISTIČKE AKTIVNOSTI UPOTREBOM RAČUNARSKIH MREŽA

Siniša Karanović, mr.

Apstrakt: Autor u ovom radu govori o načinima zloupotrebe računarskih mreža od strane terorističkih kolektiviteta ili pojedinaca s obzirom da terorističke organizacije izrazito mnogo zloupotrebljavaju moderne tehnologije. Organizacije tog tipa, moderne tehnologije mnogo koriste za komunikaciju, transfere, a zatim i za informisanje i za svoju propagandu. Finansiranje terorizma je poseban problem. Policije sveta imaju posebna odeljenja koja se bave tom problematikom, odnosno finansiranjem terorizma upotrebom moderne tehnologije. Pojava modernih transfera novca umnogome je olakšala teroristima prikupljanje fondova. Danas postoje milioni načina kako da se izvrši transfer novca, a da to praktično niko ne sazna. Saznati se može jedino ako se slijи velika količina novca.

Ključne reči: cyber, terorizam, organizacija, zloupotreba, kompjuter

UVOD

Aktivnosti međunarodnih terorističkih organizacija ne jenjavaju mada su pojedine zemlje poslednjih godina osnivale antiterotistički savez i postigle odredjene rezultate na tom planu. Terorističke organizacije mogu brzo da se prilagode novim uslovima, poboljšaju svoju taktiku i sposobnosti i iskoriste najnovija naučna i tehnološka dostignuća.

Razvojem računarske tehnologije, terorističke organizacije su dobine novo oružje za ostvarivanje svojih ciljeva. Terorističke grupe koriste računare i Internet za širenje svojih ideja. Oni koriste veb sajtove za regrutovanje novih članova kao i za prikupljanje sredstava. Kriminalci čak pomoću svojih tehničkih veština kradu informacije sa kreditnih kartica, kako bi finansirali terorističke aktivnosti. Vrlo je teško boriti se protiv sajber terorizma, jer novi, napredni alati za sajber kriminal onemogućavaju identifikaciju terorista tokom njihovih napada.

Zloupotreba interneta činjenica je s kojom se danas dnevno susrećemo, a sigurno je najopasnija ona od strane terorista. Oni se internetom ponajprije služe u svrhu širenja terorističkih ideologija i podsticanja na činjenje terorističkog akta te kao platformom za regrutovanje i obučavanje terorista. Internetom se služe u pripremi te tokom terorističkog napada kada im on služi kao komunikaciona infrastruktura.¹⁷

Kako naglašavaju Gabriel Vajman i Konrad Vin u svojoj studiji Pozorište terora jedan od glavnih problema na koje nailazimo suočavajući se sa modernim terorizmom je kako da se branimo.¹⁸

1. POJAM TERORIZMA I CYBER TERORIZMA

Terorizam je višedimenzionalan društveni fenomen, te je u određivanju njegovog pojma potreban multidisciplinarni pristup. Tako se terorizam može posmatrati sa aspekata politike, kriminalistike, kriminologije i krivičnog prava. Sa aspekta kriminalistike, terorizam je vrsta organizovanog kriminaliteta, te je u sprečavanju i suzbijanju terorizma potrebno koristiti naučne ili na praktičnom iskustvu zasnovane metode i sredstva koja su najpogodnija da se terorističko delo otkrije i razjasni, otkriju teroristi i obezbede dokazi, kao i da se spriči izvršenje planiranih terorističkih akata. Kriminološki pristup pojavi terorizma ogleda se u izučavanju pojavnih oblika i uzroka terorizma (etiologija i fenomenologija terorizma), kao i mera za sprečavanje i otklanjanje terorizma, kao oblika kriminaliteta. Međutim, pokušaji kriminoloških pristupa pojavi terorizma, kao društvenoj pojavi, su retki i uglavnom se svode na tretiranje otmica vazduhoplova, kao međunarodnog

¹⁷ K. Antoliš, Internetska forenzika i cyber terorizam, Polic. sigur. Zagreb, godina 19, broj 1, 2010, str. 121.

¹⁸ G. Weimann, and Conrad Winn, The Theater of Terror, Longman Publication, New York, 1994.

terorističkog akta.¹⁹ Krivičnopravne teorije posmatraju terorizam tako što pod terorizam podvode više krivičnih dela koja čine jedno krivično delo terorizma. Prema nekim autorima, potrebno je da postoje politički motivi, dok je prema drugima potrebno da su teroristički akti izvršeni organizovano, ali u svakom slučaju mora da nastupi opšta opasnost za ljude i imovinu. Pored ovih aspekata terorizma, prisutno je sagledavanje terorizma i sa stanovišta drugih nauka, pre svega sociologije, vojnih nauka, i slično. Međutim, konsenzus o pojmu terorizma do sada nije postignut, odnosno različiti su pristupi u određivanju pojma terorizma. Problem definisanja terorizma decenijama predstavlja izvor nesporazuma među državama, zbog čega ni danas nema zajedničkog stava o definiciji terorizma. O ovom problemu vodeći svetski stručnjaci imaju oprečne stavove. Valter Loker (*Walter Laqueur*) dokazuje da je nemoguće definisati terorizam, Aleks Šmid (*Alex P. Schmidt*) navodi da je uzaludno nastojanje da se odredi neka sveobuhvatna definicija terorizma, dok Brus Hofman (*Bruce Hoffman*) ukazuje na karakteristike terorizma koje ga bitno razlikuju od drugih oblika nasilja. Hofman navodi da postoji jedna stvar sa kojom se svi slažu, a to je da je terorizam pežorativan termin. Po njemu, to je reč sa izrazito negativnom konotacijom, koja se obično upotrebljava za neprijatelje ili suparnike, ili za one sa kojima se čovek ne slaže i koje bi, inače, želeo da ignoriše.²⁰ Razvijanjem zajedničkog shvatanja i definisanja terorizma obezbedila bi se potpuna saglasnost i univerzalan odgovor o pojavnom određenju i suštini terorizma. Sadašnje proučavanje terorizma proizilazi iz dva nametnuta dominantna shvatanja terorizma u svetu od strane zapadnih naučnika i oficijelnih stavova, odakle proizilaze i prve definicije terorizma. Otuda dolazi i sistematizacija i analiza svih informacija o terorizmu, uključujući uzroke i faktore koji podstiču širenje terorizma, prvenstveno u međunarodnim osnovama. *Prvo* shvatanje proizilazi iz državnocentričnog modela sveta, na osnovu temeljnih spoljнополитичких определений санкционисаних међународним пoretком и међународним правом. Unutar ovog modela uglavnom se razmišlja o terorizmu i analizira se njegova fenomenologija. *Druge* shvatanje polazi od terorizma kao oblika savremenog ratovanja, surrogata za oružane sukobe, a naročito je dominantno u SAD. U prilog ovom shvatanju je činjenica da vlade mnogih zemalja objavljaju rat terorizmu. Prvenstveno se misli na SAD i Rusku Federaciju, koje su objavile neograničeni rat terorizmu²¹, pri čemu su formirane različite antiterorističke koalicije širokih razmara. Pored ovakvih shvatanja postoje i druga shvatanja koja nastaju negiranjem i eliminisanjem prethodna dva shvatanja.²²

Pri određivanju pojma terorizma, potrebno je poći od etimološkog značenja reči "terorizam", koja je nastala od latinske riječi *terror*, što znači intenzivan strah, ili francuske reči *terreure*, što znači sejanje straha. Zbog toga, mnoge definicije se pretežno, ili isključivo oslanjaju na strah kao definicioni element terorizma. Međutim mnogo je drugih oblika nasilja, pretnji, pa čak i samoiniciranih doživljaja koji mogu izazvati strah, zbog čega terorizam ovakvim definicijama, zasigurno, nije ni precizno definisan, niti je dovoljno razgraničen, ne samo od političkih, već i od niza socijalnih, pa i psiholoških fenomena.²³

Iz tih razloga potrebno je pojmovno razgraničiti teror i terorizam. Pod pojmom terora, u političkom smislu, podrazumeva se akcija nasilja koja se preduzima u političke svrhe - radi zastrašivanja i slamanja otpora onoga prema kome se vrši. Teror predstavlja čvrsto organizovanu vlast, koja strah

¹⁹ Belgijski kriminolog Jecquemin uradio je dve studije u kojima se posebno bavi kriminološkim aspektima otmica vazduhoplova. U prvoj studiji, koju bazira na 140 slučajeva otmica vazduhoplova, ističe da su u velikom broju otmičari mlađi ljudi željni svetskog publiciteta, ili neki odvažni ljudi koji na jeftin način žele doći u izabranu zemlju, ili su to asocijalni tipovi, odnosno kriminalci koji žele izbjeći pravdi za učinjene zločine, ili ljudi koji te akte vrše iz osvete ili mržnje. U drugoj studiji, koju je uradio na bazi 390 registrovanih otmica-vazduhoplova, osvrće se na kriminološke klasifikacije, odnosno tipologije zločinaca i priklanja se osnovnoj deobi društveno normalnih zločinaca na profesionalne i slučajne. U: Z. Šeparović, Kriminologija i socijalna patologija, Narodne novine, Zagreb, 1987. Šire o ovoj tematiki videti studiju američkog psihijatra Hubbard-a, D. G.: The Skyjacker, His Fights of Fantas, New York, 1981.

²⁰ B. Hofman, Unutrašnji terorizam, Narodna knjiga Alfa, Beograd, 2000, str. 26.

²¹ Na vanrednom zasedanju američkog Kongresa 20. septembra 2001. godine, povodom samoubilačkih terorističkih napada na SAD 11. septembra 2001. godine, predsednik Džordž Buš je izjavio: "Naš rat protiv terora/terorizma počinjemo sa Al Kaidom, ali on se neće završiti time. Završće se onda kada svaku terorističku grupu globalnog karaktera, pronademo, zaustavimo i uništimo". President George W. Bush, address to Joint Session of Congress, 20. September 2001. U: Patterns of Global Terrorism 2001. United States of Departments, May 2002.

²² S. Kovačević, Terorizam i Jugoslavija, Arkade print, Beograd, 1992, str. 12 – 13.

²³ M. Šikan, Terorizam – aktuelni i mogući oblici, Banja Luka, 2006, str. 66.

pretvara u nerazdvojni deo svakodnevnog života najširih slojeva građana. Osnovne karakteristike terora su: ograničavanje zakonitosti u materijalnom i proceduralnom smislu, neminovna arbitarnost, iracionalnost sa stanovišta onih koji misle da njime postižu opštekoristan cilj i izazivanje širokog sraha i opšte dezorientisanosti. Iz ovoga proizilazi da se terorom označava metod vladanja. Međutim, pojmom terora označava se i metod borbe protiv vlasti, a na isti način se koristi i pojам terorizma. Tako se za teror vlasti kaže da je „teror odozgo“, „proces terora“, „režim terora“ ili „državni terorizam“, dok se za teror protiv vlasti govori da je „individualni teror“, „teror odozdo“, „agitacioni teror“ ili jednostavno „terorizam“. ²⁴

Da bi se mogao definisati pojам terorizma, potrebno je odrediti one elemente terorizma koji se konstantno pojavljuju u terorističkim aktima. Holandski naučnici Aleks Šmid (*Alex P. Schmidt*) i Albert Džongman (*Albert J. Jongman*) izvršili su kvantitativnu analizu 109 definicija terorizma i došli do zaključka da se u njima konstantno pojavljuje 22 elementa, po redu učestalosti u pomenutom uzorku, sa procentualnom zastupljenošću svakog elementa u analiziranim definicijama.²⁵ Na osnovu ova 22 zajednička elementa, koja je pronašao empirijskom analizom, Šmid je razvio definiciju terorizma koja sadrži 13 od tih elemenata, uopšteno smatrajući pod terorizmom metod borbe, u kojoj žrtve služe kao simboličke mete.²⁶

Ujedinjene nacije nemaju jedinstvenu definiciju terorizma, ali u brojnim rezolucijama, konvencijama, deklaracijama i protokolima određeni akti i ponašanja grupa ili pojedinaca označavaju se kao terorizam. Tako, pod terorizmom UN podrazumevaju akte lišavanja života ili ranjavanja, ili akte uništavanja ili oštećenja imovine civila ili vlada, bez jasne dozvole određene vlade, od strane pojedinca ili grupe ljudi koji samostalno djeluju, ili vlada koje deluju iz vlastitih pobuda ili verovanja, da bi postigle neki politički cilj. Shodno tome, u Rezoluciji Saveta bezbednosti br. 1373, koja je izglasana 28.9.2001. godine, navodi se da međunarodni terorizam predstavlja izazov svim državama i ukupnom čovečanstvu, jer se terorizmom svuda ugrožava dostojanstvo i sigurnost ljudi, podriva društveni i privredni razvoj svih država i u svetskim razmerama potkopava stabilnost i blagostanje. U novembru 2004. godine UN su označile terorizam kao svaki akt: „koji uključuje ubistva ili povređivanje civila ili ne - boraca, u svrhu zastrašivanja populacije, vlada ili međunarodnih organizacija, sa ciljem da nešto učine ili ne učine, što proizilazi iz tog akta“.²⁷

Evropska unija je definisala terorističke akte kao namerne radnje koje mogu opasno oštetiti zemlju ili međunarodnu organizaciju, zakonom označene kao protivpravne radnje, a počinjene sa ciljem ozbiljnog uznemiravanja naroda, prisiljavanja vlade ili međunarodne organizacije da počini ili se uzdrži od činjenja i s siljem ozbiljne destabilizacije ili uništavanja osnovnih političkih, ustavnih, ekonomskih ili socijalnih struktura zemlje ili međunarodne organizacije (napad na ljudski život, napad na fizički integritet lica, uzimanje talaca, otimanje aviona, broda ili drugih transportnih sredstava, itd.).

U zbirci *Federalnih propisa SAD* terorizam se definiše kao protivpravna upotreba prinude ili sile protiv ljudi ili imovine, da bi se zastrašila ili prisilila vlada, civilno stanovništvo ili jedan njegov deo, kako bi se postigli određeni politički ili socijalni ciljevi. Prema ovoj definiciji, teroristički akt označava aktivnost koja: 1) uključuje akt opasan po ljudski život, koji krši krivične zakone SAD ili

²⁴ V. Dimitrijević, Strahovlada, Dosije, Beograd, 1997, str. 121.

²⁵ Elementi koji se pojavljuju su: upotreba sile ili nasilja (83,5%), političko nasilje (65,0%), izazivanje straha ili užasa (51,0%), pretinja (47,0%), psihološki efekat i očekivane reakcije (41,5%), razlikovanje žrtve i šire mete napada (37,5%), ciljano, planirano i organizovano delovanje (32,0%), metod borbe, strategija, taktika (30,5%), anomalije kršenja prihvaćenih pravila, odsustvo humanitarnih razloga (30,0%), ucena, prinuda i navođenje na poslušnost (28,0%), želja za publicitetom (21,5%), samovolja, bezličnost, nasumičnost, odsustvo diskriminacije (21,0%), žrtve civili, neborci, nestrelici, lica bez veze sa samom stvaru (17,0%), zastrašivanje (17,0%), naglašena nevinost žrtava (15,5%), izvršilac, grupa, pokret ili organizacija (14,0%), simbolička priroda, pokazivanje drugima (13,5%), nepredvidivost, neočekivanost pojave nasilja (9,0%), tajnost i prikrivenost (9,0%), ponavljanje niza ili kampanje nasilja (7,0%), kriminalni, zločinački karakter (6,0%) i zahtevi postavljeni trećim stranama (4,0%).

²⁶ B. Hofman, Unutrašnji terorizam, Narodna knjiga Alfa, Beograd, 2000. str. 35; Videti šire u: S. Kovačević, Terorizam i Jugoslavija, Arkade print, Beograd, 1992. g. str. 35; Uporedi: A. Savić, Od tradicionalnog ka postmodernom terorizmu, Bezbednost, 5/04, str. 656.

²⁷ M. Šikan, Terorizam – aktuelni i mogući oblici, Banja Luka, 2006, str. 70.

bilo koje od saveznih država, ili koji bi bio krivično delo ako bi bio počinjen pod jurisdikcijom SAD ili bilo koje savezne države i 2) čini se u nameri da se: a) zastraši ili zlostavlja civilno stanovništvo, b) utiče na politiku vlade putem zastrašivanja ili prinude ili v) utiče na ponašanje vlade putem atentata i otmice.²⁸

Krivični zakon Francuske definiše akte koji se odnose na terorizam kao akte pojedinaca ili grupe koje koriste zastrašivanje ili teror da poremete javni red.

U *pravnim propisima Velike Britanije* (Akt o prevenciji terorizma iz 1989. Akt o Severnoj Irskoj iz 1996. I Akt o terorizmu iz 2000.) terorizam se definiše kao korišćenje nasilja u političkoj borbi, kao i u cilju unošenja straha u javnost.²⁹

U *Krivičnom zakonu Jugoslavije*, krivično delo terorizma sastoji se u izazivanju eksplozije, požara ili preduzimanju druge opšteopasne radnje kojom može da se stvori osećaj lične nesigurnosti kod građana, a u nameri ugrožavanja ustavom utvrđenog državnog i društvenog uređenja ili bezbednosti SRJ.³⁰

Krivični zakon Bosne i Hercegovine u članu 201. Pod terorizmom podrazumeva činjenje terorističkog čina sa ciljem ozbiljnog zastrašivanja stanovništva ili prisiljavanja organa vlasti Bosne i Hercegovine, vlada druge zemlje ili međunarodne organizacije, da što izvrši ili ne izvrši, ili s ciljem ozbiljne destabilizacije ili uništavanja osnovnih političkih, ustavnih, privrednih ili društvenih struktura Bosne i Hercegovine, druge zemlje ili međunarodne organizacije.³¹

Krivični zakon Republike Srpske pod terorizmom podrazumeva činjenje terorističkog akta ciljem ozbiljnog zastrašivanja građana ili prisiljavanja organa vlasti u Republici Srpskoj da što ucini ili neucini ili s ciljem ozbiljnog narušavanja ili uništavanja osnovnih političkih, ustavnih, ekonomskih ili društvenih organizacionih jedinica u Republici Srpskoj.³²

Odeljenje za unutrašnje poslove SAD (*State Department USA*) definiše terorizam na malo drugačiji način, podrazumevajući pod terorizmom unapred smišljeno, politički motivisano nasilje počinjeno protiv civilnih ciljeva od strane subnacionalnih grupa ili tajnih agenata, obično sa pokušajem da utiču na širu javnost. Međunarodni terorizam je terorizam koji uključuje građane ili teritorije više od jedne države.³³

Federalni istražni biro SAD (*Federal Bureau of investigation*) definiše terorizam kao nezakonitu upotrebu sile ili nasilja protiv imovine i lica, sa zastrašivanjem i primoravanjem vlade, civilne populacije ili nekog njihovog segmenta sa ciljem ostvarivanja političkih ili socijalnih ciljeva.³⁴

Američko Ministarstvo odbrane koristi definiciju terorizma po kojoj je terorizam nezakonita upotreba nasilja ili pretnja silom ili nasiljem uperenim protiv pojedinca ili nečije imovine da bi se izvršila prisila ili zastrašivanje vlada ili društva, a u mnogim slučajevima da bi se postigao neki opšti politički, verski ili ideološki cilj.³⁵

Obaveštajna agencija Ministarstva odbrane SAD terorizam definiše kao unapred planirano političko nasilje koje se vrši protiv neborbenih ciljeva, a od strane subnacionalnih grupa ili tajnih državnih agenata, obično sa ciljem da se utiče na neki auditorijum.³⁶

Priručnik američke vojske za borbu protiv terorizma definiše terorizam kao sračunatu upotrebu nasilja i pretnje nasiljem da bi se postigli ciljevi koji su političke, religijske ili ideološke prirode, koja se čini putem zastrašivanja, prinude ili širenja straha.

Kao što smo u ovom delu rada i videli, o pojmu terorizma i uopšte o njegovom pojmovnom određenju se može pisati veom široko. Postoji mnoštvo različitih definicija terorizma, ali se na ovom

²⁸ *Ibidem*.

²⁹ *Ibidem*.

³⁰ Član 125. KZJ – U: B. Čeđović, Krivično pravo – poseban deo, Srpsko udruženje za krivično pravo, Beograd, 2002, str. 20.

³¹ M. Babić, Lj. Filipović, I. Marković, Z. Rajić, Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini, Savjet/Vijeće Evrope i Evropska komisija, Sarajevo, 2005, str. 659.

³² Krivični zakon Republike Srpske („Službeni glasnik Republike Srpske“, broj 49, od 25. Juna 2003. godine)

³³ M. Šikman, *op. cit.*

³⁴ R. Dž. Vajt, *Terorizam*, Aleksandria Press, Beograd, 2004, str. 15.

³⁵ *Ibidem*.

³⁶ M. Milošević, *Odbrana od terorizma*, Svet knjige, Beograd, 2005, str. 26.

mestu mi nećemo baviti njima, s obzirom da smo naveli definicije koje su zakonske, što je u svakom slučaju jedino obavezujuće za organe gonjenja i sprečavanja vršenja terorističkih krivičnih dela.

Sajber terorizam obično podrazumeva napade na kompjuterske sisteme ili mreže iza kojih stoje neki politički ciljevi. Često su namenjeni za zastrašivanje vlade ili građana neke države ili izazivanje ekonomskog gubitka. Pod sajber terorizmom podrazumevaju se i fizički napadi i uništavanje važnih kompjuterskih sistema i infrastrukture.

Postoje tri osnovna načina na koja teroristi mogu da koriste računare za koordinisanje, planiranje i izvršavanje svojih aktivnosti u ostvarivanju svojih ciljeva:

Korišćenje računara kao alata. Terorističke grupe koriste internet za propagiranje svojih ideja preko web sajtova i prikupljanje finansijskih sredstava, obično u vidu dobrotvornih priloga, kao i prikupljanje i razmenu obaveštajnih podataka,

Teroristi mogu da koriste računare u planiranju i organizovanju svojih programa rada. Oni u računarima drže svoje finansijske knjige, terorističke planove, potencijalne ciljeve, dnevnike prismotre, planove napada...

Cyber-teroristi mogu da koriste računare za neovlašćen pristup vladinim i privatnim informacionim sistemima u cilju izazivanja ozbiljnih, čak i katastrofalnih posledica.

Cyber - terorizam se odnosi na smisljene, politički motivisane napade na kompjuterske sisteme i programe, kao i na podatke, kojima treba da se izazovu nasilje, strah i gubici kod civilnih meta.

Cyber - terorizam predstavlja teroristički akt, ali koji se u odnosu na „klasičan“ akt odvija na nešto drugačijem prostoru - računarskim sistemima, računarskim i komunikacijskim mrežama. Ovde se teroristi svojom veštinom, znanjem i tehnikom obračunavaju sa zaštitnim sistemima potencijalnih žrtvi -takođe kompjuterskim sistemima, u cilju nanošenja određenog oštećenja, uništenja pa čak i izazivanja velikog broja ljudskih žrtava. Ranije se pretpostavljalo da ovaj vid terorizma ne može naneti neke veće štete a naročito ne ljudske žrtve, i zato mu se nije pridavao poseban značaj, tj. nije se shvatao ozbilnjom pretnjom. Međutim praksa je takav način razmišljanja demantovala. On nije bio samo velika pretnja za stvaranje kolapsa u raznim segmentima društva, već je takođe predstavljao veliku mogućnost u izazivanju katastrofalnih posledica po ljudske živote.

Uprkos značajnim ulaganjima u tehnologiju i infrastrukturu, sajber terorizam predstavlja jednu od najvećih izazova u borbi protiv terorizma. Svakog dana Internet i mnogi računari izloženi su raznim napadima. Prema istraživačkoj studiji (anketi) objavljenoj od strane Istraživačkog Centra za Kompjuterski Kriminal za 2002. godinu, u 90% slučaja od ukupnog korišćenja računarskih sistema, došlo je do izvesnog narušavanja sistema. U još jednoj detaljnijoj studiji od strane *CIO Online*, 92 % kompanija bilo je podvrgnuto napadima u poslednjih 12 meseci. I pored zabrinjavajućih statističkih podataka, stručnjaci za bezbednost upozoravaju na dalje povećanje sofisticiranosti pretnji i napada na kompjuterske sisteme.

Cyber terorizam je veoma atraktivan metod u odnosu na „klasičan ili tradicionalan“ terorizam. Njegove prednosti se ogledaju kroz sledeće:

Jeftiniji je od metoda tradicionalnog terorizma (kod sajber terorizma, teroristima je potreban samo kompjuter i običan telefonski priključak;

Ne moraju kupovati razna naoružanja kao što su bombe ili eksplozivi, jer mogu naneti isto tako razorne posledice i preko kompjutera..);

Cyber terorizam pruža veliku mogućnost anonimnosti (veoma je teško otkriti pa čak i pratiti sajber teroriste; teroristi mogu vršiti operacije sa bilo koje pozicije u svetu);

Veliki broj mogućih potencijalnih meta (teroristi mogu napasti sisteme vlade, individualne sisteme, javne institucije, sisteme privatnih avio kompanija, sisteme zdravstva,...);

Cyber terorizam pruža mogućnost vršenja operacije daljinskim upravljanjem;

Cyber terorizam ima veće mogućnosti nanošenja većih ljudskih žrtava od tradicionalnog terorizma.

Teroristi nisu svi istovremeno i u punoj meri počeli da koriste internet prostor. Na primer, sada najpoznatija teroristička organizacija, Al Kaeda, je relativno kasno „otkrila“ internet, a počeli su ga intenzivno koristiti tek nakon što su proterani iz Afganistana. Razlog tome je verovatno taj što u Afganistanu tada, za vreme talibanske strahovlade nije bilo ni struje, a kamoli interneta. Seobom Al Kaede u Irak sve više se koristi internet pa se uskoro pojavljuju razni filmovi u kojima bombaši-samoubice svedoče o svojoj veri ili propagandni filmovi u kojima se poziva na sveti rat protiv Amerike. Vrhunac je dostignut kada je na internetu objavljen video na kome se vidi odrubljivanje glave Amerikanca Nika Berga (Nick Berg). Na početku je Al Qaeda slala materijale arapskoj tv stanici Al

Džazira (al Jazeera), ali su kasnije počeli izrađivati sopstvene internet stranice. Dve stranice koje su bile sinonim za Al Kaidu na internetu su Alnedu (Alnedu.com) i Džihad (Jehad.net).³⁷

Analize pokazuju da su se terorističke mreže na internetu udvostručile svake pojedine godine od 2003. do danas, pa je zbog toga britanska služba MI5 povećala svoje ljudstvo sa 1800 u 2001 na preko 3500 u 2008. godini. Brojne organizacije su ušle u internet prostor (cyberspace) i stvorile svoje intenet stranice. One uključuju Hamas, Libanski Hezbolah (Stranka Boga), egipatski Al-Gama'a al Islamiya, Narodni front za oslobođenje Palestine (PLFP), Islamski džihad za oslobođenje Palestine, Tupak-Amaru Perua (MRTA), i „Obasjana putanja”, pokret Kahane (Kahane Lives), ETA pokret Baskije, Iranska republikanska partija (IRA), „Vrhovna istina”, Kolumbijska nacionalna oslobođilačka armija, Tamilski tigrovi, Oružane revolucionarne snage Kolumbije, Narodni demokratski oslobođilački front Turske, Radnička partija Kurda, Zapatistička nacionalna oslobođilačka armija, japanska Crvena armija i islamski pokret Uzbekistana. Pojedine terorističke organizacije, kao na primer Mudžahedini Irana (PMOI-Mujahedin-e Khalq) su imale samo verziju na Farsiju, tako da nismo uspeli da ih unesemo u ovu analizu. Neke druge, kao na primer Al Kaida prvo nisu imale prevedenu internet stranicu, pa su ga preveli samo na francuski jezik, ali su ubrzo nestali usled poznatih pritisaka. Zbog svega navedenog, internet stranice ove organizacije nisu razmatrane. Oslobođilačka vojska Preševa, Bujanovača i Medveđe nema svoj nezavisnu internet stranicu već se informacije o pomenutoj organizaciji mogu naći na stranicama drugih terorističkih organizacija koje deluju u okviru ovog prostora. I na ovaj način možemo videti koje organizacije deluju nezavisno, a koje imaju logistiku „sa strane”, odnosno koje su samo deo neke veće organizacije.³⁸

2. KOMUNIKACIJA TERORISTIČKIH GRUPA PUTEM REČUNARSKIH MREŽA

Zna se da teroristi maksimalno koriste pogodnosti računarskih i komunikacijskih sistema npr. Interneta, mogu neometano da ostvaruju kontakte sa velikih udaljenosti i između više grupa. To im veoma olakšava planiranje i izvođenje terorističkih operacija. Velika prednost se ogleda i u tome što se sada može ostvarivati komunikacija i među manjim grupama, koje inače ne ostvaruju kontakte iz bezbednosnih razloga, pa će samim tim procenat uspešnosti planirane operacije biti veći. Bitno je i napomenuti da su sve učestalije i pojave komunikacija i saradnji između različitih terorističkih organizacija. Čak šta više, u budućnosti se predviđa povećanje njihove međusobne saradnje, tako da će se problem iskorenjavanja terorizma dodatno usložiti. Više neće biti samo vertikalnih korelacija na nivo matične terorističke organizacije, već će se postepeno oformljavati i horizontalne korelacije između različitih terorističkih grupacija.³⁹ Značajna prednost pri korišćenju računarskih i komunikacijskih sistema ogleda se u planiranju i koordinaciji terorističkih operacija. Za razliku od „klasičnog“ terorizma, gde je planiranje bilo otežano, zbog mogućnosti otkrivanja poverljivih informacija, što bi naravno dovelo u pitanje realizaciju čitave operacije pa i samu sudbinu pojedinih razotkrivenih članova organizacije, planiranje se izvodilo u strogoj tajnosti među veoma malom grupom ljudi. Ali korišćenjem kompjuterskih resursa, čitava procedura planiranja je u mnogome olakšana bez dodatnog ugrožavanja i narušavanja faktora tajnosti. Tako je npr. poslednja poruka Mohamed Atte (jednog od ključnih članova i koordinatora prilikom napada 11.09. u SAD) ostaloj osamnaestorici članova bila: „Semestar počinje za tri nedelje. Primili smo 19 odobrenih potvrda za studiranje na pravnom fakultetu, fakultetu urbanog planiranja, fakultetu fine umetnosti i fakultetu inžinjerije (mašinskom ili elektrotehničkom)“. Međutim, poruka koja je bila vezana za navedene fakultete predstavljala je u stvari šifru za potencijalne mete napada, tj svaki od navedenih fakulteta je predstavljao jednu od potencijalnih meta napada. Iz ovog primera se može zaključiti da je veoma teško ući u trag određenim informacijama koje se razmenjuju među teroristima putem mreže računarskih i komunikacijskih sistema, jer su izuzetno dobro skrivene i šifrovane i naočigled su krajnje bezazlene ali u stvarnosti među svojim redovima nose sasvim drugačiju poruku.

³⁷ M. Zirojević-Fatić, Zloupotreba interneta u terorističke svrhe, MP 3, 2011, str. 427.

³⁸ Ibidem.

³⁹ G. Weimann-Special Report 116, How Modern Terrorism Uses the Internet, march 2004.

U cilju bezbednosti i nemogućnosti otkrivanja od strane protivterorističkog subjekta, čitava komunikacija kao i planiranje se izvodi šifrirano tj. putem enkriptovanih⁴⁰ poruka. Na taj način se sprečava neautorizovano čitanje ili menjanje podataka. Stepen zaštite se određuje algoritmom ili ključem. Postoje dve vrste sistema za kriptovanje: *simetrični* i *asimetrični* sistem.

Za *simetrični* sistem koristi se isti ključ (tajni ključ) za kriptovanje i za dekriptovanje, a za *asimetrični* sistem jedan ključ (javni) za kriptovanje poruka a drugi (tajni) za dekriptovanje.

Inače komunikacija među teroristima se najčešće ostvaruje preko određenih (*chat*) programa putem Interneta, preko mnogih porno-sajtova (gde su poruke obično upakovane u razne i teško uočljive fajlove), korišćenjem metode steganografije⁴¹ „dead drops“ metodom i još mnogih drugih načina.

Steganografija je način pakovanja određene poruke u cilju tajne ili skrivene komunikacije. Određena informacija se najčešće „upakuje“ u neki drugaćiji oblik podatka, kao npr u vidu određene slike, fotografije, tako da postaje veoma teško prepoznatljiva pa je u tom slučaju proces njenog razotkrivanja od strane PTS znatno otežan. *Dead drops* predstavlja još jednu od tehnika zaštite poruka koje se razmenjuju između terorista. Poruka se postavlja na server, korišćenjem npr. *ftp* protokola, nakon čega posle izvesnog vremena primalac preuzima navedenu poruku. Moguće je koristiti čak i neke neobjavljene servere kao *host* i držati tako poruku samo trenutno na serveru, dok je primalac ne preuzme. Ovo je inače moderna elektronska verzija „dead drops“ tehnike, koju su koristili obaveštajni oficiri dugi niz godina. Ako bi se postavili u ulogu protivterorističkog subjekta, možemo slobodno reći da su im ruke skoro vezane po pitanju ove oblasti. Veoma je teško ući u trag nekoj kriptovanoj poruci, a ako se to i uspe, veoma je teško dešifrovati vešto kriptovane poruke. O određivanju pozicije i lokacije terorističke grupe da i ne govorimo. To je skoro i nemoguće. Iz svega navedenog možemo zaključiti da su računarsko-komunikacijske mreže veoma pogodno tle za teroriste i njihove operacije.

3. PRIKUPLJANJE INFORMACIJA SA INTERNET MREŽE

Korišćenje Internet mreže od strane terorističkih organizacija nije vršeno samo u cilju stvaranja komunikacija između grupa, podgrupa pa i različitih organizacija, već su teroristi pronašli još mnogo pogodnosti koje im ta mreža pruža. Svima nama je poznato da Internet mreža predstavlja jednu globalnu i svetsku tvorevinu gde se prožimaju informacije različitih sadržaja. Upravo u tome se ogleda još jedna velika pogodnost terorista, prikupljanje različitih korisnih informacija, koje im u mnogome olakšavaju proces u odnosu na prikupljanje informacija kod „klasičnog ili tradicionalnog“ terorizma. Više se ne moraju izlagati javnosti u onoj meri, koliko je to bilo potrebno ranije, kako bi se izvršio određeni zadatak u fazi pripreme. Sada je to znatno jednostavnije a ujedno i bezbednije. Jednostavnim pristupom Internetu, u ulozi više manje anonimnog korisnika, teroristi mogu doći do njima bitnih podataka, fotografija, slika, planova i šema određenih objekata, pojedinih podataka o određenim ličnostima, kao i mnogih drugih informacija o potencijalnoj meti napada. Međutim treba napomenuti da se sav taj proces prikupljanja određenih informacija ne može osuđivati, jer sam po sebi ne predstavlja krivično ili nezakonito delo. U toliko je rad i zadatak PTS i u ovom slučaju znatno iskomplikovan i otežan. U ovom slučaju ne preostaje PTS ništa drugo neko neprestano vršiti monitoring i praćenje.

Kako bi se moglo oceniti da li je neko od trenutnih korisnika Interneta terorista ili ne, na osnovu njegovog prikupljanja informacija sa Internet mreže, konstruisani su mnogi sistemi praćenja i detektovanja o kojima će biti reči u nekom od sledećih poglavљa. U cilju bolje zaštite ponuđenih informacija na mreži, u sve većoj meri se na sajtovima oformljava sistem prijave i autorizacije, koji u neku ruku predstavljaju zaštitu ili preventivnu meru od zloupotrebe, tj. korišćenja određenih informacija u kriminalne ili destruktivne svrhe.

⁴⁰ Enkripcija – način zaštite poruka od neželjenog čitanja.

⁴¹ Steganografija – način tajnog pisanja.

4. PREZENTACIJE TERORISTIČKIH ORGANIZACIJA NA INTERNETU

Poznato je da veliku ulogu u terorističkim aktivnostima imaju mediji i propaganda. Putem istih teroristi su uspevali da izazovu veliki strah i paniku u okolnom društvu i to sve u cilju pojačavanja pritiska na određenu vlast protiv koje je inače sve i usmereno. Kako su se protiv-teroristički subjekti počeli uspešno suprotstavljati teroristima putem ne objavljivanja pojedinih slučajeva i pokušaja terorističkih napada, tako su teroristi ipak pronašli način i mogućnost da se ta situacija predupredi u njihovu korist. (Poznati su pojedini slučajevi, gde su teroristi čak i odustajali od planiranih napada ustanovivši da neće biti medijski podržani). Tako je i prezentovanje terorističkih organizacija jedna od značajnijih i javnosti dosta poznatih delatnosti terorista. Ovde teroristi koriste globalnu mrežu Internet u cilju objavljivanja pojedinih delova kao što su:

- razlozi borbe (najčešće se prikazuje kao borba za oslobođanje od velikog zla i ugnjetavanja);
- motivi i ciljevi te organizacije;
- podstrek drugih subjekata da se priključe toj borbi;
- propagiranje uspešnih terorističkih napada u cilju izazivanja straha i panike kod civilnog stanovništva i ujedno podizanje morala kod svojih članova;
- istorijat organizacije.

Danas postoji veoma veliki broj sajtova raznih terorističkih organizacija, koji su dostupni čitavoj svetskoj populaciji. Inače cilj tih sajtova je obelodanjivanje svrhe postojanja tih terorističkih organizacija, objavljivanje njihovih aktivnosti, motiva i mogućnosti prijema novih članova a naročito vršenje uticaja na menjanje svesti kod "neutralnog" sveta, tj. da se opravdaju njihovi postupci i da se protumače kao oslobođilački a ne kao teroristički. Redovni sadržaji sajtova čine informacije koje se odnose na istoriju organizacije i biografije lidera, osnivača, heroja ili značajnih ličnosti organizacije, informacije o političkim i ideološkim ciljevima i vesti. Većina sajtova sadrži detaljan pregled istorijskih događaja značajnih za organizaciju, političko i društveno određenje, selektivan opis značajnih aktivnosti u prošlosti i ciljeve organizacije. Nacionalne organizacije (separatističke ili teritorijalne) obično prikazuju opšte mape područja u sukobu. Na primer, na sajtu „Oslobodilačke Vojske Kosova“ prikazana je mapa četiri albanske enklave tokom Ottomanskog carstva iz 1878. godine, na sajtu Hamasa nalazi se mapa Palestine, sajt „Tamilskih Tigrova“ sadrži mapu Šri Lanke.⁴² Među najposećenijim terorističkim sajtovima je sajt HAMAS-a⁴³, koji sadrži linkove na arapskom i engleskom jeziku. Na sajtu su objavljeni izvori Hamasa, karakteristike te organizacije kao i pojedini podaci o njihovom vojnem krilu (*Izz al-Din al-Kassam Brigade*).

Na sajtovima se uglavnom ne prikazuju kriminalne i amoralne aktivnosti organizacije, ali se zato navode „uzvišeni“ ciljevi (npr. „Oslobodenje“ i sl.). Iako gotovo sve organizacije imaju debele dosijee o krvoprolaćima, nikada na sajtu ne pominju takve aktivnosti. Izuzetak su Hezbollah i Hamas. Hezbollah pokazuje valjane statističke podatke vezane za svoje akcije („dnevne operacije“). Na posebnoj strani daje obaveštenja o broju mrtvih „mučenika“, ubijenih „izraelskih neprijatelja“ i „kolaboracionista“.

Sajt Hamasa sadrži dugačke diskusije o vojnim operacijama, dok „OVK“ detaljno opisuje svoj nastanak i prikazuje filmove o vežbama vojnika, prikazuju mapu velike Albanije u cilju psihološkog efekta na stanovništvo koje se nalazi na tim prostorima.

Kako je navedeno, cilj ovih sajtova je i regrutovanje novih članova. Ali i pored dugogodišnjeg praćenja aktivnosti mnogih terorističkih sajtova, nije poznato koliki je faktor uspešnosti regrutovanja preko tih sajtova. Predpostavlja se da je itekako na zavidnom nivou.

Redovan sadržaj internet stranica terorističkih organizacija predstavljaju informacije koje obuhvataju istoriju organizacije i biografije lidera, osnivača, heroja ili značajnih ličnosti organizacije, informacije o političkim i ideološkim ciljevima i vesti. Većina internet strana daje detaljan pregled istorijskih događaja bitnih za organizaciju, političko i društveno određenje, selektivan opis značajnijih aktivnosti u prošlosti i

⁴² M. Zirojević, Terorističke organizacije i Internet, Vojno Delo 1/2004.

⁴³ www.palestine-info.org

ciljeve. Nacionalne organizacije (separatističke ili teritorijalne) daju opšte mape područja u sukobu. Na primer, internet strana Oslobođilačke vojska Kosova predstavlja mapu četiri albanske eklave tokom Ottomanskog carstva iz 1878, internet prezentacija Hamasa pokazuje mapu Palestine, dok internet strana Tamilskih tigrova pokazuje mapu Šri Lanke.⁴⁴

5. FINANSIRANJE TERORISTA PUTEM RAČUNARSKIH SISTEMA

Iako je značajna razlika između sajber-terorizma i kompjuterskog kriminala, oni su direktno povezani u pogledu pojedinih delatnosti. Pojam kriminala se najčešće vezuje za rukovodeće organe ili vlast, tj. dobija izvesnu podršku od pojedinih grupa sa vlasti, dok se nasuprot tome terorizam izričito suprotstavlja postojećoj vlasti i njenim principima. Poznato je i to, da se kriminal najčešće odvija u cilju sticanja određene materijalne dobiti, dok je terorizam pojam koji je podstreknut određenom političkom ideologijom. Da bi se pojedine terorističke organizacije uspešno razvijale i suprotstavljale, neophodna im je finansijska podrška. Kada se dotaknemo oblasti finansiranja terorista, ubrzo ćemo doći do zaključka da je ovo tačka „raskrsnica“ gde se kriminalci i teroristi susreću. Ovo je tačka njihovog zajedničkog delovanja. Kriminalnim putem se dolazi do prikupljanja određenih materijalnih dobiti, koje se koriste u mnoge svrhe (za pribavljanje naoružanja, raznih neophodnih sredstava i aparata ...)

Finansiranje pojedinih terorističkih organizacija realizuje se na više načina :

- putem nezakonitih kriminalnih aktivnosti u cilju materijalne dobiti (švercom, prodaja oružja, droge, belog roblja, komp.kriminal,...);
- formiranjem pojedinih organizacija ili firmi u cilju pranja novca;
- preko mnogih lažnih humanitarnih organizacija;
- sponzorisanja od tzv. „treće“ strane i još mnogih drugih načina.
- Konkretno vezano sa sajber terorizam, finansiranje je moguće na već navedene načine:
- preko sajtova lažnih humanitarnih organizacija;
- preko kompjuterskog kriminala (krađom preko slabije zaštićenih sistema određenih banaka);
- lažnom prodajom određenih artikala;
- korišćenjem lažnih kreditnih kartica za kupoprodaju;
- pranjem novca.

Jedan od najvećih aduta protivterorističkog subjekta, jeste otkrivanje i presecanje terorističkih finansijskih tokova čime se dovodi u pitanje njihovo delovanje. Bez finansijske podrške, terorističke organizacije nisu u stanju da ozbiljnije realizuju svoje planove, pa se samim tim dovodi i u pitanje njihovo dalje postojanje. Možda je ovo i jedan od najboljih mogućih načina pomoću kojeg se može doći do skoro da nedodirljivih sajber terorista. Praćenjem njihovih finansijskih tokova može se ugrubo odrediti destinacija ili čak otkriti mogući pojedini saučesnici pa čak i u zavisnosti od sume koja se prenosi navedenim tokovima može se ugrubo odrediti stepen njihove spremnosti i ozbiljnosti. Poznato je da Hezbolah podiže svoj novac u SAD-u preko sajta Asocijacije *Podrška Islamskičkog Otpora*. Takođe je oformljena i fondacija „*Sveta zemlja*“ za oslobađanje i razvoj, gde posetioci sajta mogu dati svoje donacije i dobrovoljne priloge. Međutim, navedeni sajt je 2002. godine ugašen od strane vlade SAD-a. Mnogi sajтовi ovakvih sadržaja bili su ugašeni ali su teroristi i tada prikazali svoju impresivnu upornost i veština, neprekidnim formiranjem novih sajtova i to van domena vlade SAD-a. Postavlja se pitanje, koliko gašenje sličnih terorističkih sajtova predstavlja efikasnu borbu protiv terorista?

⁴⁴ M. Zirojević-Fatić, Zloupotreba interneta u terorističke svrhe, MP 3, 2011, str. 429.

6. NEPOSREDNA BORBA USMERENA KA PTS PUTEM RAČUNASKIH SISTEMA

Neposredna borba usmerena ka protivterorističkim snagama (PTS) je takođe jedna od značajnih mogućnosti terorista putem računarskih i komunikacijskih mreža. Teroristi mogu putem navedenih mreža vršiti ne samo određene napade već i praćenje delatnosti PTS, stvaranje određenih diverzija njihovim sistemima i još mnogo drugih delatnosti. U koliko uspeju da premoste sve odbrambene sisteme PTS, i uđu u njihov sistem, mogućnosti terorista postaju neograničene. Od brisanja već postojećih podataka vezanih za teroriste preko menjanja njihovih sadržaja do možda neprimetnog špijuniranja bez posebnih diverzija, kako bi odgnali svaku sumnju da imaju pristup navedenim podacima. Iako se zna da je pristup navedenim podacima veoma zaštićen i selektivan, ipak se ne može isključiti mogućnost njihove zloupotrebe. Teroristi mogu unazaditi PTS za nekoliko koraka, ukoliko uspeju u navedenim pokušajima. Svesni toga, oni izuzetno puno pažnje posvećuju tom pitanju, detaljno analizirajući sve moguće načine kojima se njihovi ciljevi mogu realizovati. Kako je država definisana određenom hijerarhijskom strukturi, tako i kod terorističkih organizacija postoje velike sličnosti. Teroristi su takođe organizovani hijerarhijski po principu „piramide“. U tom sistemu značajnu ulogu imaju njihove obaveštajne službe, koje se nikako ne smeju potcenjivati. Osnovni zadatak obaveštajnih službi terorista je da:

- neprekidno prate aktivnosti PTS
- otkriju planove PTS
- vrše otkrivanja podataka kojima raspolaže PTS o pojedinim terorističkim organizacijama
- vrše otkrivanje raspoloživih snaga i mogućnosti PTS-a

Na osnovu efikasnosti obaveštajne službe i verodostojnosti njihovih prikupljenih podataka, celokupno planiranje operacija terorističke organizacije biće znatno efikasnije. Na osnovu tih podataka, teroristi će operaciju usmeriti prema snagama PTS koje su najslabije, prema žrtvi koja je nebranjena ili slabo zaštićena, s namerom da postignu najveću efikasnost sa najmanjim mogućim rizikom po organizaciju i njene članove. Jedan od najvećih problema u oblasti korišćenja računara predstavljaju destruktivni programi koje pišu i distribuiraju razni antisocijalni i destruktivni korisnici sa namerom da naprave štetu što većem broju korisnika. Najveću opasnost za sigurnost korisnika računarskih sistema predstavlja instaliranje i korišćenje softvera i hardvera koji su nabavljeni od nesigurnog izvora. Oni mogu sadržati takozvanu zlonamernu logiku (*malicious logic*) koja je namerno uključena ili ubaćena radi narušavanja rada računarskih sistema. Za otkrivanje i uklanjanje destruktivnih programa postoji veći broj programa nazvani jednim imenom *antivirusni*. Osim konstatovanja potencijalne destruktivnosti, ovi programi imaju i mogućnost eliminisanja destrukcije pre njenog aktiviranja. Međutim, kako se novi destruktivni programi svakodnevno generišu potrebno je antivirusne programe stalno usavršavati (*updating*) novim podacima i novim verzijama programa. Antivirusni programi mogu da budu aktivirani radi provere nekog memorijskog medijuma na zaraženost, ili se mogu aktivirati po uključenju računara, kada služe kao štit koji trenutno registruje ubacivanje destruktivnog programa u računarski sistem.

U narednom dijelu rada ćemo detaljnije govoriti o savremenim računarskim mrežama, informacionim sistemima i sistemima zaštite, a nakon toga o višeslojnoj arhitekturi sistema zaštite savremenih računarskih mreža te u samoj razradi teme o kriptografskim metodama zaštite u informacionim sistemima.

ZAKLJUČAK

Trenutno u svetu Internet predstavlja najrasprostranjeniju mrežu, sa brojem korisnika koji se izražava u stotinama miliona i, u skladu s tim, sa ogromnom količinom informacija koje se kroz mrežu prenose. Najčešći oblici korišćenja Interneta su pretraživanje naučnih, zabavnih, kulturnih, sportskih, poslovnih informacija, odnosno razmena istih u čemu učestvuju odgovarajuće organizacije i pojedinci koji koriste Internet u službene i privatne svrhe.

Kao i u drugim aspektima života, pored konstruktivnih postoje i destruktivne snage koje koriste nesavršenosti, bilo Interneta, bilo ljudi koji ga koriste, radi obavljanja protivpravnih aktivnosti koje ugrožavaju organizacije i pojedince, korisnike Interneta. Pored konstantnog razvoja Interneta tj. uporedo sa razvojem i implementacijom računarskih mreža Interenet tipa, i razvojem destruktivnih pojava vezanih za Internet razvijaju se i različiti mehanizmi zaštite specijalizovani za odbranu od pojedinih vrsta napada.

Opšte je poznato te potvrđeno analizama američkih stručnjaka, da se u oko 95% slučajeva terorističke organizacije same obraćaju medijima kako bi preuzele odgovornost za pojedini teroristički napad. Osnovna strategija od 60-ih godina 20. veka baskijske terorističke organizacije ETA, je da se pokretanje akcija redovno najavljuje, a da se po izvršenju terorističog akta javno preuzme odgovornost. Česta je pojava kada manje i neafirmisane terorističke organizacije ili politički pokreti lažno preuzimaju odgovornost za pojedini napad kako bi ih se pojavili u javnosti i stekli „reputaciju“.

LITERATURA

- [1] A. Savić, Od tradicionalnog ka postmodernom terorizmu, Bezbednost, 5/04.
- [2] B. Čeđović, Krivično pravo – poseban deo, Srpsko udruženje za krivično pravo, Beograd, 2002.
- [3] B. Hofman, Unutrašnji terorizam, Narodna knjiga Alfa, Beograd, 2000.
- [4] G. Weimann, W. Conrad Winn The Theater of Terror, Longman Publication, New York, 1994.
- [5] G. Weimann-Special Report 116, How Modern Terrorism Uses the Internet, march 2004.
- [6] K. Antoliš, Internetska forenzika i čber terorizam, Polic. sigur. Zagreb, godina 19, broj 1, 2010.
- [7] Krivični zakon Republike Srpske („Službeni glasnik Republike Srpske“, broj 49, od 25. Juna 2003. godine)
- [8] M. Babić, Lj. Filipović, I. Marković, Z. Rajić, Komentari krivičnih/kaznenih zakona u Bosni i Hercegovini, Savjet/Vijeće Evrope i Evropska komisija, Sarajevo, 2005.
- [9] M. Milošević, Obrana od terorizma, Svet knjige, Beograd, 2005.
- [10] M. Šikan, Terorizam – aktuelni i mogući oblici, Banja Luka, 2006.
- [11] M. Zirojević, Terorističke organizacije i Internet, Vojno Delo 1/2004.
- [12] M. Zirojević-Fatić, Zloupotreba interneta u terorističke svrhe, MP 3, 2011.
- [13] Patterns of Global Terrorism 2001. United States of Departments, May 2002.
- [14] R. Dž. Vajt, Terorizam, Aleksandria Press, Beograd, 2004.
- [15] S. Kovačević, Terorizam i Jugoslavija, Arkade print, Beograd, 1992.
- [16] V. Dimitrijević, Strahovlada, Dosije, Beograd, 1997.
- [17] Z. Šeparović, Kriminologija i socijalna patologija, Narodne novine, Zagreb, 1987. Šire o ovoj tematiki videti studiju američkog psihijatra Hubbard, D. G.: The Skyjacker, His Fights of Fantasz, New York, 1981.
- [18] www.palestine-info.org

КОНЦЕПТ САЈБЕР ОРУЖЈА У РАЧУНАРСКИМ И ТЕЛЕКОМУНИКАЦИОНИМ СИСТЕМИМА

МСц Небојша Иваниш дипл.инж.инф.

ИТ Вештац, Београд, Србија, nebojsaivanis@sezampro.rs

Апстракт: Концепт рата у последњој деценији се дубоко променио због масовног увођења технологија у свакодневни живот. То је отворило простор за такозвано „сајбер ратовање“. Операције сајбер напада и сајбер шпијунаже су у највећој мери политички мотивисане а њени планери су најумнији експерти из више различитих области. У сајбер рату нема елемената физичке сile или ни јавних политичких циљева. Због наведеног се не може рећи да „постоји“ рат између Америке и Кине, Ирана и Израела, Русије против Естоније и Грузије. Оваква врста рата се не уклапа у дефиницију конвенционалног рата јер нема елемената сile нити је јасно изражених политичких циљева, али у бити постоји „електронско бојно поље“ такозвано „сајбер поље“.

Кључне речи: сајбер рат, сајбер простор, сајбер оружје, сајбер ћелија, сајбер војник, малвер, код, хакер.

УВОД

Последице сајбер рата из виртуелног простора се могу пренети у стваран простор и те последице могу бити катастрофалне за неку суверену земљу као на пример да одређени простор државе остане без воде, возови се сударају или искачу из шина, банке губе податке или новац, авиони падају са неба, улицама шетају руље бесних организованих људи, људи умиру због неадекватне медицинске неге, а све се дешава док идентитет нападача остаје покрiven мистеријом. Због наведених тешких последица сајбер ратовања јавља се потреба бржег решавања превентивне заштите нашег сајбер простора. То се најефикасније постиже развојем нових сајбер јединица заштите земље – сајбер ћелија. Ретке су земље које нису увиделе значај сајбер ратовања, из тог разлога многе улажу значајна средства за превентивну заштиту свог сајбер простора. Експерт за безбедност у америчкој влади по имену Ричард А. Кларк је дефинисао у својој књизи маја 2010. године шта је сајбер рат: „Сајбер рат је акција националне државне безбедности ради упада у компјутер/компјутере или мреже другог народа за потребе прикупљања корисних информација, наношења штете или прекида рада делимично или у потпуности оних система који су кључ вођења једне суверене земље.“

Ако знамо да су физички простор, копно, море и ваздух четири домена где је могуће водити рат, онда се сајбер простор посматра као пети домен ратовања. Заменик америчког секретара одбране Вилијам Ј. Лин, каже да је Пентагон званично признао да постоји сајбер простор као нови домен у ратовању али и да још не постоји потпuna свест код великог броја држава сиром планете о могућим злоупотребама, нарушувању и злоупотреби истог. Са подацима у сајбер простору се оперише, они путују, а на многим местима се са њима тргује. Сајбер домен је препун софтверских замака.

Историјска анегдота указује на прве кораке сајбер шпијунаже и сајбер напада. Верује се да је сајбер напад и сајбер шпијунажу „измислио“ Роналд Реган у време када није постојао интернет. На једном самиту у Отави 1981. Реган је од Митерана добио обавештење да је француска тајна служба регрутовала високо рангираних КГБ официра по имену Владимир који је доставио четири хиљаде копија тајних совјетских докумената. Јасно се видело да је Совјетски Савез очајнички покушавао да се дочепа западне технологије за развој гасовода на релацији Уренгој – Сургут - Чељабинск. На предлог Регановог саветника Гаса Веиса, Реган је одлучио да дозволи Совјетима да сазнају оно што им је потребно. Кључна компонента, је био софтвер који контролише рад вентила на гасоводу. Совјетски агенти су од канадске компаније укради електронске нацрте и шеме, а да нису били свесни да ће у њихов гасовод ући „тројански коњ“ у којем се крије „логичка бомба“. Неколико месеци гасовод је функционисао као сат, а онда је софтвер „полудео“, активирала се логичка бомба и променила рад вентила који су почели да подижу притисак гаса у гасоводу. Амерички војни сателити су 4. јуна 1982. године открили експлозију у Сибиру снаге мање атомске бомбе. Експлозија је довела ситуацију до усијања јер су Совјети подигли своју војну

готовост до општег ванредног нуклеарног стања. Само Вајс и Реган су знала шта се заправо дододило.

Руски извори, међутим, оспоравају ову верзију приче. Пензионисани генерал КГБ-а Василиј Пчелинцево рекао је да је експлозија била много мањег интензитета и да се догодила на сасвим другом месту. Рекавши да је узрокована клизиштем носача цеви због влажног земљишта у сибирској тундри. Људских жртава није било, а штета је поправљена у року од једног дана, изјавио је генерал КГБ-а.

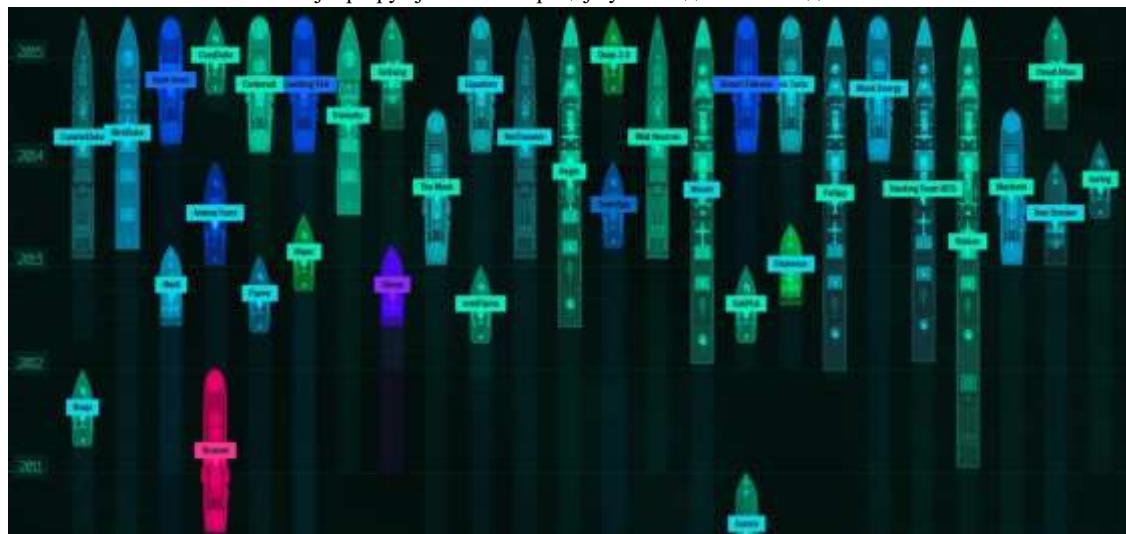
1. УТИЦАЈ САЈБЕР ОРУЖЈА НА САЈБЕР ПРОСТОР

Сајбер простор је „виртуелни“ простор у којем постоје и њиме се крећу дигитални и аналогни подаци. Те податке могу да користе државне институције, војска, полиција, грађани, једне или више земаља. Да би упростили апстрактне чињенице о сајбер простору узмимо на пример интернет као сајбер простор, али можемо узети и интранет мрежу неке компаније или државне институције и то може бити сајбер простор.

Предходно поменуте чињенице нас обавезују да повећамо свест у сектору безбедности земље од могућих претњи у сајбер простору. Такве операције могу имати офанзивну, дефанзивну и обавештајну улогу, а све у сврху предности у односу на конвенционалне нападе. За разлику од конвенционалног напада, сајбер напад може бити спроведен у мирнодопском режиму на веома подмукли начин. То доводи до потребе да се размотре све могуће претње које захтевају висок степен припремности. Владе широм света су забринуте због нивоа безбедности својих инфраструктура које користе дигиталне технологије и промовишу темеље квалификованих сајбер јединица како би се омогућиле акције у новом домену.

Како пример се може навести да је Амерички председник Барак Обама у 2009. години прогласио да су Америчке дигиталне инфраструктуре уствари "стратешко национално благо", а само годину дана касније је морао да одобри формирање нове сајбер команде (US Cyber Com.) са примарним задатком да одбрани америчку војну мрежу и да спроведе пун спектар војних акција у сајбер простору. Тиме су се омогућиле акције у свим доменима заштите државних ресурса. САД нису једина нација која улаже у стварање способности заштите сајбер простора, сајбер ратовања и сајбер операција. Кина, Израел и Русија управо раде све као и САД. За предходно поменутим ништа не заостају ни Северна Кореја и Иран. Њихово присуство у сајбер простору последњих година бележи знатна побољшања. Званични извори наводе да је најмање 140 земаља на планети у процесу развоја сајбер оружја и деловања у сајбер простору. Забележен је велики пораст сајбер операција у сајбер простору у последњих 5 година. Процењује се да се приближно хиљаду напада сваког дана води против владиних система широм планете. Поставља се питање: Колико таквих напада ће у будућности бити реализовано успешно, а колико њих ће бити осуђени? Тренутно нико не може да да одговор на ово питања.

Слика 1. – Списак познатих сајбер оружја нове генерације у последњих пет година



Извор: <http://www.kaspersky.com/>

Сајбер оружје није „неко специјално недокучиво“ средство већ је то софтвер који је писан у једном или више програмских језика по одређеној методологији потребној за деловање у сајбер простору.

Сајбер оружје – софтвер, је предефинисан (написан - програмиран) и има улогу да „увреди“ непријатеља у сајбер простору.

Али, упркос честој употреби термина „сајбер оружје“, данас не постоји формална и правна дефиниција у терминологији на нивоу државе и институција (у току прослододишњих зимских месеци аутор овог текста незванично сазнај да је дат нацрт закона о Сајбер безбедности у Скупштину Републике Србије на даљу процедура због изгласавања). Узимамо примера ради, речник војних термина, који садржи мноштво дефиниција за разноразна оружја и оруђа али не садржи посебну дефиницију за сајбер оружје. Ни међународно право не дефинише која је улога, за шта је намењен и шта је уопште једно сајбер оружје.

Може се слободно рећи, да је недостатак правно регулативне дефиниције за сајбер оружје, озбиљан проблем. Недостатак правне дефиниције чини не могућност разлике између улоге сајбер оружја и његовог правилног коришћења. Исто тако немогуће је проценити правну и политичку одговорност агресора и реалног нивоа опасности направљеног у контексту сајбер ратовања.

2. ОДАБИР САЈБЕР ОРУЖЈА ЗА ЕФИКАСНОСТ У ВОЋЕЊУ САЈБЕР РАТА?

Примарни фактори успеха употребе сајбер оружја су ефикасност и смањење трошкова који се користе у технологијама за конвенционални рат.

Случај „Стакнет“ малвера (у даљем тексту без знака навода) је први прави пример сајбер оружја. Тај малвер је писан/програмиран у С програмском језику. Стакнет је показао сву своју силину и утицај на критичне инфраструктуре једне суверене земље. Употреба сајбер оружја не прави буку као конвенционално оружје, па се каже да је то оружје „не чујно“. Нападач – агресор – сајбер ратник може извршити напад и „побећи“, а да се физички није појавио на лицу места, тачније да никада није био физички присутан на тој локацији, да је без звучног и визуелног ефекта извршио напад и да у је тренутку напада боравио заштићен у некој држави хиљаду километара далеко од места где се одиграо напад - злочин. То је права моћ сајбер оружја која истражитеље, дигиталне форензичаре и инспекторе ставља на веома тежак задатак откривања и доказивања починиоца злочина. Отежава истрагу и немогућност доношења цињеничног стања и изношења доказа пред извршне државне органе нападнуте земље.

Најјаче светске војне силе попут Америке, Кине, Русије итд. су услед великог броја сајбер операција и напада немоћне у проналажењу починиоца. Нападачи – сајбер ратници у великом броју случајева раде под покрићем своје владе што представља бег од санкција у међународној заједници, јер анонимна природа кривичног дела омогућава избегавање санкција и спречавање да оштећена страна одобри војну офанзиву или надокнади штету.

Слика 2. – Илустрација тренутних сајбер напада широм планете



Извор: <http://www.kaspersky.com/>

Фазе развоја и припреме сајбер оружја из војне перспективе у далекој мери су лакше за скривање од „радозналих очију“. Лакше је открити изградњу конвенционалног оружја као нпр. ракете, беспилотне летелице, борбеног авиона итд. у односу на развој сајбер оружја. Објашњење је логично, сајбер оружје може развијати једна или више особа тајно. На пример, сајбер оружје се може развијати у некој војној бази или у неком бункеру ко зна где, локација је не битна али исто тако може се програмирати у кафићу преко пута вашег стола док пијете кафу или ручате са породицом. Поновићемо опет, сајбер оружје је еквивалент софтверу и развој сајбер оружја је еквивалент развоју софтвера. Значи, особа која развија сајбер оружје може да пише неку линију кода у програмском окружењу за било који програмски језик, а да ви све време гледате у монитор и пратите шта та особа ради и да не видите ништа сумњиво што би указивало на стварање сајбер оружја. Та особа може развијати само пар метода које ништа не значе док се не обједине/развију/генеришу у готов софтвер тј. у том случају малвер који има улогу сајбер оружја. Употреба сајбер оружја је комплементарна са конвенционалним војним ударима и може бити:

- подршка операцији за уништавање инфраструктуре непријатељске одбране или
- убачен малвер у непријатељске технолошке системе.

Предности, могућности и циљеви сајбер ратовања су веома атрактивни за технолошко, финансијски и војно индустријски „мале“ земље. Упркос томе што су им средстава за развој конвенционалног наоружања у војној индустрији мала и не могу да парирају најјачим војним силама ипак имају могућност да улагањима у развој сајбер оружја буду приближно еквивалентне најјачим војним силама на планети.

Koји су циљеви за сајбер ратовања?

Спектар могућности сајбер оружја је веома широк. Чињенично гледано, сајбер оружје би могло погодити сваку критичну инфраструктуру и витални систем једне земље, као што су:

- индустриски контролери, елементи од посебног значаја који надгледају рад постројења за производњу енергије и користе се за водовод, хидро или електро централе,
- системи за надгледање (мониторинг) територије,
- државне и приватне болнице, пример је Немачка која улаже велика новчана средства у „даљинску медицину“. Преко 3G телефонске мреже се прати пацијентово стање и дежурни лекар или робот рачунар врше информисање пацијента потребама за узимање терапије и о стању пацијента. Стање пацијента прате сензори који контролишу притисак, откуцаје срца итд,
- седнице Владе које се одржавају преко линка када министри нису у могућности да физички буду присутни, користе се спољни путеви у комуникацији који никада не могу 100% бити безбедни, они су само обезбеђени спољни линкови,
- комуникационе мреже државних и приватних провајдера,
- системи одбране,
- војни и цивилни ваздушни саобраћај и контрола ваздушног простора,
- финансијски и банкарски системи.

Због предходно наведеног, можемо рећи да је сајбер домен ипак присутан у стварном свету. У стварном свету имамо уговоре, агенције за праћење и надзор. Такве агенције врше контролу за нуклеарно, биолошко и хемијско оружје, па зашто не би радиле контролу и за сајбер оружје?

Овакво питање је иссрпно и наглашава потребу за оснивање „Међународне сајбер регулаторне комисије“. Пре свега, потребно је да се обезбеди валидна дефиниција о концепту шта је сајбер оружје.

Занимљиву дефиницију за сајбер оружје обезбедио је италијански адвокат Стефано Меле, иначе експерт за сајбер ратовање, у својој публикацији „Ciberweaphons – Правни и стратешки аспекти“: „Сајбер оружје је исто што и уређај или било који скуп рачунарских инструкција дизајнираних да незаконито оштети рачунар или телекомуникациони систем који има природу критичне инфраструктуре, да искористи његове информације, податке или програме садржане у њему или у његовим везама, или да би се олакшао прекид, потпуно или делimično, или преиначење свог рада.“

Поред предходно поменуте дефиниције имамо још једну дефиницију за сајбер оружје коју најчешће користе стручњаци за сајбер безбедност и она гласи овако: „*Уређај, апарат или сваки скуп рачунарских инструкција дизајнираних да уверди особу у сајбер простору.*“ Обе дефиниције су комплетне и правно ваљано исказане да квалификују суштину сајбер оружја.

Софтвери за сајбер шпијунажу се могу користити да изврше напад на специфичне циљеве једноставним учитавањем одговарајућег дела кода - модула – метода функције у коду који је развијен за напада. Тако развијен софтвер представља модуларну структуру која омогућава употребу малвара у офанзивно дефанзивне сврхе. Постоји пример као већ изолован случај, за предходно наведене чињенице, а то је малвер „Дуку“ (у даљем тексту без знака навода). Малвер Дуку из извора Викилиksа настао је под покровitelјством безбедносне агенције америчке државе, али се званично и дан данас води под непознатим пореклом. Циљ сајбер шпијунаже је прикупљање података, осматрање и даљинско управљање. Малвер Дуку користи исту платформу којом је писан малвер Стукнет. Та платформа се назива „Tilded платформа“ са могућношћу отвореног IoC (inversion of control) фајла. Фајл IoC има могућност да се генерише узимајући команде у току самог рада и пунећи базу која има могућност промене структуре у зависности од информација које је пуне кроз IoC фајл.

Предходно наведено, се може видети из следећег представљеног метода који је део фајла IoC, а то је:

```
public class ServerFacade {  
    public <K, V> V respondToRequest(K request) {  
        if (businessLayer.validateRequest(request)) {  
            DAO.getData(request);  
            return Aspect.convertData(request);  
        }  
        return null;  
    }  
}  
  
public class ServerFacade {  
    public <K, V> V respondToRequest(K request, DAO dao) {  
        return dao.getData(request);  
    }  
}
```

Ово је приказ основног нацрта у Јава програмском језику и даје пример кода израђеног у методологији IoC фаја. У ServerFacade класи имамо објекат DAO (назив објекта из наведеног примера) који је део базе. Све претпоставке могу бити важне у неком тренутку. Имамо методу са наредбом if која користи две промењиве K,V које пуне DAO објекат. Израда оваквог метода има за циљ улогу инверзије контроле објекта.

3. TILLED ПЛАТФОРМА

А шта је то „Tilded платформа“ (у даљем тексту без знака навода)? Tilded платформа је специјално дизајнирана „посуда“ (у даљем тексту без знака навода) за неопажен пренос малвера на неком електронском медијуму до жељене локације – рачунара, дигиталног уређаја или мреже. Циљ нападача је да инфильтрира посуду са малвером (малвер може бити дизајниран – писан тј. програмиран за било коју врсту напада или шпијунаже) на неки чврсти диск или преносни медиј. Особа која ће бити курир не треба да зна да у систем уноси малвер. Чим особа унесе малвер у изоловану мрежу, тиме се посао курира и Tilded платформ - посуде завршава. Потом ће се у систему малвер временски активирати на одређени датум.

Дефиниција - Tilded платформу је комуникатор за злонамерни софтвер. Tilded платформа је развијена крајем 2007. године и прошла је значајане трансформације у 2010. години како би се спречило да је нови антивирусни производи открију. Према исказима стручњака за сајбер безбедност и безбедност информационих система може се предпоставити колики је био број циљаних напада у последњих неколико година због могућности праћења неких верзија Tilded платформа. Најзначајнији тројански малвери који су користили Tilded платформу су Стукнет и Дуку. Верује се да постоје и други малвери или шпијунски софтвери који користе Tilded

платформу или да још нису идентификовани. У јануару 2012. године у извештају антивирусне компанија „Касперски Лаб“ наведена је повећана употреба Tilded платформе на интернету.

4. СТУДИЈА СЛУЧАЈА – СТУКНЕТ

Стукнет малвер је откријен 2009. години када је инфицирао индустриске контроле у специфичним системима распоређеним у иранским инфраструктурима који имају намене критичног управљања гасовода, термо, хидро и нуклеарних електрана. Крајњи циљ Стукнeta је био да саботира инфраструктуру критичне намене на начин да репрограмира логичке контролере (ПЛЦС), а потом би контролери наставили рад по жељи нападача. Намера је била да се повећају извршне способности свих механичких уређаја у систему. Учесталост у раду им се тако повећава до максимума и како би били доведени у стање физичког отказа. Тиме би се нанела велика материјална штета. Операција сајбер напада је тако развијена да доведе до отказа система. Стукнет се састоји од више комада злонамерних програма са мноштвом различитих компоненти и функционалности које укључују:

- нулти-дан,
- windows рооткит,
- ПЛЦ рооткит,
- анти технику за антивирусну семантичку претрагу,
- сложен процес ињекције за напад,
- рутине за мрежну инфекцију,
- процес мутирања,
- peer-to-peer исправке,
- временски окидачи и
- командне и контролне интерфејсе.

Употребом различитих техника у програмирању Стакнeta довело је до закључка да није једина мета био Иран и нуклеарна постројења, већ је имао улогу да настави своје ширење и на земље политички и дипломатски близске Ирану. Даље инфекције би се сматрале као „колатерална штета“ изазвана нестручном употребом иранског тајног оружја, што би за циљ навело њихове савезнике на прекид дипломатских односа. Из предходно наведеног се поставља питање да ли су аутори сајбер оружја били у стању да контролишу ширење малвера Стакнет?

Према изјавама многих америчких војних званичника, није могуће сто постотно имати сигурност у управљању сајбер оружјем јер постоји могућност да се поред мете заразе и друге мете које нису биле циљ напада. Разлог лежи у томе да када се сајбер оружје убаци у систем преко Тилдед платформе, нападачи – сајбер војници само чекају реакцију, а оштећена страна може у великој мери да утиче својим поступцима на даље прогресивно инфицирање система у сајбер простору. У таквим ситуацијама кључну улогу носе методологије заустављања, изоловања инфицираних клијената и отклањање инфекције, а све у зависности од методологије припреме напада од стране нападача. Када су ирански стручњаци за безбедност извршили дигиталну форензику и направили скицу претпоставки методологије нападача видели су да постојале разлике у коду сајбер оружја које су указивале на могућност дифузије модула и временског окидача за процес мутирања. Тиме је сајбер оружје постало комплексно сложен софтвер са могућношћу да мења своје понашање, да мења структуру и да сваки модул или метод може имати разарајући утицај.

Борба против оваквог сајбер оружја, из предходно наведених чињеница, делује веома сложена и тешка, а неки би рекли скоро немогућа.

Дејство Стакнeta је нанело велику материјалну штету. Наравно да постоји могућност одбране и то у више фаза:

- провера програмског кода сваког постојећег софтвера који делује - функционише у систему (пример је лабораторија за софтвер у ТОЦ-у која је технички оснапсобљена и има могућност да стручно одговори овим захтевима, ту је и ЦКИСИП и J6),
- потпуна изолација критичних инфраструктурних система,
- системе свести на одвојене независне делове ако могућности дозвољавају (разлог је лакша изолација инфицираног подручја),

- направити паралелну копију цelog система или кључних делова (ако се главни систем инфицира, изолује се целокупним искључењем, а могуће је активирати копију и наставити са радом),
- контрола уноса информација путем преносних медија у систем (подићи на највиши ниво),
- едукација о безбедносним мерама и повећању безбедносне свести запослених,
- мониторинг система које спроводе особе, никако мониторинг уз помоћ софтвера,
- обавештајни рад у прикупљању информација о потенцијалним нападачима,
- развијање сајбер оружја на нивоу државе због могућег одговора или првог напада и
- свакодневна контрола система од стране дигиталних форензичара како би се закрпиле рупе.

5. УТИЦАЈ НА САЈБЕР ПРОСТОР

Ширење злонамерног софтвера – сајбер оружја у сајбер простору може довести до уништавања критичне инфраструктуре па чак и до губитка људских живота. Сајбер напад може изазвати сличну штету као што изазива конвенционални напад са озбиљним утицајем на грађане. Постоје „колатералне штете“ изазване неконтролисаном дифузијом сајбер оружја. У сајбер нападу примарни циљеви наношења штете су електронски системи:

- националне одбране - систем одбране једне земље могу се контролисати, самим тим и конвенционално наоружање, па тако на пример, постоји могућност да се покрене ракета против своје државе или других народа,
- здравствених установа и болница - пацијети у болницама и домовима здравља могу бити изложени сајбер шпијунажи (прикупљање информација) или сајбер нападу,
- контроле критичних објеката - сајбер напад би могао угрозити систем управљања хемијског постројења или нуклеарне електране (мењање процеса рада и производње),
- водовод - вода је битан ресурс за становништво. Прекид снабдевања водом може оставити велике површине територије без воде. Измена у систему контроле водоводне мреже може омогућити рањивост на системе за филтрирање воде и тако изазвати између осталога и тројање воде (повећано присуство хлора итд.) на индиректан начин,
- потпуно аутоматизоване контроле превоза цивилног и војног копненог, воденог и ваздушног саобраћаја - управљање ваздушним саобраћајем. Размислите о ефекату напада на систем контроле железничког саобраћаја око пропуштања и мимоилажења два воза и могућ судар,
- електро мреже - овај циљ представља виталан систем једне земље. Електро мреже представљају привилеговану мету за сајбер нападе, а њихова одбрана мора бити основа у свакој сајбер стратегији одбране. Нападом је могуће прекинути снабдевање електричном енергијом, због чега је нарушен укупан блок активности нације и нанета је велика материјална штета,
- банака и финансија - су од критичног значаја за нацију и напад на њих може да изазове озбиљне проблеме. Сајбер напад може изазвати финансијски колапс једне нације. Сценариј је забринавајући, јер знамо да је економија ступ стабилности сваке државе.

Слика 3. – Утицај малвера „Carbanak“



Извор: <http://www.kaspersky.com/>

Као пример у илустрацији 3. је наведен малвер „Carbanak“ (у даљем тексту без знака навода) који прикупља информације из банкарског и финансијског сектора. Писан је за пробој у Windows оперативне системе. Оперативно обавештаним активностима сајбер ратници су прикупили информације да је у тим секторима најзаступљенији Windows оперативни систем. Сам Windows има велики број пропушта у заштити неовлашћеног уласка на back doors (задња врата), у хакерским круговима се зна да за ту активност није потребна нека претерана способност хакеришања.

Генерал Џон С. Каскиано, бивши директор ваздухопловства, надзора и извиђања Владе САД, потврдио је концепт непредвидивости сајбер оружја, изјављујући следеће: „ми никада нећемо имати 100% гаранција да ће сајбер напад радiti као што смо испланирали.“ То значи да би сајбер оружје у екстремним случајевима могло да нападне извор, па би такав напад са последицама добио термин „бумеранг ефекат“. Присуство сајбер оружја у сајбер простору може отворити могућност обрнутог инжењеринга у односу на изворни код. Стране владе, злонамерни појединачи, сајбер терористи, хакактивиси и криминалци могу да детектује, изолују и анализирају сајбер оружје, изврше пројектовање сајбер оружја и пусте га у сајбер простор. Цурење информација о постојању сајбер оружја је значајан фактор који може подстаки активности противника у сајбер рату. Други фактор који излаже унутрашњу безбедност озбиљном ризику у случају сајбер напада је недостатак свести грађана о сајбер ратовању и одговарајући поступци одговора у случају напада. Већина људи у потпуности игнорише термин сајбер ратовање.

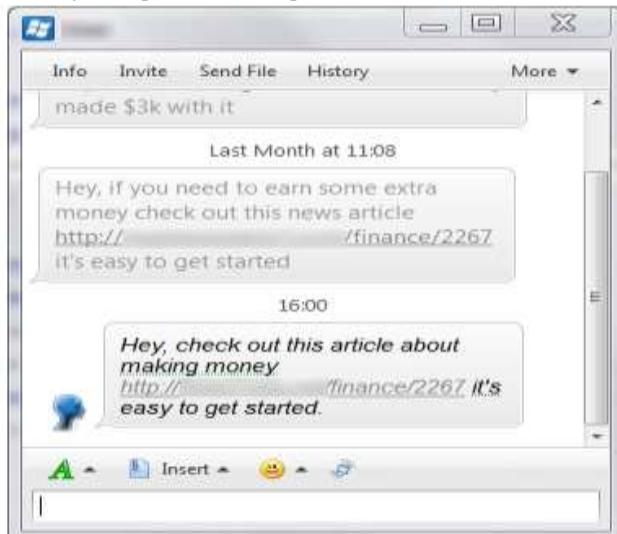
6. НОВА УЛОГА ХАКЕРА И РАЂАЊЕ НОВОГ ТРЖИШТА – ЦРНИ МАРКЕТ

Битан, можда и најбитнији елемент у развоју сајбер оружја је спознаја његове рањивости, тј грешке у програмском коду. Други битан елемент је рањивост софтвера или система који према коме се планира напад.

Ове чињенице су познате широм планете под термином - рањивост нултог дана. То је фактор који утиче на ефикасност али и омогућава да циљате одређене рупе у софтверу или инфраструктури. Владе земаља и одређени бизнис кругови су изненада открили значај у откривању овакве врсте грешке - бага у софтверима који имају широке намене и које грађани користе у свакодневном животу. То отворило могућност креирања новог тржишта за трговину „драгоценом робом – грешке у софтверском коду“ које је добило термин – црни market.

Рањивост софтверског кода је суштина рада сваког сајбер војника - хакера. На црним маркетима грешке – багови у софтверском коду имају велику вредност, па се могу купити/продати по ценама и до неколико милиона евра/долара.

Слика 4. – Пример комуникације хакера и особе за врбовање



Извор: <http://windows.microsoft.com/en-us/messenger/messenger-to-skype>

Илустрација 4. приказује класичну „злоупотребу“ обичног корисника од стране сајбер нападача – хакера због тестирање софтвера. Циљ хакера је да прикупи корисне информација о баговима у коду неког софвера бесплатно или за веома малу новчану надокнаду, а те информације ће потом продати на црном тржишту за пуно новца. Хакер користи легални софтвер за комуникацију као што је приказано на илустрацији 4. и ствара слику о безазлености ситуације, нуди лаку новчану зараду коју многи не одбијају и обмањује обичног корисника у његовом даљем коришћењу сајбер простора - интернета, а да тога корисник није ни свестан.

Фигура хакера се у потпуности променила у очима произвођача софтвера. У прошлости, хакери су углавном радили за њихово задовољство, личне фрустрације и због потреба за мерењем личних вештине не мешајући се у послове државе. Данас су хакери кључна фигура у сајбер свету, јер своје вештине могу уновчiti откривајући грешке у коду па их потом продају, уценjuју друга лица или злоупотребљавају на црним маркетима. Када је откривена рањивост софтверског кода, владе земаља су увеле у пословање куповине/продаје софтера брокерске куће ради чувања тајне о грешкама у коду али и да споје понуду и потрежњу. Тада су и хакери затражили свој део „колача“. Тржиште црних маркета као и њени актери су обавијени велом мистерије. Велики број стручњака за безбедност пропагира увођење правне регулативе и контроле за преговоре при куповини/продаји софтверских грешака у коду. Тренутно се продаја/куповина на подручјима црних маркета одвија са „опасним“ и „тајанственим“ особама које су спремне на разноразне опасне последице како би дошли до жељених грешака. Други проблем је немогућност да се оствари увид у реалне токове новца на црном маркету, избегавање плаћања пореза и других законских норми.

Слика 5. – Пример интернет огласа за приступ сајбер школи



A School for Cybercrime: How to Become a Black Hat

January 16, 2012, 8:46 pm. [Fabio Assolini](#)

[Twitter](#) 0 | [Facebook](#) 0 | [Google+](#) 6 | [Email](#) 1024 | [Print](#)

To help beginners interested in a life of cybercrime, some Brazilian bad guys started to offer paid courses. Others went even further, creating a Cybercrime school to sell the necessary skills to anyone who fancies a life of computer crime but lacks the technical know-how. [Read Full Article](#)

Извор: <http://thehackernews.com/>

Од пре пар година уназад су све учесалији огласи на интернету о приступу сајбер школама широм света. Понуда је лака и добра зарада за младе (велика незапосленост приморава младу особу са добрым знањем на овакав корак) и могућност дамлада особа добије шансу за такозваним „престижом“ у друшту и заједници ако постане део црних шешира или било које друге хакерске организације. Само је потребно да приступи хакерској школи, као што приказује илустрација 5. Најјачи ефекат оглас постиже у Бразилу, Индији, Кини али и у земљама источне европе. Разлог је једноставан – велика незапосленост и проблеми социјалне и финансијске природе.

Владе земаља које улажу у сајбер безбедност су заинтересоване за хакере – сајбер војнике које могу користити за своје сајбер операције. Кина, Русија, САД али и Северна Кореја и Иран, јавно су показали велико интересовање за „куповину“ хакера. У многим случајевима владе су најавиле ангажовање најбољих хакера за стварање нових сајбер јединица, као на пример начелник нове хакер сајбер јединице Генералштаба САД-а Кеит Б. Александер током последњег скупа „Дефкон“ конференција хакерских достигнућа, затражио је хакере за помоћ обезбеђивања сајбер простора САД-а.

7. ШПИЈУНСКИ ФАЈЛОВИ – SPY FILES

Масовни мониторинг популације широм планете постао је реалност и нова тајна индустријске шпијунаже која тренутно обухвата 25 земаља. Звучи као нови филм из Холивуда, али од данас, системи масовног мониторинга и пресретања информација који су изграђени од западних обавештајних служби су реалност. Данас постоји јавна база података, на десетине, а може се слободно рећи и на стотине документата из чак 160 обавештајних служби које масовно прате најразвијеније индустрије на планети. Међународне компаније за надзор и управљање дигитално/аналогних података су засноване у више земаља, технолошки су напредне и продају своју технологију свакој земљи на свету која је спремна да плати и за то има интерес. Оваква трговина у пракси није регулисана правно. Обавештајне агенције, војне силе и полиције су у стању да масовно, тихо и тајно пресретају позиве и преузимају рачунаре без помоћи или знања од телекомуникационих и интернет провајдера. Физичка локација корисника се може пратити, па чак и ако је мобилни телефон на стенд-бју, из разлога јер је мобилни телефон у сталној „комуникацији“ са базном станицом оператора или провајдера али и сателита преко GPS локатора (перифидно је понуђена опција на пример да када се сликаје, GPS вам омогући да уз име слике дода и назив локације, као да сами не знate где сте се сликали, а у ствари је класична потреба за надзором личности које су занимљиве службама безбедности). Западне компаније продају обавештајним агенцијама широк спектар опреме за масовни надзор, праве софтвере и апликације које омогућавају праћење али праве и уређаје за „сигурну“ комуникацију са огромним бројем бита у крипто кључу итд, а уствари имају клијенте на длану.

У последњих десет година системи за неселективни, масовни надзор су постали норма и обавеза. Компаније као што су „VASTech“ тајно продају опрему која може да трајно бележи телефонске позиве читавих народа. Могу да бележе положај сваког мобилног телефона у граду, са тачношћу радијуса од неколико метара али и тачније. Компаније развијају системе за инфицирање уређаја сваког корисника Facebook-а ако се јави потреба за мониторингом становништва. Компаније као што су „Hacking team“ из Италије и „Vupen“ из Француске производе малвере (тројанаце) којима је могуће да преотму појединачне компјутере и телефоне (iPhone, Bluberry и Android) преузму уређај, изврше преузимање снимљеног садржаја на уређају из свакодневне употребе, прате

кретање лица путем (GPS), па чак и слушају звуке у просторији у којој се уређај налази. Могу да идентификују појединце према полу и старости и да их прате на основу гласа. Постоји база података у Америци где се сваки глас везује за једну особу (на десетине параметара идентификују један глас једне особе као нпр. тоналитет, начин изговора, боја гласа итд.) додаје им се ID број и похрањује се у базу. Када се особа огласи преко било ког другог уређаја (може нон стоп да мења уређаје за комуникацију) увек буде препозната (ништа не помаже да се особа скрије од ове методе).

У јануару 2011. године, Агенција за националну безбедност уложила је 1.5 милијарду долара у објекат у пустињи у Јути који је дизајниран да заувек чува терабајте и терабајте домаћих и страних обавештајних података. Те податке је могуће обрађивати накнадно у наредним годинама или у реалном времену.

Телекомуникационе компаније сарађују са обавештајним службама у одавању информација својих клијента без обзира на земљу. Током августовских немира у Великој Британији компанија „Research in Motion“ (RIM) доноси одлуку да понуди властима да помогне у идентификацији својих клијената који су користили „Blackberry“ и који су учествовали у нередима (пошто се зна да велики број Британаца користи уређаје поменутог бренда). Компанија RIM је после наведеног догађаја ступила у преговоре са владама Индије, Либана, Саудијске Арабије и Уједињених Арапских Емирата и понуди им све податке из комуникације са BlackBerry Messenger.

Званичници CIA су купили софтвер који им омогућава да прате телефонске сигнале и прикупљају гласовне отиске одмах (у реалном времену) како би одредили конкретан идентитет лица које прате, као и место на коме се налази. Као пример навешћемо илустрације 6. и 7.

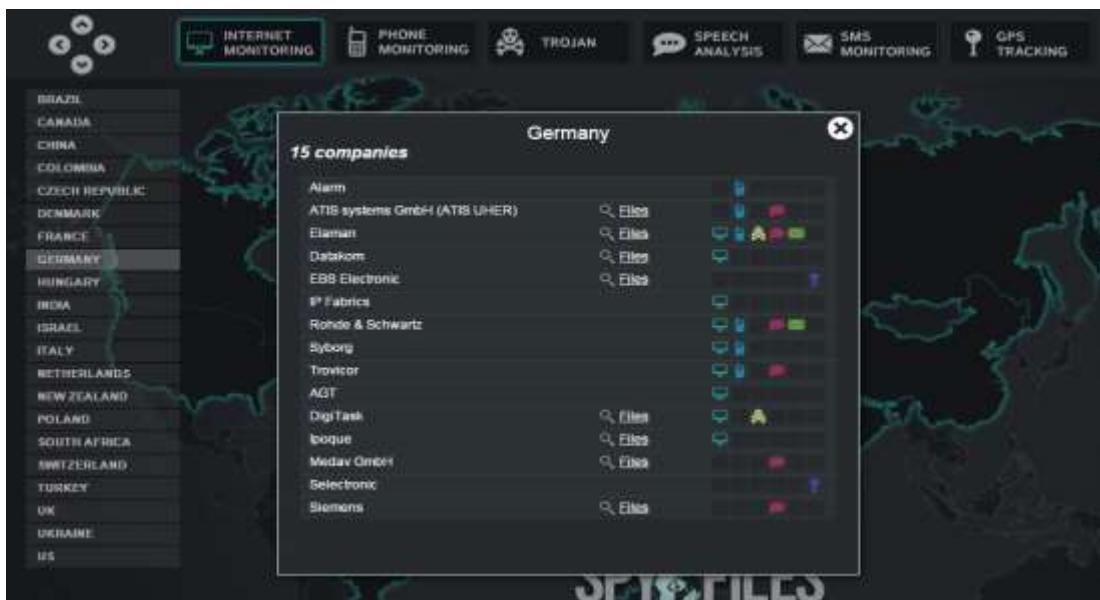
Слика 6. – Приказ земаља који су под свакодневним мониторингом



Извор: <http://www.kaspersky.com/>

Илустрација 6. показује 25 земаља које су под свакодневним мониторингом у последњих неколико година и методе којим се мониторинг врши.

Слика 7. – Приказ 15 компанија које врше мониторинг у Немачкој



Извор: <http://www.kaspersky.com/>

Илустрација 7. показује које компаније врше мониторинг или су можда продале кодове софтвера обавештајним агенцијама. У 25 земаља се одвија праћење грађана у комуникацијама преко:

- интернета,
- мобилних уређаја,
- убацивања малвера – тројанаца,
- анализе говора,
- праћења sms порука и
- GPS праћења.

По наводима Викилиksа, Америчка служба националне безбедности (NSA) пратила је разговоре између Немачке канцеларке Ангеле Меркер и њених министара. Као што је наведено у илустрацији 7. види се да су чак 6 од укупно 15 компанија биле ангажоване на мониторингу телефонског саобраћаја у Немачкој.

8. САЈБЕР ЋЕЛИЈА

Сајбер ћелија је јединица сачињена од групе сајбер ратника који користе сајбер оружје. Методологијом прикупљања информација долази се до закључка да једну сајбер ћелију могу да чине пар или неколико стотина ратника, исто тако могу бити на једној или на више различитих локација и у једној или више различитих држава, јер јединственог правила нема. Једно правило за креирање сајбер ћелије може да буде присутно, а оно зависи од методологије напада сајбер оружјем према противнику. У зависности од логистике напада креирају се потребни капацитети сајбер ћелије. По улоги сајбер ратника и „формацијским местима“ једна сајбер ћелија би требало да изгледа:

- извршилац (сајбер ратник),
- оператор,
- аналитичар,
- менаџер (организује буџет, набавку хардвера, софтвера и купује/продaje разне информације на црним маркетима),
- удаљени помоћници,
- систем администратор (особа едукована за рад на рачунарским мрежама),
- хардвераш,
- бот који прикупља информације у сајбер простору (често се дешава да ово место не раде људи већ софтвери),
- бот нападач (често се дешава да ово место не раде људи већ софтвери),
- лица која прикупљају информације из реалног света и баве се обавештајним радом,
- лица која креирају методологије напада,
- технички консултенти,
- лица за развој малвера – сајбер оружја,

- лица за тестирање сајбер оружја (контрола отицања информација о нападачу и контрола одстрањивања ефекта „бумеранг“).

Слика 8. – Пример сајбер ћелије за истрагу сајбер криминала у Индији

Извор: <http://cybercellmumbai.gov.in/>

Види се из предходне илустрације 8. да је Индија развила тим – ћелију за борбу у сајбер простору. Реч је о полицијској јединици. Индија као једна од најмноголјуднијих земаља на планети има више аспеката због којих је била у обавези да развије овакву врсту одбране земље.

Доба Сајбер рата - конфликт без правила

Широм света безбедносне службе едукују владе земаља да смо у сајбер добу и да у сајбер сукобима учествују борци без правила и не поштују се никакве конвенције у борби. Свака држава је дужна да инвестира у развој сопствене сајбер способности. Главни фактори који излажу становништво потенцијалном ризику од сајбер напада су:

- велика размера дифузије рачунарских и комуникационих мрежа,
- немогућност обједињеног управљања критичних система,
- еволуција технолошког пејзажа,
- недостатак граница у сајбер простору.

Из регулаторне перспективе, неопходно је обезбедити следеће одговоре:

- Шта се подразумева под употребом сile у сајбер простору?
- Када би требало сајбер напад изједначити са оружаним нападом?
- Које су методе, како правити методологију и ниво сразмераног одговора на сајбер напада?
- Који скуп правила треба да важи за овакву врсту одговора?
- Како регулисати законску одговорност актера укључених у сајбер операције?
- Како балансирати потребе националне безбедности са императивом потребе да се заштите индивидуалне слободе грађана?

На ова питања аутор овог рада није дао одговор јер је потребно да се у укључе све свере друшта и да се на националном нивоу одлучи о пименутим питањима. Сајбер простор је значајан као нови домен за могуће поље ратовања, у којој употребу сајбер оружја треба тачно регулисати на исти начин као што је регулисано за нуклеарни или хемијски арсенал у конвенционалном рату. Сајбер домен је баш као могући домен конфликта у стварном свету. У стварном свету имамо уговоре и конвенције као и агенције за надзоре и праћења поштовања за нуклеарно, биолошко и хемијско оружје па зашто не и за сајбер. Циљ је веома изазован.

Постаје очигледно да владе водећих земаља због тренутних предности у сајбер пољу у критичним тренуцима не желе да ограниче своје способности конвенцијама и прописима о сајбер рату у сајбер простору. Свесни су да многи противници тајно улажу у област сајбер простора због страха да ће се наћи неспреми да одговоре сајбер офанзиви.

Експерти су дали правну дефиницију за концепт шта је сајбер напада и сајбер оружје: „*Сајбер напади, сајбер шпијунаже или сајбер операције, биле увредљиве или дефанзивне, а које ће за последице изазвати повреде или смрт лица или оштећења инфраструктуре или уништење објеката*“. Пример представа коришћеног за сајбер напад и метода напада би могао бити ddos напад који се спроводи помоћу ботнет-а. У овом случају ботнет има улогу средства у сајбер ратовању док метод напад представља ddos. Експерти су такође навели два основна концепта којих би требало да се придржавају сајбер ратници, а то су:

- забрањено је коришћење представа и метода у сајбер рату које ће да изазову претерану (без цивилних жртава, колатералних штета итд.) или непотребну патњу,
- сваки пут када би се користило средство или метод за сајбер рат потребно је да се спроведу правне анализе као би се утврдили технички опис, природа циљева, утицај на циљеве, прецизност и обима жељених ефеката.

9. ЗАКЉУЧАК

Задатак да се одгонетне шта је сајбер оружје, сајбер домен и сајбер ратовање није ни мало једноставан, а последице њиховог утицаја могу бити тешке чак и катастрофалне како по деловима тако и за целу државу.

Упркос заједничком интересу многих влада широм планете, стручњаци за сајбер домен верују да је концепт сајбер оружја превише „апстрактан“ и због тог разлога постоји бојазан да се према сајбер оружју државне институције односе подцењивачки и да немају свест о правој опасности које сајбер оружје може да нанесе. Главни аргументи за предходну тврђњу су да је до данас постојање сајбер оружја под утицајем неколико хиљада људи, сва јавно позната сајбер оружја имају далеко мању ватрену моћ него што се обично претпоставља у јавности и сајбер оружје се може користити у комбинацији са средствима НВО. Сајбер простор ће се дубоко променити, а са њим и концепт сајбер безбедности.

Јасно се види да је главни адут свих претњи у сајбер простору јесте сајбер оружје које се креира писањем програмског кода у неком програмском језику са пред припремним активностима – обавештајним радом и креирањем методологијом за напад од сајбер ратника једне или више сајбер ћелија.

Државна администрација, војска, полиција и приватни сектор морају улагати у развој сајбер јединица – ћелија, да би спремани дочекали изазове сајбер напада, не потцењујући могуће ризике.

За крај приведимо овај рад са једном мишљу и изјавом:

„Reset your thoughts“ илити ресетуј своје мисли,

а што би допринело значају очувања дигиталне имовине наше земље јер:

„**ми смо сви међусобно повезани свесно или несвесно на огромној глобалној мрежи. Онај ко контролише мрежу, контролише све нас и контролише свет.**“

DIGITALNA FORENZIKA-MOBILNI TELEFON KAO IZVOR DIGITALNIH DOKAZA

Prof.dr Vojo Laković¹, Doc. dr Slobodan Simović², Mr Jovana Simović³

¹Univerzitet „Hercegovina“ Mostar-FDZMB

²Fakultet za diplomaciju i bezbednost-Beograd,Srbija, slobodandsimovic@gmail.com

³The Learning Academy UK, London ,Engleska, Operations director

Apstrakt: Pojava prvi digitalnih zločina registrovana je sa pojavom personalnih računara.. Kako se ovakav kriminal ne može suzbiti bez otkrivanja krivaca, a do njih se ne može doći samo putem klasičnih operativno istražnih radnji, te DNK analiza, došlo je vreme da se osformi novi vid prikupljanja dokaza sa virtuelnih mesta zločina. Ta oblast koja se bavi prikupljanjem digitalnih dokaza je upravo digitalna forenzika. S druge strane,danas, mobilni telefon predstavlja multifunkcionalni telekomunikacioni uređaj koji je, kao nijedan drugi, postao neodvojivi deo svakodnevnice. Takve karakteristike mobilnih telefona i osobine njihovih korisnika naglašavaju značaj prikupljanja podataka koji se u njima nalaze za potrebe rada tužilaštva I policije i obezbeđenja dokaza za uspešno vođenje krivičnog postupka.

Ključne reči: digitalna forenzika, digitalni dokazi I mobilni telefon.

UVOD

Kako se sve više IT tehnologija razvija i digitalni zločini se sve više razvijaju. Postoji svakog dana sve više načina za prevare i razne zločine putem računara. Velika većina zločina koji se odvijaju uživo mogu se činiti i putem računara ili interneta. Elektronski dokaz ima sve veći značaj i zbog toga se sa njima mora postupati vrlo pažljivo. Često se prikupljanje i analiza tih dokaza ne može obaviti pomoću jednog alata već kombinacijom više njih. Svaki od alata je namenjen jednoj ili više faza istrage. Često su digitalni tragovi oštećeni, pod zaštitom ili izgubljeni ili izbrisani, zbog toga se moraju koristiti različiti alati. Glavni nedostatak svih alata je to što je velika većina njih licencirana i cene licenci su veoma visoke, što naravno zavisi od toga kakve su namene tog programa i koliko mogućnosti pružaju i da li je moguće dokupljivati njegove dodatke. Iako su alati skupi njihova primena je od ključnog značaja za forenzičku istragu i zbog toga je njihova upotreba opravdana. Cilj je da se skrene pažnja na izuzetno ranjive male sisteme "pametnih" uređaja koji su sa nama svakog dana a nismo svesni opasnosti koje iz njih vrebaju i u koje možemo doći ukoliko se neko dočepa podataka sa tih uređaja. Ti isti uređaji mogu nas zaštитiti ukoliko je potrebno. Svi ovi mobilni uređaji na ovaj ili onaj način mogu biti dokazni materijal protiv nekog zločinca. Važno je upotrebiti ga na pravi način. U poslednjih nekoliko godina zakonske odredbe su se menjale da bi podaci prikupljeni sa mobilnih uređaja bili priznati na sudu ukoliko prođu verifikaciju i validaciju. Mobini uređaji su deo svakodnevnice, svaki čovek je deo svoga dana spojen sa barem jednim takvim uređajem, ako ne i sa više. Posebno je izazov i jako dobra meta zlonamernih to što su mobilni uređaji sve "pametniji" i sve više podataka o nama samima sadrže u sebi, počev od ličnih stvari pa sve do poslovnih, koje su upravo meta kriminalaca,ili su svakodnevno u funkciji istih.

1. FORENZIKA KROZ ISTORIJU

Koreni forenzičke vode sve do Rimskog doba kada su krivične prijave podrazumevale javno iznošenje slučaja u Forumu.Lice optuženo za krivično delo i podnosič prijave,bi javno raspravljali o ovome a osoba sa boljom argumentacijom i prezentacijom bi prevladala.Otuda i poreklo samog naziva Forenzička od latinske reči forēnsis što znači “pred forumom”.Danas,Forenzička podrazumeva upotrebu čitavog spektra nauka u cilju pružanja odgovora na pitanja od pravnog interesa a u vezi sa kriminalom ili parničnim postupkom.Prema istorijskim zapisima,prva upotreba Forenzičke pripisuje se Arhimedu (287-212 pne) koji je imao za zadatak da utvrdi da li je kruna koja je bila napravljena za kralja Hieron II,od čistog zlata ili je nepošteni zlatar dodao još neki element u nju.Prvi pisani dokument o upotrebi medicine i entomologije (nauka o insektima) u rešavanju krivičnih predmeta,pripisuje se knjizi Xi Yuan Lu (宋慈, 1186–1249) koja je objavljena 1248.U jednom od slučaja osobe ubijene sa srpom istražitelj je rešio slučaj tako što je tražio da svi koji poseduju srpove donešu na jedno mesto.Na srpu koji je koristio ubica počele su da se skupljaju muve privučene mirisom krvi.Onda je na životinjskom lešu pravio rane srpovima.Pošao je od toga da će srp sa kojim je ubijen čovek napraviti identičnu ranu i na životinjskom lešu.Nakon iznošenja ovih dokaza,ubica je priznao zločin.

Knjiga je takođe davala savete o tome kako da se napravi ralika izmedju davljenja (voda u plućima) i davljenja (polomljen vrat i hrskavica) zajedno sa drugim dokazima proizišlim iz ispitivanja leša i utvrđivanja da li je smrt prouzrokovana ubistvom, samoubistvom ili je reč o nesreći. U 16-om veku u Evropi, vojni lekari su intenzivno proučavali i prikpupljali podatke o načinu i uzroku smrti kod vojnika. Ambroise Paré, francuski vojni hirurg, je sistematski proučavao efekte nasilne smrti na unutrašnje organe. Dva Italijanska hirurga, Fortunato Fidelis i Paolo Zacchia, postavili su temelje moderne patologije, proučavanjem promena u strukturi tela koje su se desile kao posledice bolesti. 1773. godine, Švedski hemičar Carl Wilhelm Scheele, osmislio je način otkrivanja Arsenal u leševima ali samo u velikoj količini. Ova istraživanja su proširena kada je Nemački hemičar Valentin Ross 1806. uspeo da otkrije otrov u zidovima želudca žrtve. 1836. englesko hemičar James Marsh je koristio hemijske procese pri utvrđivanju uzroka smrti kao posledice trovanja Arsenom. Policija je počela da koristi otiske prsiju kao dokazni materijal kada je Juan Vucetich u Argentini rešio slučaj ubistva korišćenjem krvavog otiska prstiju koji se nalazio na uzorku skinutog odsecanjem dela vrata na kome su se otisci nalazili. 1909. Rodolphe Archibald Reiss (1875-1929) otvara prvu školu Forenzičke u Lozani (Švajcarska) [1]. Što se tiče digitalne forenzičke istorije je malo drugačija. Sami računari su se pojavili tek sredinom XX veka. I tada kada su se pojavili računari još uvek nije bilo interneta pa ni samog digitalnog kriminala pa za forenzikom tog tipa nije bilo potrebe. Prvo početkom sedamdesetih godina XX veka, sa pojavom interneta, i kasnije početkom osamdesetih godina, kada personalni računari postaju pristupačniji, dolazi do njihove sve veće zloupotrebe, tj. povećanja upotrebe kompjutera prilikom izvršenja kriminalnih radnji. Zbog toga je Federalni istražni biro (Federal Bureau of Investigation - FBI) 1984. godine offormio novu jedinicu Computer Analysis and Response Team (CART) koja je imala za cilj da se izbori sa sve većim brojem slučajeva koji su uključivali digitalne dokaze. U kompjuterske zločine spadaju hakovanje, dečija pornografija, kompjuterske prevare, sabotaže, krađa identiteta itd. ASCLD-LAB društvo (American Society of Crime Laboratory Directors/ Laboratory Accreditation Board) je 2003. godine prihvatiло pojam digitalne forenzičke i značaj digitalnog dokaza u rešavanju zločina, dok je Kanada prva zemlja koja je 1983. godine donela zakon koji delimično reguliše digitalni zločin, nakon njih sledi Amerika 1986., zatim Australija 1989. godine a potom i Engleska 1990. godine. Od tada se povećalo interesovanje za edukacijom i želja za unapređenjem ove novonastale nauke. Danas, u Sjedinjenim Američkim Državama postoji više desetina koledža koji su specijalizovani za ovu oblast. SAD je trenutno lider u ovoj oblasti. [2] Iako je digitalna forenzička priznata tek pre nekoliko godina, prvi zabeleženi napad na neku digitalnu infrastrukturu se desio 1988. godine od strane Roberta Morisa. On je pronašao grešku u jednom računarskom sistemu i uz pomoć virusa "srušio" 6000 računara na internetu. Zbog toga je morao da plati odštetu od 10.000 dolara, dobio je kaznu od tri godine zatvora i 400 sati dobrovoljno korisnog društvenog rada. [3]

Forenzička i njena grana, digitalna forenzička, su postale popularne početkom devedesetih godina prošlog veka sa pojavom prvih televizijskih serija na ovu temu: *Crime Scene Investigation*, *Criminal Minds*, *Dexter*, *Law & Order*, *Forensic Files* itd. Rast kompjuterskog kriminala tokom 1980-ih i 1990-ih godina je primorao tzv. agencije za sprovođenje zakona da počnu da formiraju specijalizovane grupe da rukuju tehničkim aspektima istrage. Jedna od prvih zabeleženih primena digitalne forenzičke je kada je Cliff Stoll (Cliff Stoll) tragaо za hakerom Markusom Hesom (Markus Hess) 1986. godine. Stoll nije bio specijalizovan za ovakav vid istrage ali je koristio tehnike kompjuterske i mrežne forenzičke u svojoj istrazi. Tokom 1990-ih godina došlo je velike potražnje za ovim novim vidovima istrage. Došlo je do formiranja mnogih regionalnih, pa čak i lokalnih jedinica koje će se baviti digitalnom forenzikom. Tek 1992. godine termin "digitalna forenzička" počinje da se koristi u stručnoj literaturi, od strane Koliera (Collier) i Spaula (Spaul) koji su prvi u svom radu pokušali da objasne ovaj pojam i opravdaju ga svetu. Brz razvoj digitalne forenzičke je uzrokovao nedostatak standardizacije i obuke u ovoj oblasti. Neki od prvih pisanih radova vezanih za ovu oblast su izdati tek nakon 2000. godine. Radna grupa za digitalne dokaze (The Scientific Working Group on Digital Evidence (SWGDE)) je 2002. godine izdala rad na temu "Najbolje primene kompjuterske forenzičke", nakon toga izdat je ISO standard 2005.

2. POJAM DIGITALNE FORENZIKE

Osnovna definicija je da je digitalna forenzika vid sistematske kontrole kompjuterskog sistema, i sadržaja istog, radi prikupljanja dokaza o izvršenom krivičnom delu ili nekoj drugoj zloupotrebi, u čijem je izvođenju učestvovao računarski sistem. Takođe predstavlja primenu računarske nauke i matematike za pouzdano i nepristrasno prikupljanje, analizu, interpretaciju i prezentaciju digitalnih dokaza za potrebe rekonstrukcije događaja koji je okarakterisan kao kriminalno delo ili kao pomoć kod predviđanja i prevencije neautorizovanih događaja i akcija.^[4] Pored ove osnovne definicije ,pod digitalnom forenzikom smatra se I korišćenje naučno razvijenih i dokazanih metoda za prezervaciju, prikupljanje, validaciju, identifikaciju, analizu, interpretaciju, dokumentaciju i prezentaciju digitalnih dokaza dobijenih iz izvora kao što su hard disk računara ili memorija mobilnog telefona, a radi lakše i naprednije rekonstrukcije događaja vezanih za izvršenje krivičnog dela .^[5] Ova definicija navodi konkretnе korake, zato je I operativna, koje je potrebno preduzeti da bi se prikupljeni podaci mogli koristiti kao digitalni dokazi, naravno uz poštovanje načela kriminalistike. Forenzika mobilnih telefona, što je u osnovi I naša tema, može se definisati kao naučna disciplina koja se bavi pribavljanjem digitalnih dokaza iz memorija mobilnih uređaja i SIM kartica u forenzičkim uslovima uz korišćenje prihvaćenih metoda.^[6]

Digitalna forenzika se može podeliti na računarsku, forenziku mobilnih uređaja, mrežnu i forenziku baza podataka.U zavisnosti od oblasti digitalne forenzike koriste se različiti alati koji se osim po oblasti mogu podeliti i po načinu implementacije, tipu koda, platformi na kojoj rade i prema fazi procesa koju obavljaju u istraži.. Digitalna forenzika ima široku primenu i nije ograničena samo na policijsko-sudske i vojno-obaveštajne aktivnosti. Bankarski sektor, osiguravajuća društva i kompanije raznih profila imaju potrebu i moraju biti izuzetno oprezni sa podacima kojima raspolažu jer je mnogim kompanijama nanesena nemerljiva šteta zbog industrijske špijunaže i generalne zloupotrebe IT sistema. [7]

Iz napred iznetog, a u cilju konkretizacije predmeta našeg istraživanja, forenzika mobilnih telefona može se definisati kao naučna disciplina koja se bavi pribavljanjem digitalnih dokaza iz memorija mobilnih uređaja i SIM kartica u forenzičkim uslovima uz korišćenje prihvaćenih metoda [8]

2.1. Digitalni dokaz

Digitalni dokaz može se definisati kao bilo koji podatak sačuvan ili prenet korišćenjem računara, a kojim se potvrđuju ili opovrgavaju teorije o načinu izvršenja krivičnog dela ili označavaju kritični elementi dela kao što su namera ili alibi [9], ali i kao skup podataka koji mogu da dokažu da je krivično delo počinjeno ili da povežu zločin i žrtvu ili zločin i počinioca [10]. Definicija predložena od strane Radne grupe za standardizaciju digitalnih dokaza (Scientific Working Group on Digital Evidence - SWGDE) je da je to bilo koja informacija koja ima dokazujuću vrednost i koja je pohranjena ili preneta u digitalnoj formi. Međunarodna organizacija za računarske dokaze (International Organization of Computer Evidence - IOCE) definiše digitalne dokaze kao informacije sačuvane ili prenete u binarnom formatu na koje se može pozvati na sudu. Najuprošćenije digitalni dokaz predstavlja informaciju od značaja za istragu, a koja je skladištena u digitalnoj formi. Originalni dokaz treba da bude sačuvan u originalnom ili što približnijem stanju. Ako je potrebno dalje ispitivanje ono se vrši nad kopijom koja mora biti precizno napravljena i skladištena na „forenzički sterilnom“ medijumu (medijum na kojem prethodno nije bilo podataka). Svi dokazi moraju biti propisno označeni i dokumentovani. Ako su podaci obrisani ili oštećeni, upotrebom određenog softvera moguće ih je povratiti. Taj proces može trajati dugo ako je izgubljen ili oštećen veliki broj podataka. U digitalne dokaze spadaju digitalni video i audio signali, zapisi sa digitalne faks mašine, digitalne kamere ili foto aparata, raznih mobilnih uređaja itd. Neki digitalni materijal postaje dokaz onog trenutka kada ga sud prizna i kada se on prikupi na legalan način. Sud odlučuje da li je taj materijal relevantan za istragu i da li je materijal autentičan.

Naš čuveni profesor kriminalistike, pok. Živojin Aleksić⁴⁵ insistirao je, što je operativno opravdano, a pre svega logično, da se prikupljanjem i obradom digitalnih dokaza bavi odeljenje kriminalističke tehnike, jer

⁴⁵ Aleksić je kriminalistiku specijalizirao 1963. godine u Lozani, kod čuvenog profesora Bišopa, Interpolovog eksperta koji je metodom veštačenja ušne školjke otkrio lažnu princezu Anastasiju Romanov. Aleksić je kasnije bio zadužen od vlasti da utvrdi da li postoje dva Josipa Broza Tita, kada se poslužio upravo tom tehnikom koja se zasniva na tvrdnji da "ne postoje dva čoveka sa istim usima". "Ušne školjke imaju oko 50 karakteristika na osnovu kojih se može utvrditi identitet. Najstarija fotografija koju sam imao

ono proučava i primenjuje metode i sredstva iz oblasti prirodnih i tehničkih nauka u cilju otkrivanja i razjašnjavanja krivičnih dela, otkrivanja počinilaca i obezbeđivanja dokaza [11]. Njegova je I konstatacija da naše referentne obrazovne institucije u oblasti pravnih nauka nisu uvrstile prikupljanje digitalnih dokaza sa mobilnih telefona ili računara u svoje kriminalističke udžbenike, ali da zato postoje načela kriminalistike koja su univerzalna i po kojima se mora postupati u radu. Načela kriminalistike su: načelo zakonitosti, načelo metodičnosti, načelo operativnosti i brzine, načelo temeljitosti i načelo čuvanja službene tajne.

Digitalna forenzika mobilnih telefona za potrebe krivičnog postupka

Početkom ovog veka, inspirisan time što je na desetine ubica u Velikoj Britaniji otkriveno I uhapšeno zahvaljujući dokazima vezanim za njihove telefone ili telefone žrtava, Kris Samers je za BBC News Online, objavio članak pod nazivom “ *Mobile phones - the new fingerprints* ” (Mobilni telefoni - novi otisci) [12] ističući na taj način značaj digitalnih dokaza još pre nego što je bilo koja od danas renomiranih firmi uopšte počela da proizvodi forenzičke alate za mobilne telefone. Značaj digitalnih dokaza u otkrivanju izvršilaca određenih krivičnih dela zapažen je I u SAD, pa je 2006.godine zabeleženo da je 80% sudskih slučajeva u to vreme imalo neku vrstu digitalnih dokaza povezanih sa njima. [13] I kod nas, u Srbiji, je porasla svest o značaju digitalnih dokaza, forenzike uopšte. Mobilni telefoni se rutinski oduzimaju prilikom privođenja, zadržavanja I pretresa lica I objekata I što se same forenzike mobilnih telefona tiče, ona u srpskoj policiji sistematizovano funkcioniše tek nekoliko godina, a rezultat od preko nekoliko hiljada forenzički obrađenih telefona (i SIM kartica) je značajan čak i za države mnogo veće od Srbije, mada srazmeran stopi kriminala.

Danas mobilni telefoni, onakvi kakvi jesu, funkcionalni, jeftini, jednostavni za korišćenje, stalno prisutni kod korisnika, masovnost u korišćenju doveli su do toga da postanu značajan predmet interesovanja za učesnike u krivičnom postupku. Mobilni telefoni mogu biti objekat izvršenja (bilo da su ukradeni ili zaraženi zlonamernim softverom) mogu biti sredstvo za izvršenje krivičnog dela (na primer, snimanje dečije pornografije ili zlostavljanja), i mogu ,sto je predmet našeg interesovanja, sadržati dokaze vezane za određeno krivično delo. Telefoni se sa izvršiocem krivičnog dela nalaze na licu mesta, u toku pripreme izvršenja, pa i dok je u bekstvu (uglavnom, bar kod ozbiljnih kriminalaca, različiti uređaji u svakoj fazi). Dokazi koje sadrže su raznovrsni i brojni, a sačuvani su u digitalnom formatu.

Sve navedeno ukazuje na to da mobilni telefoni imaju raznovrsne mogućnosti kreiranja, preuzimanja i razmene velikog broja različitih datoteka i informacija potrebnih ili interesantnih korisniku, što ih upravo čini vrlo zanimljivim za forenzu i krivični postupak. Neke od informacija koje se mogu dobiti sa mobilnih telefona i koristiti kao dokazi su: [14]

- sačuvane fotografije, audio i video zapisi (posebno zanimljivi su oni snimljeni samim telefonom);
- sačuvane SMS i MMS poruke i poruke elektronske pošte, sa podacima o pošiljaocu, odnosno primaocu i temporalnim podacima;
- sačuvane datoteke sa računara i one kreirane aplikacijama sa telefona;
- datoteke instaliranih aplikacija;
- podaci iz kalendara, telefonskih imenika i drugih PIM aplikacija;
- podešavanja vezana za Internet komunikaciju i podaci dobijeni korišćenjem telefona u ovu svrhu, poput istorije aktivnosti (*History*), omiljenih stranica (*Favorites* ili *Bookmarks*) i samih Internet stranica, odnosno fragmenata kada su u pitanju dinamičke stranice.

Serijski broj kartice i podatke o mobilnom operatoru (na primer logo ili naziv) koji su najčešće odštampani na samoj kartici. To su podaci na osnovu kojih se od operatora mogu tražiti informacije važne za dalju istragu, poput podataka o preplatniku, ukoliko je registrovan (što je najčešći slučaj kada se radi o postpejd korisniku), ali i preplatnički broj kartice koji je dodeljen tom serijskom broju na osnovu koga se mogu tražiti listinzi komunikacija, PIN ili PUK kodovi i drugi podaci iz registara operatora;

bila je policijska fotografija iz 1928. godine, kada je Tito uhapšen zbog bombaškog napada u Zagrebu. Veštačenjem uva utvrdio sam da je to jedan isti čovek od 1928. godine do kraja života", rekao je prof. Aleksić u poslednjem intervjuu za "Politiku" sredinom novembra 2011. godine.

- *Location Area Identifier* (LAI) uz pomoć koga može da se utvrdi (uz asistenciju operatora) oblast u kojoj se korisnik nalazio u vreme kada je uređaj poslednji put radio;
- primljene tekstualne poruke, kojih može da bude 20 do 30. Postoji i mogućnost ponovnog pristupa određenom broju obrisanih poruka, jer se prilikom brisanja poruke samo bitovima statusnog bajta dodeljuje vrednost 0, dok sadržaj ostaje netaknut dok ga ne istisne nova poruka. Nakon istiskivanja od strane nove poruke, delovi sadržaja stare poruke ne ostaju čak ni u *slack* prostoru, jer se on ispunjava heksadecimalnom vrednošću FF;
- listu kontakata (novije verzije kartica mogu da sačuvaju do 250 kontakata);
- listu poslednjih biranih brojeva.

U postupku forenzike mobilnih telefona mora se uzeti u obzir GSM mreža u kojoj se beleže podaci o korisniku, SIM kartici i aktivnostima telefona. GSM mreža sadrži informacije koje se mogu koristiti kao dokazi, a najvređnije se nalaze u zapisima podataka o pozivima (CDR – *Call Data Record*), datotekama mobilnog operatora koje sadrže podatke o svim komunikacijama u mreži [12]. To znači da, pored podataka o pretplatniku, servisima koji su mu na raspolaganju i SIM kartici (brojevi MSISDN, IMSI, ICCID, PIN i PUK), iz CDR datoteka se mogu izdvojiti informacije o datumu, vremenu, trajanju i vrsti bilo koje komunikacije, zatim o uređaju u kome se nalazila SIM kartica, kao i identifikacija ćelije preko koje je poziv ostvaren, što može da se iskoristi za lociranje korisnika. Određeni podaci iz sistema GSM mreže koji se koriste samo radi uspostavljanja i održavanja komunikacije (drugim rečima, podaci koji nisu bitni za naplatu, što utiče na njihovo relativno kratko čuvanje), poput podataka u HLR (*Home Location Register*) bazi podataka, mogu u određenim trenucima biti od koristi. Primera radi, ukoliko korisnik ne isključi telefon već mu se isprazni baterija ili dođe do prekida neke druge vrste, postojeće podatak u kom rejonu se telefon nalazio u momentu gašenja, što može biti od važnosti prilikom istraga o nestalim osobama. [15]

3. FORENZIČKA ANALIZA MOBILNIH TELEFONA

Kod forenzičke analize mobilnog telefona susrećemo se s mnogo problema. Pre svega, različiti alati za ekstrakciju podataka iz telefona i memoriskih kartica proizvode različite setove podataka. Nema šire u-svojenih standarda, pa podaci i primljene tehnologije nisu interoperabilni, a nailazi se na ogromne količine podataka, često i više od 100.000 podataka različite vrste samo na jednom telefonu.[16] Teško je odvojiti podatke koji su u vezi s krivičnim delom od ostalih, a sami podaci su nekonsolidovani i neprovezeni. Kompleksnost analize povećava veliki broj izvora i vrsta podataka na koje nailazimo, kao što su: IM-SI (International Mobile Subscriber Identity), korisnički brojevi, lista poziva, lista SMS poruka, lista kontakata, IMEI (International Mobile Equipment Identity), sistem datoteka, muzika, fotografije, video-snimci... Uzmimo kao primer digitalnu forenzičku analizu grupe dilera narkotika od kojih je oduzet veći broj telefona, kao i mnogo veći broj SIM kartica. Prvo što možemo da predpostavimo je kompleksnost podataka vezanih za međusobnu komunikaciju i ogroman broj ostvarenih kontakata. Dodajmo tome sve ostale moguće podatke i korelacije u relativno maloj grupi telefona i SIM kartica i shvatićemo koliko je složeno napraviti sudske prihvatljive forenzičke digitalne analize mobilnih telefona. S obzirom na to da je u redovnom istražnom postupku oduzimanje mobilnog telefona osumnjičenog kao dokaznog materijala postalo redovno, možemo samo predpostaviti koliko je veliki sajber prostor svih trenutno oduzetih mobilnih telefona koji na neki način predstavljaju dokazni materijal.

Savremena forenzička analiza mobilnih telefona mora da se zasniva na alatima koji će omogućiti forenzičarima efikasno, brzo i jeftino dobijanje obaveštajnih podataka i potrebnih dokaza iz mobilnih telefona i telekomunikacionih mreža. Tehnologija treba da omogući otkrivanje kritičnih informacija iz kompleksnog spektra mogućih na analiziranim medijima. Savremeni alati treba da omoguče korišćenje za istraživanje jedne jedinice ili hiljadu jedinica u isto vreme. Važno je da se može automatski procesirati velika količina telekomunikacionih podataka i omogućiti pristup tim podacima u realnom vremenu. Analiza treba da bude takva da se ne troši mnogo vremena na manipulaciju podacima i odbacivanje nepotrebnih informacija, da se omogući lak pristup najbitnijim informacijama, kao što su brojevi, SMS poruke, kontakti i slike, s mogućnošću analize kompletne korelacione slike podataka.

Obzirom na ogromnu količinu podataka, složenost i dugotrajnost sudskega postupaka, potrebu za čuvanjem i distribuciju velikog broja različitih sadržaja po strogo kontrolisanim procedurama, važno je da, uz alate savremene forenzičke laboratorije za visokotehnološki kriminal, i istražni organi imaju kvalitetan

softver za upravljanje, obradu, analizu, arhiviranje i distribuciju podataka, kako mobilnih tako i klasičnih digitalnih uređaja.

Na kraju, moramo konstatovati nesporну činjenicu, da je od svih faza forenzičke mobilnih telefona koje su navedene u definiciji digitalne forenzičke, akvizicija ili prikupljanje digitalnih dokaza predstavlja, u kontekstu svega do sada navedenog, vitalnu fazu, a sa tehničke strane pravi suštinsku razliku između forenzičke mobilnih telefona i forenzičke računara. Postupak akvizicije podređuje se očuvanju integriteta podataka i shodno tome se prilikom njegovog sprovođenja moraju poštovati određeni principi. [17]

4. PRINCIPI I METODI PRIKUPLJANJA PODATAKA

- akcije koje se preduzimaju ne smeju menjati podatke sadržane na mobilnom telefonu ili na mediju za skladištenje (memorijska kartica);
- lica koja pristupaju originalnim podacima moraju biti kompetentna za to i sposobna da objasne akcije koje preduzimaju;
- neophodno je precizno dokumentovati svaki korak u radu;
- lice koje vodi istragu ima odgovornost da obezbedi da se principi poštuju i da su u skladu sa važećim zakonima.

Brian Carier je dobro zapazio da se u praksi nailazi na problem pri pokušaju poštovanja prvog principa: da bi se podaci prikupili sa mobilnog telefona, on mora da bude aktivan, a uključivanje uređaja ili njegovo povezivanje sa računarom će najverovatnije promeniti određene podatke. Zato on I sugerise da, ukoliko je menjanje podataka neizbežno, treba da bude u što manjoj meri. [18]

4.1. Prikupljanje podataka iz GSM mreže

Prikupljanje podataka iz GSM mreže je, pored manuelnog pregleda mobilnih telefona, akvizicije putem koneksionih servisa, direktnog pristupa memoriji i koneksionih agenata, jedna od metoda prikupljanja podataka. Jednostavno telefon radi u okviru GSM mreže, te se svi podaci koje sistem beleži mogu se koristiti u forenzičkoj analizi telefona. Na ovaj način se, pre svega, mogu saznati detaljni podaci o ostvarenim komunikacijama uređaja za duži vremenski period, a koji su pri tom mnogo pouzdaniji nego oni koji se čuvaju na samom telefonu, pa se često ova metoda akvizicije koristi za validaciju podataka prikupljenih nekom drugom metodom[19], po čemu je nama I interesantna.

Može se zaključiti da ne postoji idealan metod akvizicije podataka, već mora da se napravi kompromis između efektivnosti i efikasnosti, odnosno da se na osnovu operativnih podataka odredi prioritet i izabere odgovarajuća metoda za svaki slučaj ponaosob. Savremeni forenzički alati objedinjuju više metoda i pristupa, uz nastojanje da vrše što manje izmene na telefonu, a da prikupe što više digitalnih dokaza. Ali prilikom istraživanja mobilnih uređaja često se javlja potreba pisanja po njihovoj memoriji kako bi se došlo do informacije. U ovakvim slučajevima treba težiti da se zapiše što manja količina informacija. Najbolji primer akvizicije podataka korišćenjem neforenzičkih alata je korišćenje sinhronizacijskog softvera kako bi se pristupilo podacima na mobilnom uređaju. Tada se podaci kopiraju sa originalnog uređaja, ali se tom prilikom menjaju datumske i vremenske oznake podataka. U tom slučaju je teško dokazati da nije komprimovan integritet podataka. Problem se javlja i ukoliko se istraga sprovodi na nekom novom mobilnom uređaju za koji još ne postoje modifikovani forenzički alati, što je čest slučaj uzimajući u obzir brzinu menjanja tržišta mobilnih uređaja.. Zato, u cilju dokazivanja da svojim akcijama nije narušilo očuvanost digitalnih dokaza, lice koje vrši akviziciju mora da dokumentuje sve aktivnosti u radu sa mobilnim telefonom, izradi dodatne kopije I da precizno zapiše upotrebljene procedure I metode[18], i da interakciju sa uređajem svede na minimum. Što je više interakcija, to je komplikovanje dokazati da akcije nisu kompromitovale digitalne dokaze [19]. Ukoliko je mobilni telefon prilikom privremenog oduzimanja stavljen u omot i zapečaćen (što je u širem smislu i propisano članom 84. ZKP-a), a branilac ili okrivljeni prisustvuje uklanjanju omota i izvođenju akvizicije, ostvareni su svi uslovi da se tako prikupljeni podaci mogu koristiti kao digitalni dokazi, odnosno otklonjene su sumnje u eventualno narušavanje dokaznog materijala. Ovde svakako treba spomenuti i tzv. lanac nadzora (*chain*

of custody), koji podrazumeva hronološko dokumentovanje prikupljanja, kontrole, transfera i analize privremeno oduzetih predmeta, ali samo spomenuti, jer ga kao takvog naš zakon ne prepoznae.

5. DIGITALNA FORENZIKA U SRBIJI

Kao i svaka nova naučna disciplina, tako se i kompjuterska forenzika, godinama unazad, postepeno probija do statusa opšte prihvaćene metode utvrđivanja porekla i validnosti digitalnih dokaza. Kako se metode prikupljanja, analiziranja i prezentovanja digitalnih dokaza razlikuju u državama u kojima se istraga sprovodi, jasno je da se razlikuju i propisi koji važe u odgovarajućem pravnom procesu, kao i u samoj proceduri iznošenja digitalnih dokaza u formi dokaznog materijala, prihvacenog i prepoznatog od strane suda. Propisi koji regulišu ovaj segment kriminalističke istrage u stalmu su zaostatku za razvojem tehnologije. Ovakav odnos je prirodno stanje koje će u budućnosti stvoriti i veće razlike, a samim tim, i uzrokovati veće probleme. Pravna nauka je, po prirodi stvari, rigidna kategorija, dok tehnologija konstantno napreduje. Primena naprednih tehnologija doživjava eksponencijalni rast, čak i u tehnološki zaostalim sredinama poput Srbije. Na ovaj način, mnoge zloupotrebe ostaju u domenu nevidljivih za pravosudni sistem.[20]

Iako je Srbija među prvim zemljama u svoje zakone uvrstila i zakon o visokotehnološkom kriminalu, još uvek ne postoji institucija u kojoj je moguće obavljati delatnosti kompjuterske forenzike, a i proces verifikacije eksperata diskutabilno bi mogao biti rešen u okviru postojećih institucija. Sve što se radi a vezano je za digitalnu forenziku, radi se pre svega u kompaniji Data Solutions koja se nalazi u Beogradu, Kragujevcu i Novom Sadu. Oni rade na polju digitalne forenzike od 2001. godine a spadaju u privatne istražiteljske agencije⁴⁶.

Ako prihvatomo, da je kompjuterska forenzika disciplina koja ima za cilj da prikupi, sačuva i prezentuje podatke koji su dobijeni sa medija za čuvanje podataka (hard disk, CD ROM, DVD ROM, disketa, USB stik itd.). Kombinujući elemente prava i kompjuterske nauke sakuplja i analizira podatke koji se dalje koriste kao dokazi na sudu, neophodno je i da je prati odgovarajuća zakonska regulativa.[21].

Nažlost, u Srbiji, zakonska regulativa ne priznaje informacioni kriminalitet kao posebni oblik kriminaliteta niti ga sankcioniše. Kao dva najtipičnija primera mogu se navesti krađa iznosa od oko 20.000 DEM sa računa kreditnih kartica i isplata sume u gotovini preko strane banke, te DOS napad na servere tada najpopularnijeg internet sajta na srpskom jeziku (www.serbiancafe.com), tj. mogućnosti za korišćenje IRC-a čime je prekinuta komunikacija između hiljada naših građana kako u Srbiji tako i u inostranstvu, a preduzeću "PTT Srbija - Internet" nanesena milionska šteta zbog prekida u pružanju usluga internet pristupa. U oblasti borbe protiv visokotehnološkog kriminala u Srbiji najznačajniji pomak učinjen je osnivanjem specijalizovanih organa na nivou policije, tužilaštva i suda. Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji je stupio na pravnu snagu 25. jula 2005. godine, osnovano je Posebno tužilaštvo u okviru Okružnog javnog tužilaštva u Beogradu, posebno sudska odeljenje u Okružnom sudu u Beogradu i specijalizovana policijska jedinica pri Službi za borbu protiv organizovanog kriminala.[22]

Mesna nadležnost navedenih specijalizovanih organa uspostavljena je na celoj teritoriji Republike Srbije, dok je stvarna nadležnost propisana članom 3. navedenog zakona i odnosi se na krivična dela protiv bezbednosti računarskih podataka propisanih Krivičnim zakonom (glava 27.) kao i na krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili

⁴⁶. Inače, jedna od najpoznatijih svetskih privatnih agencija u sferi kompjuterske forenzike je američka agencija "Guidance Software". Ovu agenciju osnovala je grupa bivših policijaca, kompjuterskih forenzičara, a njihove sisteme danas koristi oko 90 odsto svih američkih istražitelja i brojne vladine i vojne ustanove. Uz to, Guidance Software godišnje trenira više od 6000 osoba koje rade u preduzećima, u pravosudnim i vladinim organima. Zanimanje digitalni forenzičar je ubedljivo najpopularnije u SAD gde se i pojavilo još krajem osamdesetih godina.

elektronskom obliku, ako je broj autorskih dela veći od 500 ili nastala materijalna šteta prelazi iznos od 850 000 dinara.[23]

Navedenim zakonskim propisom stvarna nadležnost posebnog tužilaštva je postavljena suviše „usko“, odnosno da pojedina krivična dela koja bi po svojoj prirodi trebalo da se nalaze u nadležnosti specijalizovanog organa gonjenja ostaju van njegovog domaćaja. Konkretno, radi se o krivičnom delu prikazivanje pornografskog materijala i iskorišćavanje dece za pornografiju i krivičnom delu falsifikovanje i zloupotreba platnih kartica.

Ukoliko se uzmu u obzir elementi počinilaca ovih krivičnih dela i mogući načini njihovog izvršenja - da se distribucija sadržaja uglavnom vrši preko Interneta kao i da su pribavljanje relevantnih identifikacionih podataka za izradu lažne platne kartice, kao i sama izrada i korišćenje, nezamislivi bez upotrebe specifičnih elektronskih uređaja i programa koji po svojoj prirodi i nameni jesu računari i računarski programi - vidi se da je veliki propust učinjen činjenicom da se krivično gonjenje učinilaca ovakvih krivičnih dela i dalje nalazi u okviru organa gonjenja opšte nadležnosti. Rešenja drugih zemalja koja regulišu ovu oblast su mnogo stroža i vode računa o prirodi ovih krivičnih dela, društvenoj opasnosti koju predstavljaju i zaštitnom objektu, pri čemu je i samo posedovanje ovakvih materijala krivično delo, a kao pozitivan primer može se uzeti Norveška čija regulativa je otišla korak dalje i sankcioniše i samo pristupanje Internet sajtovima sa ovakvim sadržajem. Većina slučajeva iz oblasti klasičnog kriminala takođe se može istraživati alatima digitalne forenzike. Mejlovi, Fejsbuk, kao i mobilni telefoni i drugi uređaji koji se koriste za komunikaciju mogu da posluže kao sredstvo za dogovaranje krivičnog dela.

ZAKLJUČAK

Suočeni smo sa činjenicom da su digitalni dokazi sve zastupljeniji u kriminalnim istragama i da je značaj izvora digitalnih dokaza kao što su mobilni telefoni veliki. Zato je neophodno, kroz operativno povezivanje svih učesnika u procesu prikupljanja podataka, konkretizovati probleme koji sprečavaju prikupljanje relevantnih podataka I dokaza, iste prevazići primenom raspoloživih alata i izborom odgovarajućih principa i metoda za svaki konkretan slučaj. Iako ceo postupak pribavljanja podataka sa mobilnih telefona nije normativno regulisan, postupanjem po propisima iz ZKP-a vezanim za privremeno oduzimanje predmeta, zatim poštovanjem načela kriminalistike i principa forenzike moguće je obezbediti dokazni kredibilitet tako prikupljenih podataka, što je i krajnji cilj. Odnosno saglasiti se sa „The Scientific Working Group on Digital Evidence“ koja smatra da neki objekat postaje dokaz kada je priznat od strane suda i prikupljen na legalan i zakonit način.

Zato je I potrebno da, pre prihvatanja digitalnih dokaza, sud proveri da li su ti dokazi relevantni, autentični, takođe se proverava da li predstavljaju originalne dokaze ili kopije. Najbolji dokaz u kriminalnom postupku je originalan dokaz. I na kraju, ali ništa manje bitno, forenzički stručnjaci, kako bi uspeli da izvuku najviše iz digitalnih dokaza, moraju da razumeju i pravilno upotrebe naučne metode. Naučne metode zajedno sa digitalnim forenzičkim metodama i tehnikama omogućavaju prilagodljivost različitim događajima i zahtevima, a osiguravaju da se zaključci donose zasnovani na činjenicama. Poznavanje ograničenja forenzičke analize digitalnih dokaza pomoći će istražiteljima i advokatima da uhapse moderne kriminalce i oslobode nevine. Odnosno, celokupni pravni sistem ogleda se u pravičnom vođenju krivičnog postupka tako da нико невин не буде осуђен, a да се учиниоцу krivičnog dela izrekne krivična sankcija под uslovima predviđenim Krivičnim zakonom i na osnovu zakonito sprovedenog postupka. U smislu digitalnih dokaza, koji će u narednom periodu predstavljati najrealniji izvor činjenica, trenutno ne postoji mogućnost da se tvrdnja montiranog procesa opovrgne, kao ni то, на основу садашњих zakonskih rešenja, да се заhtev за nepristrasnom analizom ili superveštačenjem uopšte sproveđe.

LITERATURA

- [1] http://en.wikipedia.org/wiki/Digital_forensics
- [2] Seminar o Cyber terorizmu – „Krise i krizno upravljanje“, Hrvatska, 27.03.2012.
- [3] http://sr.wikipedia.org/sr/digitalna_forenzika_i_alati
- [4] Palmer, G., “A road map for digital forensic research”, Technical report, First Digital Forensic Research Workshop, 2001.

- [5] Jansen W., Ayers R., "Guidelines on Cell Phone Forensics", National Institute of Standards and Technology, U.S. Department of Commerce, 2007
- [6] http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-19.pdf
- [7] Jansen W., Ayers R., "Guidelines on Cell Phone Forensics", National Institute of Standards and Technology, U.S. Department of Commerce, 2007
- [8] Vacca, J.R., "Computer Forensics: Computer Crime Scene Investigation", Charles River Media, INC., Hingham, Massachusetts, 2002.
- [9] Casey, E., "Digital evidence and computer crime: forensic science, computers, and the Internet", 2nd edition, Academic Press, London, 2004
- [10] Aleksić, Ž., Škulić, M., „Kriminalistika”, Dosije, Beograd, 2002.
- [11] http://news.bbc.co.uk/2/hi/uk_news/3303637.stm
- [12] Rogers M., "A Practical Approach to Digital Crime Scene Analysis", Department of Computer Technology, Purdue University, 2006
- [13] Jansen W., Ayers R., "Guidelines on Cell Phone Forensics", National Institute of Standards and Technology, U.S. Department of Commerce, 2007
- [14] Willassen S., "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence, 2003
- [15] <http://pcpress.rs/digitalna-forenzika-otkriva-kriminalce/>
- [16] Ayers, R., Jansen, W., Cilleros, N., Daniellou, R., "Cell phone forensic tools: An overview and analysis", National Institute of Standards and Technology, Gaithersburg, Maryland 2005.
- [17] Carrier, B., "Open source digital forensic tools – the legal argument", Research report, At Stake, 2002
- [18] Volonino, L., Anzaldua, R., Computer Forensics, Wiley publishing inc.2008
- [19] Mokhonoana P., Olivier M., Acquisition of a Symbian smart phone's content with an on-phone forensic tool , September 2007.
- [20] <http://www.datasolutions.rs/srp/osnove-digitalne-forenzike/zakonska-regulativa-kompjuterske-forenzike>
- [21] <http://www.datasolutions.rs/srp/kompjuterska-forenzika/kompjuterska-forenzika-osnove.htm>
- [22] Krivični zakonik Republike Srbije, Službeni glasnik RS, br.85/05, 88/05 i 107/05.
- [23] Zakon o posebnim ovlašćenjima radi zaštite prava intelektualne svojine, Službeni glasnik RS, broj 46/06.

NAJPOZNATIJE VRSTE CYBER KRIMINALA (PHISHING, BRUTEFORING, KEYLOGGING, DoS ATTACK, SQL INJECTION) I NAJBOLJA ZAŠTITA OD NAVEDENIH NAPADA

Nehad Gaši, BA

Sveučilište/Univerzitet „VITEZ“ Vitez, nehad.gasi@unvi.edu.ba

Apstrakt: U ovom radu opisano je šta je cyber kriminal i koje su najpoznatije vrste cyber kriminala koje su danas zastupljene, odnosno koje cyber osobe (hakeri) najčešće koriste kako bi došli do svog cilja. Također su opisane i najbolje zaštite od navedenih napada, kako privatnih korisnika, tako i poslovnih korisnika odnosno firmi koje imaju svoju vlastitu mrežu unutar svoje firme koju koriste u svom poslovanju.

Ključne riječi: cyber kriminal, hakeri, hakiranje, phising, DoS attack, zaštita, firewall

UVOD

Od pojave prvih oblika kompjuterskog kriminala do njegovog kakvog-takvog definisanja prošlo je mnogo godina, a odmah zatim pojavio se novi fenomen kriminala - cyber kriminal. Sve učestaliji vidovi i načini zloupotrebe kompjutera podstakli su naučnu i stručnu javnost da se pozabavi ovim oblikom kriminalnog ponašanja. Ipak, ne postoji opšteprihvaćena definicija cyber kriminala. Naime, teškoće u definisanju cyber kriminala proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može obuhvatiti jednom definicijom. Treba razlikovati kompjuterski od cyber kriminala. Kompjuterski kriminal obuhvata zločine počinjene nad računarom, materijalima sadržanim u njemu (softver i podaci) i računar se koristi kao sredstvo ili cilj izvršenja krivičnih djela. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoć u izvršenju prevara. Tu spadaju hakerisanje, napad ometanja servisa, neovlašćeno korišćenje podataka i cyber vandalizam. Cyber kriminal opisuje kriminalne aktivnosti koje su počinjene korišćenjem elektronskih komunikacionih medija. U najširem smislu, Cyber criminal je svaka kriminalna delatnost koja se vrši uz upotrebu računara i računarskih sistema i mreža. Kod cyber kriminala kompjuterske mreže pojavljuju se u nekoliko osnovnih uloga i to kao:

1. Cilj napada – napadaju se servisi, funkcije i sadržaji koji se nalaze na mreži. Kradu se usluge, podaci ili identitet, oštećuju se ili uništavaju djelovi ili cjela mreža i kompjuterski sistemi, ili se ometaju funkcije njihovog rada. Svakako cilj počinilaca (hakera) je mreža u koju se ubacuju virusi ili crvi, te se vrše kriminalne radnje nanoseći tako velike štete.
2. Alat –kriminalci su od pamтивjeka koristili razna oružja i oruđa u činjenju kriminalnih djela i tako “prljali” ruke, dok današnji moderni kriminalci ne “prljaju” ruke koristeći kompjutersku mrežu u činjenju svojih kriminalnih djela. Nekada ova upotreba mreže predstavlja potpuno novi alat, dok se u drugim prilikama već postojeći toliko usavršava da ga je teško i prepoznati. Korišćenje ovog novog alata naročito je popularno kod dječje pornografije, zloupotreba intelektualne svojine ili online prodaje nedozvoljene robe (droge, ljudskih organa, djece, oružja i sl.).
3. Okruženje - Najčešće okruženje u kome se realizuju napadi služi za prikrivanje kriminalnih radnji, kao što je slučaj sa pedofilima, ali ni drugi sajber kriminalci nisu ništa manje uspješni u korištenju okruženja.
4. Dokaz - kao što se u klasičnom kriminalu pojavljuje nož, otrov, pištolj ili neko drugo sredstvo izvršenja djela, tako se i kompjuterska mreža i IKT koriste u dokaznom postupku za cyber kriminal.

Hakeri crni šeširi najobičniji su kriminalci, o kojima se može čitati u novinskim člancima kao o hakerima koji su ukrali, provalili ili uništili. Bijeli šeširi su hakeri o kojima se rijetko može čitati u novinskim člancima. To su hakeri koji svoja znanja koriste kako bi zaštitili računala i mreže od crnih šešira i spriječili njihove aktivnosti ili u najgorem slučaju minimizirali štetu koju su crni šeširi sposobni počiniti. Sivi šeširi su, najjednostavnije rečeno, pokajnici, nekadašnji crni šeširi koji su se preobratili i prešli s tamne strane na svijetu ili igraju za obje momčadi. Etički haker i pojam penetration tester često se koriste za opisivanje iste osobe - IT stručnjaka koji raspolaže znanjima i alatima koje koriste oni na svijetloj, kao i oni na tamnoj strani, ali naravno, ne da se zavesti primamljivim ponudama koje pristižu s tamne strane. U većini slučajeva sve što napadač mora učiniti je pokrenuti program i pričekati da odradi svoj posao. Napadač koji nema pisano dopuštenje da napadne određena računala i mreže najobičniji je kriminalac i lopov te ga kao takvog treba i tretirati. Riječ koja se koristi za takav tip kriminala je cyber-kriminal.

1. CYBER KRIMINAL PREMA TIPOVIMA

a) Politički :

- cyber špijunaža;
- haking;
- cyber sabotaža;
- cyber terorizam;
- cyber ratovanje.

b) Ekonomski:

- cyber prevare;
- haking;
- krađa Internet usluga i vremena;
- piratstvo softvera, mikročipova i baza podataka;
- cyber industrijska špijunaža;
- prevare Internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti).

c) Proizvodnja i distribucija nedozvoljenih i štetnih sadržaja:

- dečija pornografija;
- pedofilija;
- vjerske sekte;
- širenje rasističkih, nacističkih i sličnih ideja i stavova;
- zloupotreba žena i dece.
- Manipulacija zabranjenim proizvodima, supstancama i robama:
- drogom;
- ljudskim organima;
- oružjem.

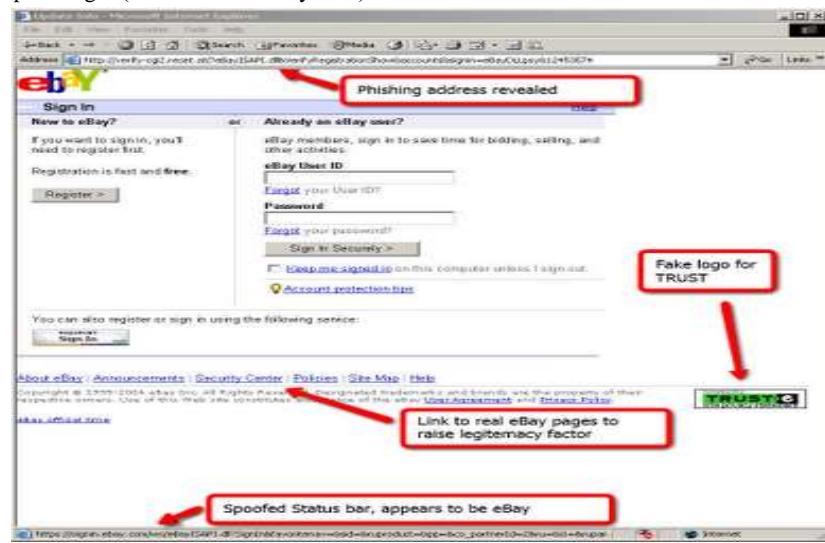
d) Povrede cyber privatnosti:

- nadgledanje e-pošte;
- spam
- phiching
- prisluškivanje
- praćenje e-konferencija
- prikačinjanje i analiza "cookies".

2. PHISHING

Phishing ili mrežna krađa identiteta, vrsta je prevare putem elektroničke pošte odnosno elektroničke poruke. Pošiljatelj navodi žrtvu otkriti osobne informacije (obično finansijske) upisivanjem istih na lažiranoj internetskoj stranici čija je poveznica dana u poruci. Adresa i sadržaj te lažirane stranice vrlo su slični adresi i sadržaju neke stranice. Odatle i engleski naziv "phishing" koji je iskrivljeni oblik riječi "fishing" (engl. pecanje) - obje riječi se izgovaraju isto iako se pišu različito. Phishing se može iskoristiti tako da se osobi ukrade novac ili nanese neka druga šteta (primjerice, provala u žrtvin račun elektroničke pošte). Poruka može izgledati kao obavijest iz banke, internetske trgovine i sl., te se žrtvu navodi kliknuti na poveznicu koja je "udica" na kojoj počinitelj internetskog zločina izvlači tražene podatke od žrtava. Žrtve potom na njoj upišu osobne informacije (u poruci se često navodi da korisnik treba potvrditi ili promijeniti podatke). Kad korisnik upiše podatke na lažiranoj stranici, informacije dolaze do vlasnika lažirane stranice. Lažna internetska stranica izgleda skoro identično autentičnoj stranici, ali je URL u adresnoj traci drukčiji. Korisniku koji je postao žrtva krađe identiteta može pomoći ako promijeni lozinku ili PIN za pristup na svoj korisnički odnosno bankarski račun ili u krajnjem slučaju da zatvori račun kod davaljelja usluge.

Slika 1: Primjer phishing-a (lažna stranica ebay.com)

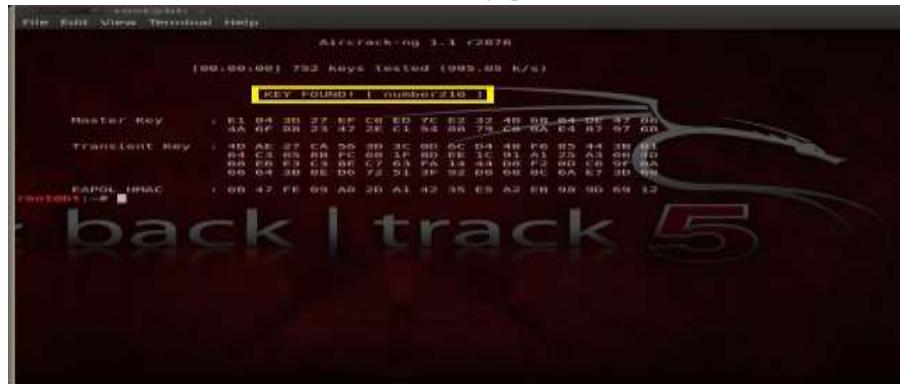


Izvor: http://3.bp.blogspot.com/-u9ryHYjZz1Q/Tt14fPAXKXI/AAAAAAAUAU/Ale_OENiE08/s1600/PhiExample3_Site.png

3. BRUTEFORsing

Kraker je osoba koja se bavi krakovanjem (razbijanjem zaštitnog koda). U pitanju su lozinke za ulazak u zaštitene informacione sisteme kao što su banke, bolnice, policija i sl. ili kodovi koji štite softver i druge intelektualne svojine od nelegalnog kopiranja. Pojavom ličnih računara i Interneta, otvorena je mogućnost nelegalnog ulaska u tuđe sisteme, a zatim i zloupotreba istih. Na primer, kupovina preko Interneta korištenjem tuđih krakovanih kreditnih kartica. Krakeri odigravaju značajnu ulogu probijanja zaštita sa softvera koje većina ljudi nemože da kupi. Zahvaljujući krakerima, u Srbiji je razvijeno značajno piratsko tržiste jeftinih, nelegalnih kopija softvera, filmova, igrica. Krakeri vrše napade koristeći razne metode naprednog programiranja, ali u posljednje vrijeme sve više njih koriste programe koji sami vrše napade, ne znajući uopšte ni kako radi takav jedan program. Neke od metoda su ubacivanje koda, prenatrpavanje bafera, korupcija memorije itd.

Slika 2: Krekovanje password

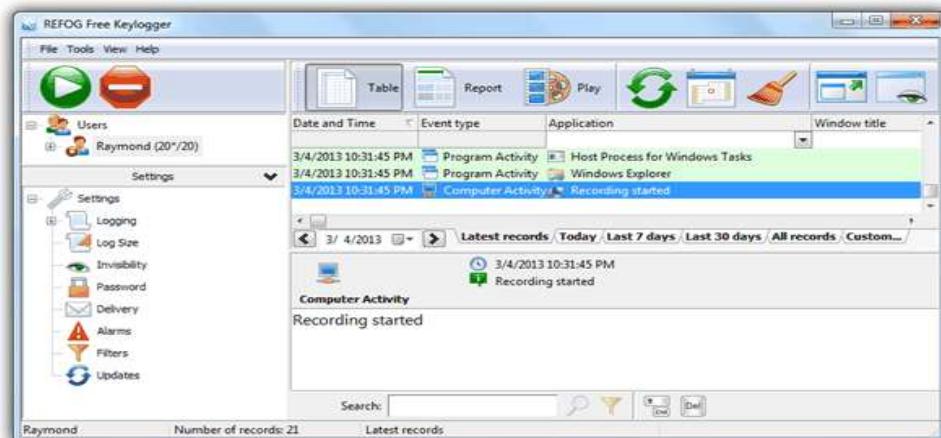


Izvor: http://s20.postimg.org/gpb3czzfx/6th_command.png

4. KEYLOGGER

Keylogger je maliciozni program kojem je cilj praćenje korisnikovih unosa preko tipkovnice. Pojedini bezopasni, legitimni programi koriste neke njegove funkcije za pozivanje specijalnih programske funkcija (*hotkeys*). Povremeno keylogger namjerno instalira neka osoba na računalo ili više računala kako bi mogla tajno pratiti druge korisnike (npr. roditelji kako bi pratili kako djeca koriste računalo dok su roditelji, primjerice, na poslu). Osim te osnovne funkcije keylogger može s vremenom na vrijeme (ili na svaki korisnikov klik miša) uzimati snimak ekrana tako da se na njemu može vidjeti, između ostalog s kojim programima korisnik trenutno radi ili gdje surfa na Internetu. Ponekad je nevidljiv u upravitelju zadataka (*Task manager*) koji prikazuje procese koji se trenutno izvode na računalu kako bi spriječio ili otežao mogućnost otkrivanja od strane korisnika. Informacije koje keylogger prikupi u većini slučajeva šalju se zlonamjernoj osobi.

Slika 3: Izgled keylogger programa

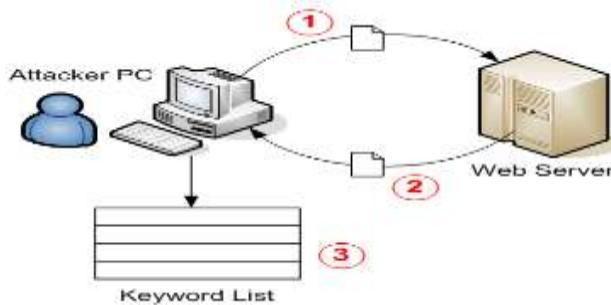


Izvor: <https://bd23.https.cdn.softlayer.net/80BD23/142.4.51.106/images/refog-free-keylogger.png>

5. SQL INJECTION

SQL injekcija (engl. *SQL injection*) je tehnika koja eksplloatira sigurnosnu ranjivost koja se događa u sloju baze podataka aplikacije. Najčešće se eksplloatiraju web aplikacije koje u svojim SQL upitim koriste podatke koje je isporučio korisnik, ali bez prethodnog ispitivanja da li ti isti korisnički podaci sadrže neke potenijalno štetne znakove poput navodnika, točke-zarez i sl. SQL injekcija je tehnika koja se sastoji od upisivanja odgovarajućeg teksta u polja obrasca koja aplikacija koristi u svojim SQL upitim, tako da upiti iz baze vrate podatke koje inače ne bi. Ova metoda, kao i većina hakerskih postupaka, počiva na metodi pokušaja i pogrešaka i temelji se na pogadanju strukture SQL upita i imena atributa i tablica.

Slika 4: Šema SQL injekcije (napad na bazu podataka pomoću SQL naredbi)



Izvor : http://4.bp.blogspot.com/_6Y3t2XpO2oE/TSBDvjrbox-I/AAAAAAAABa0/seNNJLWHGO0/s400/concept_sqlinjection_smaller.png

6. DoS NAPADI

DoS ili DDoS (engl. Distributed Denial of service) napad je pokušaj napadača da učini računar nedostupnim korisnicima kojima je on namjenjen. DoS napad onesposobljava mrežu, računar ili neki drugi dio infrastrukture na taj način da ih korisnici ne mogu koristiti. Većina DoS napada na internetu spada u jednu od sljedeće tri vrste:

- 1) Napad na ranjive djelove mreže – slanje nekoliko poruka na ranjive aplikacije ili operativne sisteme koji se izvršavaju na računaru koji je meta napada i na taj način određena usluga prestaje sa radom
- 2) Zakrčenje propusnog opsega – pristupni link napadnutog računara postaje zagušen od paketa kojima napadač preplavljuje napadnuti računar čime se sprječava da pravi paketi dospiju na odgovarajući server.
- 3) Plavljenje vezama – napadač uspostavlja veliki broj poluotvorenih ili potpuno otvorenih TCP veza na računaru koji je meta napada i na taj način računar postaje prezauzet lažnim vezama do te mjere da prestaje da prihvata ispravne veze

Iako djeluje kao da iza DDoS-a stoji grupa ljudi sa željom da onesposobi ciljani računar, istina je da je to u najvećem broju slučajeva jedan zlonamjerni korisnik koji traži druge korisnike na Internetu preko kojih vrši napade, a da oni toga nisu ni svjesni. Dakle, zločinac traži ranjive sisteme na Internetu (one koji imaju poznate sigurnosne propuste, nemaju ažurirane antivirusne programe ili ih uopšte nemaju), a kada ih pronađe, na svakom od njih obavlja dodatne korake, obično ovim ili sličnim redom:

- 1) Instaliranje programa kako bi se prikrila provala sistema i svih narednih aktivnosti na tom sistemu (na primjer, nemoguće je vidjeti proces napadača u spisku pokrenutih programa na ranjenom računaru)
- 2) Instaliranje procesa za udaljenu kontrolu računara koji prima naredbe napadača i pokreće napade putem Interneta prema određenoj žrtvi.

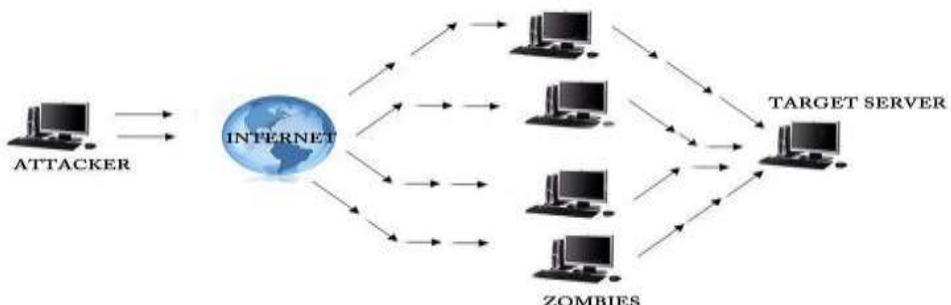
Rezultat ovog automatizovanog procesa je stvaranje mreže (botnet) koju čine zaraženi računari (deamoni, botovi) koji su spremni da prime naredbe napadača (mastera) i ne obavještavajući svog vlasnika učestvuju u DDoS napadu. Učestalo pojavljivanje DDoS napada, njihova snaga i opasnost koju sa sobom donose su uticali na doношење mnogobrojnih mehanizama zaštite. Uprkos tome, DDoS su i dalje prava prijetnja mrežnim administratorima jer i dalje ne postoji sigurna zaštita zato što je nemoguće imati tako koordinisan sistem odbrane koji će reagovati na nepoznati i veoma dobro koordinisan sistem napada. Kako bi sa velikom sigurnošću DDoS napad bio spriječen, potrebno je da web sajt bude distribuiran preko više servera. Na taj način bi, padom jednog servera, web stranica bila dostupna preko drugih na kojima je distribuirana. Podrazumjeva se konstantno nadgledanje cjelokupne mrežne infrastrukture na svim nivoima referentnog modela i najbrže moguće reagovanje i na najmanju moguću opasnost po infrastrukturu posmatrane mreže.

Pored reaktivnog sprečavanja DDoS napada, potrebno je stalno sprovoditi i preventivne mjere zaštite koje sigurno doprinose da računar ne postane dio botnet-a, a to su:

- 1) Pravljenje popisa pokrenutih procesa na serveru, kao i popisa mrežnih priključaka preko kojih se obavljaju usluge.
- 2) Onemogućiti sve procese osim onih koji su potrebni za normalan rad servera
- 3) Uvesti filtriranje paketa (npr. pomoću programa IP Filter).

Filtriranje paketa ima nekoliko izuzetno važnih funkcija kao što su: onemogućavanje lažiranja izvorne adrese, blokiranje paketa koji dolaze s nepoznatih adresa kao i osiguranje nadzora nad uslugama (definisati prava pristupa pojedinog korisnika uslugama). Pored softverske zaštite koja se nalazi na aplikacionom sloju referentnog modela, postoji još bitnija zaštita na nižim slojevima mreže. Ruteri i svičevi mogu biti konfigurisani tako da skeniraju pakete (provjera IP adrese, porta) prije ulaska u transportni i aplikacioni sloj. Takođe, time se osigurava mreža nekog preduzeća kao potencijalnog izvora DDoS napada. Još jedan način zaštite je korišćenje zaštitnog zida (engl. firewall), koji radi na sličan način kao i usmjerivači za filtriranje prometa.

Slika 5: DDoS napad



Izvor: <http://www.satoconor.com/Portals/0/thinclient2.jpg>

Slika 6: Hakerski program za napad i obaranje web stranica



Izvor: <http://images62.fotosik.pl/53/1a6cab33bb088f58med.jpg>

7. ZAŠTITA OD CYBER NAPADA – FIREWALL

Vatrozid (engl. Firewall) je mrežni uređaj čija je namjena filtriranje mrežnog prometa tako da se stvori sigurnosna zona. Program koji želi pristupiti Internetu treba imati dopuštenje od vatrozida. Obično se kombiniraju usmjernici i sigurnosne stijene, kao jedan uređaj, ili se kaskadiraju, npr. unutarnja (osigurana) mreža - sigurnosna stijena - usmjernik - vanjski svijet. Vatrozid može biti programska i sklopovska, sa širokom dostupnošću Interneta 24 sata dnevno postale su popularne osobne sigurnosne stijene koji štite jedno računalo od upada zlonamjernih osoba, dok je posebno računalo koje radi samo

kao sigurnosna stijena/usmjernik uglavnom rješenje koje se primjenjuje kad se štiti više od jednog računala.

Sklopovska sigurnosna stijena je također računalo, ali obično bez tvrdog diska, grafičke kartice, sastoji se obično od procesora, memorije i EPROMa (sabirnice, mrežni/paralelni portovi se podrazumijevaju). Danas ih klasificiramo u 4 grupe, obzirom na kojoj razini modela OSI “djeluju”.

1. filtriranje paketa
2. sigurnosne stijene na transportnom sloju
3. sigurnosne stijene na aplikacijskom sloju (proxies)
4. sigurnosne stijene s višeslojnim ispitivanjem paketa

7.1. Sonicwall

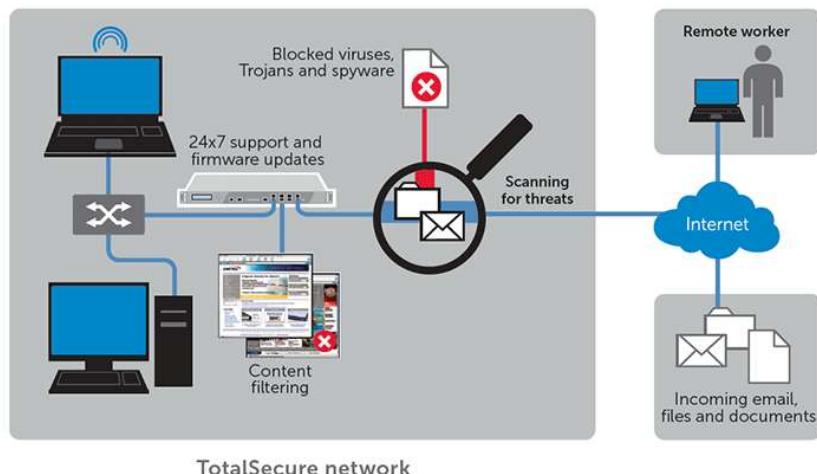
SonicWall prvobitno privatna kompanija sa sjedištem u San Jose, Kalifornija, a sada u vlasništvu Dell, prodaje niz Internet opreme prvenstveno usmjerena na sadržaj za kontrolu i sigurnost mreže. To uključuje uređaje za pružanje usluga mreže, firewall, UTM I VPN , backup i oporavak, i anti-spam za e-poštu.

Slika 7: Izgled Dell-ovog firewall-a SonicWall



Izvor: <http://cdn.firewalls.com/media/wysiwyg/firewalls/nsa-2600-high-res.png>

Slika 8: Provjera dolazećih podataka i email poruka uz pomoć SonicWall-a



Izvor:

<https://www.google.ba/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=&url=http%3A%2F%2Fwww.sonicguard.com%2FComprehensive-Gateway-Security-Suite.asp&psig=AFQjCNFP1-ANhY5uVPAiALIHKt3STvZxAA&ust=1456387022406272>

IDENTIFIKACIJA I PREVENCIJA POJAVNIH OBLIKA NASILJA MEĐU DJECOM U SREDNJIM ŠKOLAMA NA PODRUČJU OPĆINE TRAVNIK

Mr Adnan Pirić¹, Mr Almira Salkić², Selim Hibić dipl krim³

¹Viši asistent Fakultet pravnih nauka - Sveučilišta/Univerziteta „Vitez“ u Vitezu

²Viši asistent Fakultet informacijskih tehnologija – Sveučilište/Univerzitet „Vitez“ u Vitezu

³Predsjednik udruženja kriminalista SBK/KSB Travnik

Apstrakt: Nasilje među djecom obuhvata širok spektar agresivnih ponašanja koja se događaju prvenstveno u školama, počevši od rješavanja manjih sukoba nasilnim putem, zatim neprihvatljivog izražavanja ljutnje ili frustracije, do ozbiljnih incidenata uz upotrebu oružja. Nasilništvo karakterišu, namjera da se drugi povrijedi, ponavljanje ustaljenog obrasca ponašanja u kojem je uvijek jedna strana žrtva a druga nasilnik, te očita neuravnoteženost snaga među njima. Nasilje među vršnjacima, posebno u školama, nije nova pojавa kako u svijetu, pa tako i u školama Bosne i Hercegovine. Problem nasilja ima veoma široke implikacije, jer zadire i u temeljna demokratska načela u kojima je jasno navedeno da svaki pojedinac mora raspolagati pravom da bude pošteden ugnjetavanja i namjernog ponižavanja u školi, kao i u društvu u cjelini. U današnje vrijeme, pod uticajem različitih faktora iz okoline, prije svega uticaja informacionih tehnologija, odgoj djece, kao jedan od najvažnijih ciljeva svakog društva, našao se u krizi, kako u školi, tako i u porodici. Zapostavljene su temeljne norme ponašanja i agresivnost i nasilje su sve više prisutni u međusobnoj komunikaciji između odraslih i djece, ali i među samom djecom. Postoji tendencija općeg neprihvatanja različitosti među djecom, što dovodi do povlačenja djece u sebe. Zbog toga se mnoga od njih, unatoč svojim potencijalima, često nalaze na margini školskih aktivnosti. Svako ko radi na području obrazovanja zna da su obrazovni ciljevi oduvijek bili vrlo zahtjevni i visoki, a školska stvarnost strogo normirana i kruta, odnosno to još uvijek jeste. Poseban problem u današnje vrijeme stvara zloupotreba internet, odnosno informacionih tehnologija, putem kojih se javljaju razni oblici vršnjačkog nasilja, što dodatno stvara problem prevencije i kontrole istog.

Ključne riječi: Prevencija, oblici nasilja, srednje škole na području općine Travnik.

UVOD

Da bi se moglo pristupiti obradi teme ovog rada, neophodno je istražiti temeljne aspekte o pojavnim oblicima vršnjačkog nasilja među djecom u srednjim školama na području općine Travnik, njegovim učiniocima, načinima učinjenja, i načinima prevencije, odnosno suzbijanja ove pojave, a posebno onih koji su predmet ovog rada. Potrebno je u prvom djelu, uvodu posebnu pažnju posvetiti metodološkim tematskim jedinicama: 1) problemu, predmetu i objektu rada, 2) glavnoj i pomoćnim hipotezama, 3) svrsi i cilju rada, 4) naučnim metodama i 5) strukturi rada.

Problem, predmet i objekt rada

Objašnjavanje o osnovnim pojmovima nastanka pojavnih oblika vršnjačkog nasilja među djecom u srednjim školama, uz pomoć teorijskih praktičnih i drugih doprinosova, sociologije kriminologije i kriminalistike kao nauka u najkonkretnijim vezama sa uzrocima, fenomenima i tehnologijama prevencije i suzbijanja ove društveno negativne pojave, od izuzetnog je značaja za cijelu društvenu zajednicu. Problematizacijom predmeta istraživanja kroz uspostavljanje funkcionalnog kauzaliteta sociološke, kriminološke, i kriminalističke teorije i prakse u vezi sa predmetnom temom smatramo da će dovesti do novog kvalitativnog pomaka u unapređenju efikasnosti prevencije i suzbijanja pojavnih oblika nasilja među djecom u srednjim školama na području općine Travnik.

Tako postavljen **problem** istraživanja determinira i **predmet** istraživanja: Istražiti i naučno utemeljeno prezentovati sve važnije činjenice o pojavnim oblicima vršnjačkog nasilja među djecom u srednjim školama na području općine Travnik. S obzirom na problem i predmet istraživanja, **objekti** istraživanja su srednjoškolci sa području općine Travnik.

Radna i pomoćne hipoteze

U skladu sa problemom, predmetom i objektom rada postavljena je **radna hipoteza**:

“Nasilje među srednjoškolcima na području općine Travnik prisutno je u različitim oblicima.”

Tako postavljena radna hipoteza implicira **pomoćne hipoteze (kraće: P.H.):**

- **PH1:** Srednjoškolci sa područja općine Travnik informisani su o svim pojavnim oblicima nasilja u školi.
- **PH2:** Nasilje nad drugim učenicima u školi vrše njihove školske kolege.
- **PH3:** Učenici koji su žrtve nasilja za pomoć se najčešće obraćaju nastavnicima i drugovima/drugarcama.
- **PH4:** Učenici koji su svjedoci nasilja nad svojim kolegama rijetko sprečavaju sprečavaju nasilje nad svojim kolegama.
- **PH5:** Žrtve nasilja trpe i neuvraćaju nasilnicima na pretrpljeno nasilje.
- **PH6:** Srednjoškolci sa područja općine Travnik ipak u većem broju slučajeva osjećaju sigurno kako u školi tako i na putu od kuće do škole.

Svrha i ciljevi

U vezi sa problemom i predmetom istraživanja, te postavljenom radnom i pomoćnim hipotezama, određena je i **svrha rada:** ukazati na neophodnost prevencije i suzbijanja pojavnih oblika vršnjačkog nasilja u svim srednjim školama na području općine Travnik. **Cilj rada:** ispitati prisutnost nasilja među vršnjacima, pojavne oblike, učestalost nasilja među vršnjacima u srednjim školama, obim nasilja koji se dešava u školama, te informiranost i znanje koje učenici imaju o ovom problemu. Definisati preporuke u cilju prevencije, smanjenja i otklanjanja nasilja među vršnjacima.

Naučne metode

Prilikom pisnja rada koristiće se relevantne naučno - istraživačke metode i tehnike, koje mogu dati najkvalitetnije rezultate u oblasti definisanja navedenih pojava. U tom cilju afirmisaće se standardne, ali i neke specifične metode, primjenjivne za oblast definisanja, kao što su: fokus grupe, analiza scenarija, kompilacija, deskripcija, analiza i sinteza, anketa i intervju.

Struktura rada

Struktura rada postavljena je tako da obradi temu rada sa svih aspekata koji su bitni za istu. Sadržaj rada primjerjen je temi rada, pri čemu će se obraditi uvod u temu, postaviti osnovna i pomoćna hipoteza, obraditi problematika navedene teme, i kroz zaključke ukazati na značaj efikasnosti prevencije i suzbijanja svih oblika vršnjačkog nasilja na području općine Travnik, kao i dati neke prepostavke za unapređenje načina suzbijanja i prevencije navedenog.

1. REZULTATI ISTRAŽIVANJA POJAVNIH OBLIKA NASILJA MEĐU DJECOM U SREDNJIM SKOLAMA NA PODRUČJU OPĆINE TRAVNIK

Pri analizi istraživanja predstavljeni su rezultati anketiranja uenika/ca srednjih škola sa područja općine Travnik.

1.1. Informiranost učenika o vršnjačkom nasilju u školi i pojavnii oblici nasilja

Prvi korak prilikom istraživanja bio je, da li učenici znaju šta je to vršnjačko nasilje, koje vrste nasilja poznaju, odnosno da li u njihovoj školi postoji bilo koji oblik nasilja od strane vršnjaka, kako i da li škola promoviše modele nenasilne komunikacije, kao i pitanje da li i koliko puta ste vi bili izloženi nasilnom ponašanju vaših vršnjaka, kojim oblicima vršnjačkog nasilja ste bili izloženi? U ispitivanju, odnosno anketiranju, učestvovalo je oko 100 učenika/ca srednjih škola sa područja općine Travnik. Sumirani podaci pokazuju da su učenici u 100% slučajeva upoznati sa pojmom vršnjačkog nasilja.

Grafikon 1: Odgovori na anketu „Znate li šta je vršnjačko nasilje?“

Znate li šta je vršnjačko nasilje?

■ DA ■ NE

0%

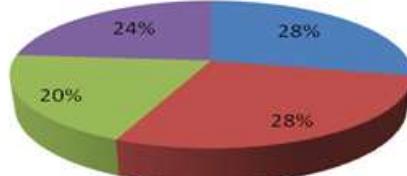
100%

Izvor: Vlastito

Grafikon 2: Odgovori na anketu „Koje vrste vršnjačkog nasilja poznajete?“

Koje vrste vršnjačkog nasilja poznajete?

■ Fizičko ■ Psihičko ■ Seksualno nasilje ■ Cyber nasilje na internetu



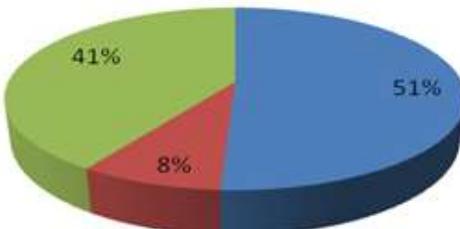
Izvor: Vlastito

Najčešći oblici vršnjačkog nasilja koje učenici poznaju su u 28% slučajeva psihičko i 28% fizičko, zatim 24% cyber nasilje ili nasilje na internetu, te 20% seksualno nasilje.

Grafikon 2: Odgovori na anketu „Koje vrste vršnjačkog nasilja poznajete?“

Da li u vašoj školi postoji bilo koji oblik vršnjačkog nasilja?

■ Da ■ Ne ■ Neznam



Izvor: Vlastito

Po pitanju, da li u vašoj školi postoji bilo koji oblik vršnjačkog nasilja 51% misli DA, dok 8% odgovara sa NE, a 41% ne znam.

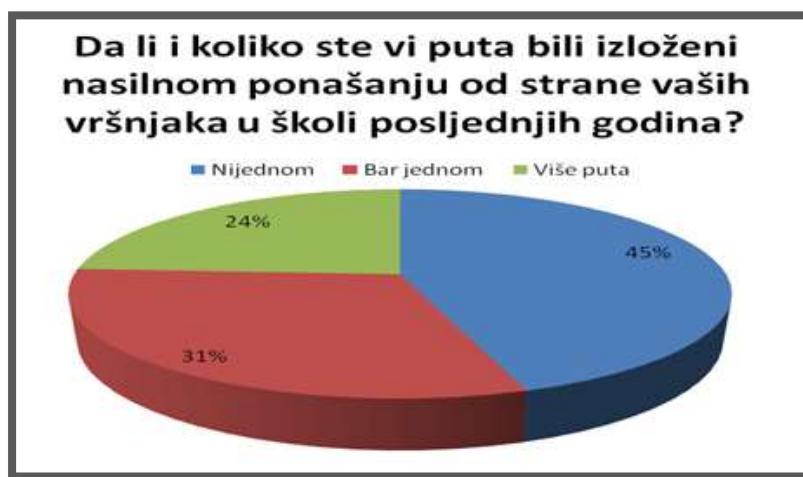
Grafikon 3: Odgovori na anketu „Da li vaša škola promoviše modele nenasilne komunikacije, međusobne tolerancije i uvažavanja?“



Izvor: Vlastito

Koliko škole promovišu modele nenasilne komunikacije, međusobne tolerancije i uvažavanja? Učenici smatraju; 44% da škola to radi ponekad, 31% da škola to radi svakodnevno, i 16% često, a 9% nikako.

Grafikon 4: Odgovori na anketu „Da li i koliko ste vi puta bili izloženi nasilnom ponašanju od strane vaših vršnjaka u školi posljednjih godina?“



Izvor: Vlastito

Da li i koliko puta ste vi bili izloženi nasilnom ponašanju vaših vršnjaka u školi posljednjih godina 45% je izjavilo da nije bilo izloženo vršnjačkom nasilju nijednom, 24% više puta, a 31% bar jednom.

Grafikon 4: Odgovori na anketu „Kojim oblicima vršnjačkog nasilja ste bili izloženi?“



Izvor: Vlastito

Kojim oblicima vršnjačkog nasilja ste bili izloženi? Od ukupnog broja ispitanika 33% je odgovorilo, kako je nazivano pogrdnim imenima i isminjavanju, odnosno 9% bilo je izloženo prijetnjama zastrašivanju, potom 9% udaranju i tući, takođe 9% otimanju novca i sl, a 40% je izjavilo da nije bilo izloženo vršnjačkom nasilju.

1.2. Provodenje nasilja nad učenicima od strane vršnjaka

Obzirom das u rezultati pokazali da postoje pojavnici oblici nasilja među djecom u školama, da djeca poznaju sve vrste nasilja i da se nasilje ispoljavaju u različitim oblicima, potrebno je istražiti, ko su nasilnici, odnosno zlostavljači, na kojim mjestima se dešavaju nasilne situacije, da li su neka djeca češće a druga rijeđe nasilnici, isto tako postavlja se pitanje, da li su neka djeca češće žrtve nasilja svojih vršnjaka, kome se povjeravaju u slučaju nasilja nad njima, kao i da li smatraju da je danas više nasilja nego predhodnih godina?

Grafikon 5: Odgovori na anketu „Kojeg uzrasta su počiniovi vršnjačkog nasilja u vašoj školi?“



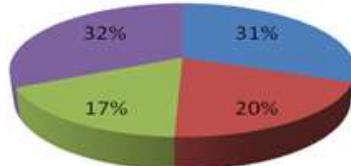
Izvor: Vlastito

Predhodni grafikon, daje nam jasno sliku da su učenici starijih razreda češće počiniovi nasilja 37%, nego učenici mlađih razreda 9%, međutim isto tako vidimo da je mišljenje vršnjaka da je manje bitno da li su to učenici mlađih ili starijih razreda, 54% ispitanika je dalo odgovor podjednako.

Grafikon 6: Odgovori na anketu „Na kojim mjestima se dešavaju nasilne komunikacije?“

Na kojim mjestima u školi se dešavaju nasilne komunikacije?

■ U učionici ■ U školskom dvorištu
■ U školskom toaletu ■ Na nekom drugom mjestu u školi



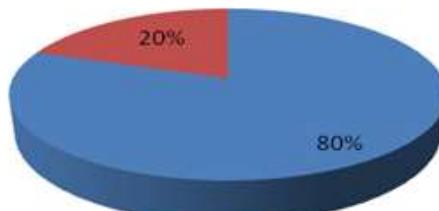
Izvor: Vlastito

Najčešća mjesta na kojima se odvija nasilna komunikacija, odnosno nasilje, su upravo školske učionice 31%, na nekom drugom mjestu 32%, školsko dvorište 20%, a školski toalet 17%.

Grafikon 7: Odgovori na anketu „Da li su neka djeca više puta bila žrtve nasilja od strane vršnjaka?“

Da li su neka djeca viša puta bila žrtve nasilja od strane vršnjaka?

■ DA ■ NE



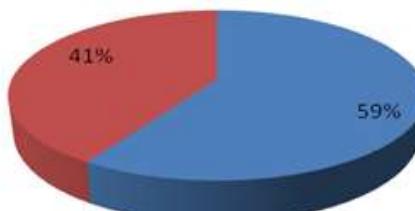
Izvor: Vlastito

Predhodni prikaz nam nedvojbeno daje predstavu, o tome kako su neka djeca vrlo često žrtve nasilja od strane svojih vršnjaka čak 80%.

Grafikon 8: Odgovori na anketu „Da li su neki od vaših vršnjaka više puta bili nasilnici?“

Da li su neki od vaših vršnjaka više puta bili nasilnici?

■ DA ■ NE



Izvor: Vlastito

Vidimo da su neki učenici češće nasilnici, povratnici (recidivisti) u vršenju nasilja nad svojim kolegama u čak 59%.

Grafikon 9: Odgovori na anketu „Ukoliko ste bili izloženi nasilju ili kada biste bili izloženi, kome bi se povjerili?“



Izvor: Vlastito

Povjerenje djece u ovom slučaju najčešće je u roditelja čak 51%, potom u druga ili drugaricu 22%, razrednom strješini 16%, a vrlo pozitivno je što je manji broj onih koji se nebih nikome povjerili 11%.

Grafikon 10: Odgovori na anketu „Da li smatrate da je danas više ili manje nasilja nego proteklih godina?“



Izvor: Vlastito

Učenici srednjih škola sa područja opštine Travnik iznijeli su stav, da je mnogo više nasilja danas nego proteklih godina 70%, a samo 1% je onih koji smatraju da je manje, dok njih 28% smatra podjednako kao i proteklih nekoliko godina.

1.3. Načini reagovanja djece na doživljeno nasilje

Uvažavajući teorijsko definisanje osobina, karakteristika žrtava nasilja, među vršnjacima, istraživanjem je sagledano emocionalno stanje žrtava, obzirom da to stanje diktira njihovo ponašanje, pokušali smo utvrditi prisutnost kolega vršnjaka iz škole prilikom vršenja nasilja nad drugim vršnjacima, potom koliko su kolege vršnjaci i na koji način spremni pomoći svojim kolegama ukoliko su isti žrtve nasilja.

Reagovanje na fizičko i drugo nasilje, isto tako veoma nam je bitno bilo koliko se srednjoškolci mossjećaju sigurnim na putu od kuće do škole, kao i u školi uopšte.

Grafikon 11: Odgovori na anketu „Da li ste bili prisutni dok je neko od vaših kolega bio izložen nasilju?“



Izvor: Vlastito

U 56% slučajeva nasilje se odvijalo u prisustvu ostalih vršnjaka iz škole, dok 44% bez prisustva kolega iz škole.

Grafikon 12: Odgovori na anketu „Ukoliko ste bili prisutni, šta ste učinili, da joj/mu pomognete?“



Izvor: Vlastito

Predhodni prikaz nam daje uvid u donekle zabrinjavajući podatak, a to je da čak 55% učenika ne bi ili nije učinilo ništa učinilo da pomogne kolegi ili kolegici koji su bili žrve nasilja. 27% njih bi ili je pozvalo nekog starijeg u pomoć, a 18% bi se lično obračunalo sa nasilnikom.

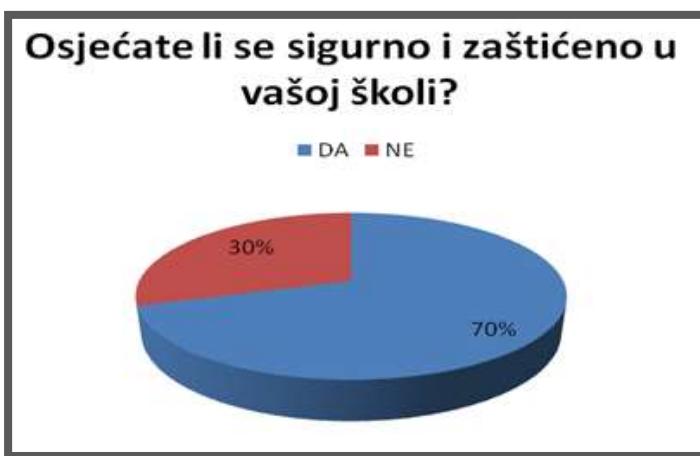
Grafikon 13: Odgovori na anketu „Kako reaguješ na fizičko nasilje?“



Izvor: Vlastito

Što se tiče reakcije učenika na nasilje, 49% učenika izbjegava nasilje, 20% odgovara istom mjerom, 12% ih se plaši, a 19% reaguje nekako drugačije na svoj način, kako to oni kažu.

Grafikon 14: Odgovori na anketu „Osjećate li se sigurno i zaštićeno u vašoj školi?“



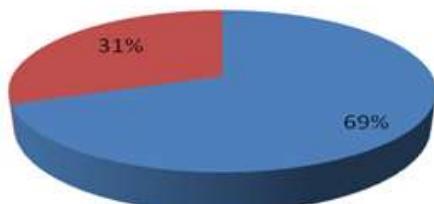
Izvor: Vlastito

Vidimo da se učenici ipak u većem broju 70% osjećaju sigurno i zaštićeno u školi, dok se 30% učenika ne osjeća sigurnim u školi.

Grafikon 14: Odgovori na anketu „Osjećate li se sigurno na putu od kuće do škole?“

Osjećate li se sigurno na putu od kuće do škole?

■ DA ■ NE



Izvor: Vlastito

Što se tiče sigurnosti učenika na putu od kuće do škole, i u tom slučaju se veći broj učenika 69% njih osjeća sigurnim na putu od kuće do škole, dok se njih 31% ne osjeća sigurnim na putu do škole i nazad.

2. ZAKLJUČCI ISTRAŽIVANJA I PREVENCIJA VRŠNJAČKOG NASILJA U SREDNJIM ŠKOLAMA NA PODRUČJU OPĆINE TRAVNIK

Teorija kontrole tvrdi, da se ljudi ponašajući primjerene odriču neodgovarajućeg ponašanja, te da su naša ponašanja duboko unutarnje motivirana, a krajnji im je cilj zadovoljavanje osnovnih tjelesnih i duševnih potreba. Svrha škole je da pomogne djeci da razviju bolje izbor ponašanja u njihovom pokušaju zadovoljavanja osnovnih psiholoških potreba, kao što su; ljubav, pripadanje, moć, sposobnost, sloboda izbora i zabava, koje moraju biti zadovoljene kako bismo bili sretni.⁴⁷ Samo sredina u kojoj se te potrebe neprestano zadovoljavaju potiče optimalan rast i zdrav razvoj ličnosti. Dok nas teorija podražaj – odražaj uči da reagujemo tražeći nagradu ili pak nastojeći izbjegći kaznu, realitetna terapija je primjena načela teorije kontrole, koja nas uči da djelujemo. To je process koji od ljudui zahtjeva da se upitaju i saznaju šta žele i kako da to djelotvornim ponašanjem i ostvare. Čim dijete prizna da je njegovo sadašnje ponašanje neprimjereno i nedjelotvorno, možemo mu pomoći da izabere djelotvorne ponašanje kako bi ostvarilo svoje želje. Poznata je činjenica da se ljudi općenito vrlo teško odriču svog ponašanja, pa je stoga potrebno mnogo truda i upornosti da bih ih se privoljelo na primjenu uvriježenih šabloni i oblika ponašanja, koja su već ukorijenjena u dječiji karakter. Ali ako ih uspijemo uvjeriti da postoji bolji izbor i da će im u tome pomoći, djeca će brzo naučiti da je njihova srča izravan proizvod njihovog odabira, te će odabrati odgovarajuće ponašanje, koje će ih do nje dovesti.⁴⁸

O nasilju među djeecom govorimokad jedno ili više djece uzastopno i namjerno unemiruje, napada, ozljeđuje ili isključuje iz igre i aktivnosti drugo dijete koje se ne može odbraniti. Psihološku pozadinu nasilja otkrivaju osobine djece, kao što su implusivnost i hiperaktivnost, postraumatski sindrom,

⁴⁷ VESTA, Companing for preventing and combating occurrences of bullying in primary schools; „Program mjera za pre prevenciju i suzbijanje pojavnih oblika nasilja među djeecom u osnovnim školama“. Tuzla, oktobar/listopad 2008.godine.p.19

⁴⁸ Ib

nesigurnost u izboru životnog puta, nasilničke scene na ekranima elektronskih medija i internet, sukobi među generacijama i među djecom.⁴⁹

Da naše škole, nisu usamljene u suočavanju sa problemom nasilja među djecom govore i istraživanja provedena u drugim općinama, kantonima u BiH, kao i istraživanja provedena u drugim zemljama svijeta, u kojima se ističe da je postotak školske djece koja su žrtve nasilja u većini zemalja sličan, da se nasilništvo najčešće događa u srednjim školama, ali isto tako da se agresivno ponašanje nauči vrlo rano i da dječaci i djevojčice zastrašuju uglavnom učenike istih spolova, osim ako se radi o seksualnom nasilju.⁵⁰

Iz predstavljenog istraživanja može se zaključiti da je problem vršnjačkog nasilja među djecom prisutan u srednjim školama na području općine Travnik, da zahtjeva brzo djelovanje i efikasne programe prevencije nasilja među djecom, da je pored toga potrebno djelovati na sve aspekte društva, porodice i odgojno – obrazovnog sistema, jer zasigurno neželimo da nesigurnost na ulicama, strah roditelja, ulične bande, prmlaćivanja i ubistva postanu naša nova stvarnost.

Zbog svega navedenog, predlažemo provođenje nekoliko sljedećih mjer na nivou škole;

- Izrada vlasitih akcioni planova na području općine Travnik za svaku srednju školu posebno,
- Savjetodavni rad sa roditeljima,
- Savjetodabni rad sa maloljetnim prestupnicima,
- Sprovođenje istraživanja o pojavnosti vršnjačkog nasilja na nivou škole i njegovim specifičnostima, uzrocima,
- Ozbiljno pristupanje realizaciji časova odjeljenske zajednice u okviru kojih će se, izmđu osalog djeca educirati o pojavi i načinima prevazilaženja problema vršnjačkog nasilja,
- Praćenje djelotvornost primjenjenih odgojno-disciplinskih mjer,
- Organiziranje stručno vođenih seminara, radionica, tribina, predavanja, igraonica i radionica za djecu i roditelje sa tematikom koja je usko vezana sa problemima koji se javljaju na relaciji nasilnik-žrtva,
- Obezbeđivanje mehanizama za brzo reagovanje,
- Omogućavanje telefonskih kontakata za prijave slučajeva vršnjačkog nasilja (SOS telefon),
- Omogućavanje prijava vršnjačkog nasilja putem e-maila.

Provođenjem ovih mjer trebala bi se ostvariti dva cilja,

- Razvijanje postupaka i stvaranje uslova u školi koji smanjuju obim nasilnog ponašanja među djecom i maloljetničke delikvencije.
- Sprječavanje stvaranja problema između nasilnika i žrtve.

Pored svega navedenog, za uspješno provođenje mera prevencije nasilja u srednjim školama na području općine Travnik, neophodna je saradnja i koordinacija između;

- Ministarstva obrazovanja, nauke, kulture i sporta SBK/KSB,
- Odgojno-obrazovnih institucija (od predškolskih do visokoškolskih),
- Ministarstva unutrašnjih poslova (MUP SBK/KSB)
- Centra za socijalni rad Travnik i td..

Shodno svemu navedenom, smatramo da su, kako glavna tako i sve pomoćne hipoteze uspješno dokazane;

“Nasilje među srednjoškolcima na području općine Travnik prisutno je u različitim oblicima.”

- Srednjoškolci sa područja općine Travnik informisani su o svim pojavnim oblicima nasilja u školi.

⁴⁹ VESTA, Companing for preventing and combating occurences of bullying in primary schools; „Program mjera za pre prevenciju i suzbijanje pojavnih oblika nasilja među djecom u osnovnim školama“. Tuzla, oktobar/listopad 2008.godine..op.cit.p13.

⁵⁰ Ib

- Nasilje nad drugim učenicima u školi vrše njihove školske kolege.
- Učenici koji su žrtve nasilja za pomoć se najčešće obraćaju nastavnicima i drugovima/drugaricama
- Učenici koji su svjedoci nasilja nad svojim kolegama uglavnom se plaše nasilja i rjeđe sprečavaju nasilje nad svojim kolegama.
- Žrtve nasilja trpe i neuzvraćaju nasilnicima na pretrpljeno nasilje.
- Srednjoškolci sa područja općine Travnik ipak u većem broju slučajeva osjećaju sigurno kako u školi tako i na putu od kuće do škole.

LITERATURA

- Instrumentarij, u okviru instrumentarija predstavljena je anketa kao instrument metode ispitivanja kojom su prikupljeni podaci na temu, „Vršnjačko nasilje u srednjim školama na području općine Travnik“
- VESTA, Companing for preventing and combating occurrences of bullying in primary schools; „Program mjera za pre prevenciju i suzbijanje pojavnih oblika nasilja među djecom u osnovnim školama“. Tuzla, oktobar/listopad 2008.godine.

SAVREMENI OBLICI KOMPJUTERSKOG KRIMINALITETA I NJIHOVA PREVENCIJA

CONTEMPORARY FORMS OF COMPUTER CRIME AND THEIR PREVENTION

Snježana Radošević, Testing centar d.o.o Gradiška.

Apstrakt: Jedno od najznačajnijihotkrića u istorijičovječanstvajestekompjuter. Brojne su mu karakteristike, ali kao posebno značajne možemo istaći ekspansivnost u razvoju, širinu primjene, značaj za najvažnije segmente i procese društvenog i ekonomskog života. Od pojave prvog kompjutera, sredinom četrdesetih godina, pa do danas, došlo je do rapidnog širenja upotrebe kompjutera u skoro svim oblastima života i rada. Prvi računar nazvan ENIAC je pušten u eksperimentalni pogon februara 1944. godine, da bi konačno bio završen tek 1946. godine. Njegova osnovna funkcija bila je da u ratne svrhe izračunava putanje artiljerijskih granata, a njegova izrada je koštala oko 400.000 tadašnjih dolara, što je u to vrijeme bila značajna svota, ali je sada, nekih pedeset godina posle tog događaja, sasvim izvjesno da su te pare bile izvanredno uložene, jer je napredak, koji je širom upotrebot kompjutera uslijedio, bio fantastičan.

Abstract: One of the most important discoveries in the history of mankind is a computer. Many of his characteristics, but as particularly significant, we can point out the expansiveness in the development, breadth of application, significance of the most important segments and processes of social and economic life.

Since the advent of the first computers, mid-forties, but to date, there has been a rapid expansion of the use of computers in almost all areas of life and work. The first computer called ENIAC was put into experimental operation in February 1944, and finally was completed only in 1946. Its main function was to warfare calculated trajectory artillery shells, and its development has cost about 400,000 of the then US dollars, which at that time was a considerable sum, but now, some fifty years after the event, quite for certain that these couples were extraordinarily invested, because the progress, which is around the use of computers came, was fantastic.

UVOD

Danas smo svi svjesni ogromnog značaja upotrebe kompjutera u savremenim društvima i činjenice da nema oblasti ljudske djelatnosti u kojoj računari nisu našli svoju primjenu. Međutim, prilično je poražavajuća konstatacija da ne postoji tehničko i tehnološko dostignuće koje u istoriji čovječanstva nije naišlo na različite vidove zloupotrebe. Specifičnost predstavljaju faze razvoja u kojima je pronalazak bio podložan zloupotrebi, zatim grupacije lica koje su vršile takve radnje i različite namjene zbog kojih su se vršile te zloupotrebe.

U početku primjene kompjuterske tehnologije, kompjutери nisu bili podobni za veće zloupotrebe, jer njihova primjena nije bila masovna, tako da se njima bavio samo uzak krug korisnika – informatičkih stručnjaka. Ono što je otvorilo vrata širenju mogućnosti da se kompjuterska tehnologija zloupotrijebi u različite svrhe, jeste njen brz razvoj, pojednostavljenje njene upotrebe, kao i dostupnost iste širokom krugu korisnika.

1. POJAM KOMPJUTERSKOG KRIMINALITETA

Sve učestaliji vidovi i načini zloupotrebe kompjutera podstakli su naučnu i stručnu javnost da se pozabavi ovim oblikom kriminalnog ponašanja.

Kompjuterski kriminalitet je nemoguće definisati jedinstvenim i preciznim pojmovnim određenjem. To je „opšta forma kroz koju se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.“⁵¹ Naime, teškoće u definisanju kompjuterskog kriminaliteta proizilaze zbog toga što se radi o relativno novom obliku kriminalnog ponašanja, ali i zbog toga što postoji velika fenomenološka raznovrsnost ove pojave, koja se teško može buhvati jednom definicijom.

Jedan od autora koji je razmatrao problem kompjuterskog kriminala jeste Don Parker. Njegov zaključak je da je: „zloupotreba kompjutera svaki događaj u vezi sa upotrebom kompjuterske tehnologije u kome žrtva trpi ili bi mogla da trpi gubitak, a učinilac djeluje u njameri da sebi pribavi ili bi mogao da pribavi korist.“⁵²

Svjetski rječnik engleskog jezika ovaj pojam određuje na sledeći način: „Kompjuterski kriminalitet obuhvata nezakonite aktivnosti koje se vrše na kompjuteru ili kod kojih je kompjuter sredstvo izvršenja. On obuhvata kriminalni upad u drugi kompjuterski sistem, krađu kompjuterskih podataka, ili korišćenja on-line sistema za vršenje ili pomoći u izvršenju prevara.“⁵³

Na desetom Kongresu Ujedinjenih Nacija za prevenciju kriminaliteta i tretman delikvenata, razmatrana je ova problematika: Kompjuterski kriminalitet je opšti pojam koji obuhvata krivična djela koja se vrše posredstvom kompjuterskog sistema ili mreže, u kompjuterskom sistemu ili mreži, ili protiv kompjuterskog sistema ili mreže. U principu on uključuje bilo koje krivično djelo koje se vrši u elektronskom ambijentu.“⁵⁴

Na našim prostorima, jedna od prvih definicija iz ove oblasti je: „Kompjuterski kriminal obuhvata krivična djela kod kojih se kompjuter pojavljuje kao sredstvo, predmet ili objekt napada, za čije je izvršenje ili pokušaj neophodno izvijesno znanje iz računarstva ili informatike.“⁵⁵

Autor Đorđe Ignjatović pod ovim pojmom podrazumijeva poseban vid inkriminiranih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje kao sredstvo izvršenja ili kao objekt krivičnog djela, ukoliko se djelo na drugi način, ili prema drugom objektu, ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike.“⁵⁶

Imajući u vidu prethodna sagledavanja pojma kompjuterskog kriminaliteta, posebno različitost u pristupima pojedinih autora, zaključujemo da je neophodno imati veoma širok pristup prilikom definisanja ove vrste kriminalnog ponašanja. Naime, jedna sveobuvatna definicija mora inkorporisati u svojoj strukturi tri bitna elementa:

- 1) način izvršenja,
- 2) sredstvo izvršenja i

⁵¹ S. Petrović, **Kompjuterski kriminal**, Bezbjednost MUP RS, Banja Luka, 1994.

⁵² D. Parker, **Computer Abuse**, Springfield, 1973.

⁵³ <http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?lextyle=3&search=computer%20crime>

⁵⁴ <http://www.un.org/events/10thcongress/2088h.htm>

⁵⁵ B. Bravar, **Pojavne oblike zlorabe računalnika**, Revija za kriminalistiku in kriminologijo, Ljubljana, 1982.

⁵⁶ Đ. Ignjatović, **Pojmovno određenje kompjuterskog kriminaliteta**, Anal Pravnog fakulteta, Beograd, 1991.

3) posljedicu kriminalnog djelovanja.

Pod načinom izvršenja se podrazumijeva svojevrsna upotreba kompjutera, koji između ostalog može biti i osnovno sredstvo za izvršenje krivičnih djela, pričemu je potrebno da nastupi i određena kažnjiva posljedica.

U tom smislu, najpotpunija definicija bi bila: „Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja kod koga se korišćenje kompjuterske tehnologije i informatičkih Sistema ispoljava kao način izvršenja krivičnog djela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično pravnom smislu relevantna posljedica.“⁵⁷

2. KARAKTERISTIKE KOMPJUTERSKOG KRIMINALITETA

Privredni kriminal, ili namjerna prevara čiji je cilj da se drugom licu uskrati posjed novca, imovine ili zakonsko pravo, ima nekoliko pojavnih oblika. To su⁵⁸:

- pronjevera imovine,
- finansijska pronevjera,
- korupcija i mito,
- pranje novca,
- piraterija,
- cyber kriminal i
- industrijska špijunaža, odnosno mešetarenje informacijama.

Kompjuterski kriminalitet ima svoje specifičnosti u odnosu na druge vrste kriminalnih djelovanja, koje nesumnjivo ukazuju na opasnost ove pojave i upućuju da se pitanju suzbijanja iste, pristupi sa velikom pažnjom. Te karakteristike su:

- velika dinamičnost,
- konstantno širenje na nove oblasti,
- težina posljedica koje nastupaju vršenjem kompjuterskih krivičnih djela,
- velika tamna brojka,
- otežano otkrivanje i dokazivanje,
- specifičan profil učinioca,
- velike mogućnosti za prikrivanje izvršenog krivičnog djela, itd.

Prethodno navedene karakteristike posljedica su specifičnog ambijenta u kojem se kompjuterski kriminalitet vrši. Taj ambijent karakterišu:

- visoka koncentracija na malom prostoru, prethodno provjerenih i uređenih podataka, dostupnih kako ovlašćenim, tako i neovlašćenim korisnicima;
- znatno proširen prostor kriminalnog djelovanja, koji, za razliku od tradicionalnih vidova kriminaliteta, ne zahtijeva prisustvo izvršioca na mjestu izvršenja krivičnog djela;
- skraćeno vrijeme kriminalnog djelovanja, s obzirom na automatizovani ambijent, čija brzina sprječava nadzor i upravljanje. Na taj način, vrijeme potrebno za izvršenje krivičnog djela skraćuje se na dijelove sekunde, što implicira visok nivo prikivenosti i značajne teškoće u otkrivanju takve djelatnosti;

⁵⁷Ž. Aleksić, M. Škuljić, **Kriminalistika**, Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik“, Beograd, 2007.

⁵⁸<http://ekonomist.com>

- na ovo se nadovezuju i suptilne tehnike i metodi koje se izvršavaju istim mehanizmima kao i legalne, ne ostavljaju tragove, niti ometaju redovan rad sistema, pa je samim tim mogućnost otkrivanja svedena na najmanju mjeru; za razliku od tradicionalnog kriminala, kompjuterski karakteriše stabilnost rizika, s obzirom da se jednom izgrađen modus može veoma dugo koristiti, sa potpuno istim, niskim rizikom otkrivanja;
- sve jednostavnije mogućnosti upotrebe kompjuterske tehnologije od strane sve većeg broja korisnika, kojima više nije nužno posebno tehničko obrazovanje.

Uopšteno govoreći, kompjuterski kriminalitet može da se ispolji korišćenjem, oštećenjem, zloupotrebatom, ili bilo kojom drugom manipulacijom dva osnovna segmenta kompjuterskog sistema – hardvera (*hardware*) i softvera (*software*). Naime, kompjuter predstavlja elektronsku mašinu sposobnu da primi i čuva informacije, obavlja matematičke, logičke i druge intelektualne operacije, a može da se koristi u različitim djelatnostima, te da se primjenjuje u opšte, ili neke posebne svrhe, kada je riječ o namjenskom ili kompjuteru za posebne potrebe.⁵⁹

Opasnost kompjuterskog kriminaliteta po društvenu zajednicu ogleda se ne samo u ekspanziji njegovih pojavnih oblika, već i u tome što pojedina tradicionalna krivična djela, kao što su prevara, zloupotreba službenog položaja, pronevjera,... itd, korišćenjem kompjuterske tehnologije dobijaju znatno opasnije oblike. Posebna karakteristika kompjuterskog kriminaliteta jeste nastala posljedica. Kriminalom „broj jedan“ u budućnosti mogao bi se okarakterisati *cyber* kriminal, od koga su štete za napadnutu firmu često katastrofalne. To je naročit problem od pojave elektronskog bankarstva: hakeri su obično spretniji od bilo kog sistema zaštite.

Štetna posljedica ispoljava se kao nastala imovinska šteta, ali isto tako može da se ispolji u vidu gubljenja povjerenja u sigurnost i tačnost dobijenih informacija iz kompjuterskog sistema, što može dovesti do različitog tretiranja i narušavanja poslovnog ugleda mnogih privrednih i vanprivrednih subjekata i izazvati strah od pojave novih kriminalnih radnji vezanih za sve nivoe funkcionisanja kompjuterskog sistema.⁶⁰

Štete koje nastupaju vršenjem kompjuterskih krivičnih djela su po pravilu veoma velike, a često su i teško sagledive. Naime, pored posljedica finansijske prirode koje mogu da nastanu kada učinilac vrši djelo u cilju sticanja protivpravne imovinske koristi, pa tu korist za sebe ili drugo lice zaista i stekne, ili je ne stekne, ali svojim djelom objektivno pričini određenu štetu, ili kada učinilac ne postupa radi sticanja koristi za sebe ili drugoga, ali objektivno učini finansijsku štetu, postoje i posljedice nematerijalne prirode koje se ogledaju u neovlašćenom otkrivanju tuđih tajni, narušavanju ugleda, povredi moralnog prava ili drugom sličnom postupanju, kao i kombinovane posljedice, koje postoje kada se otkrivanjem određene tajne, ili povredom autorskog prava, putem zloupotrebe kompjutera ili informatičke mreže nanese određeni vid nematerijalne štete, a istovremeno prouzrokuje i konkretna finansijska šteta.

U SAD je još osamdesetih godina utvrđeno i to kroz prilično opreznu procjenu, da finansijske štete prouzrokovane kompjuterskim kriminalitetom dostižu iznos između 100 i 300 miliona dolara na godišnjem nivou, pri čemu prosječna šteta prouzrokovana kompjuterskim deliktom iznosi 430.000 dolara.⁶¹ Do današnjih dana, situacija se znatno pogoršala.

Posebno zabrinjava što se korporacije često uzdržavaju od prijavljivanja slučajeva u kojima su oštećene zloupotrebatom kompjutera, jer smatraju da bi time pogoršali svoj položaj na tržištu lošim reklamiranjem, kroz isticanje sopstvene nesposobnosti da se efikasno zaštite.⁶²

⁵⁹Ž. Aleksić, M. Škulić, **Ibidem**.

⁶⁰B. Banović, **Obezbeđenje dokaza u kriminalističkoj obradi dela privrednog kriminaliteta**, Viša škola unutrašnjih poslova, Beograd, 2002.

⁶¹M. Gačić, **Kompjuterski kriminal, inostrana iskustva**, 13. maj, Zagreb, 1982.

⁶²Ž. Aleksić, M. Škulić, **Ibidem**.

Istraživanje o privrednom kriminalu pokazalo je da mnoge kompanije javno podržavaju politiku izveštavanja vlasti o svim slučajevima kriminala, ali se u realnoj situaciji ponašaju sasvim drugačije. Kao osnovni razlog takvog ponašanja navodi se strah kompanije od negativnog uticaja javnosti na poslovne veze kompanije ili moral zaposlenih, strah od troškova sudskog postupka ili uvjerenje da postoji mala mogućnost povraćaja ukradenih sredstava.

3. SAVREMENI OBLICI KOMPJUTERSKOG KRIMINALITETA

Postoje različite klasifikacije kompjuterskog kriminaliteta. Na desetom Kongresu Ujedinjenih Nacija za prevenciju kriminaliteta i tretman delikvenata, u okviru materijala za sekciju o kriminalu, zaključeno je da postoje dvije vrste ovog pojavnog oblika kriminalnog ponašanja:

- 1) kompjuterski kriminalitet u užem smislu, odnosno svako nezakonito ponašanje usmjereni na elektronske operacije sigurnosti kompjuterskih sistema i podataka koji se u njima obrađuju i
- 2) kompjuterski kriminalitet u širem smislu, odnosno svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je nezakonito posjedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža.

U istom dokumentu navode se i konkretni oblici kompjuterskog kriminaliteta, u skladu sa Preporukom Savjeta Evrope⁶³ i listom OECD-a [16] iz 1989., odnosno 1985. godine. To su:

- neautorizovani pristup kompjuterskom sistemu ili mreži, kršenjem mjera sigurnosti (haking);
- oštećenje kompjuterskih podataka ili programa;
- kompjuterske sabotaže;
- neovlašćeno presretanje komunikacija od i u kompjuterskim sistemima i mrežama i kompjuterska špijunaža.

Navedeni oblici se gotovo stalno međusobno ukrštaju, tako da činjenjem jednog oblika, dolazi do činjenja i niza drugih aktivnosti koje spadaju u neki drugi oblik kompjuterskog kriminaliteta. Tako, na primjer, neovlašćenim ulaskom u kompjuterski sistem ili mrežu može doći do oštećenja ili uništenja kompjuterskih podataka ili programa, ali i do kompjuterske špijunaže.

Od kompjuterskog kriminaliteta u širem smislu, najčešće se pojavljuju:

- kompjuterski falsifikati,
- kompjuterske krađe,
- tehničke manipulacije uređajima ili elektronskim komponentama uređaja,
- zloupotrebe sistema plaćanja (kao što su manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima).

Njima se u novije vrijeme dodaju i djela podržana računarima. Ova djela obuhvataju „rasturanje“ materijala ili samo njihovo posedovanje, pri čemu se mreža koristi za postizanje boljih rezultata kriminala ili pokušaja izbjegavanja pravde. U ova djela se ubrajaju razni nezakoniti i štetni sadržaji, kršenje autorskih i srodnih prava, prodaja zabranjene robe (oružja, kradene robe, lijekova,...) ili pružanje nedozvoljenih usluga (kockanje, prostitucija,...). Najviše pažnje u ovoj grupi djela privlači dječja pornografija i distribucija raznih materijala Internetom.⁶⁴

⁶³<http://www.justice.gov/criminal/cybercrime/crycoe.htm>

⁶⁴<http://megatrender.blog.rs/blog/megatrender/megatrender-19/2008/03/06/tipovi-cyber-kriminala>

Evropska konvencija o cyber kriminalu⁶⁵ predviđa četiri grupe djela:

- 1) djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – njih čine nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, pasvorda;
- 2) djela vezana za kompjutere – kod kojih su falsifikovanje i krađe najtipičniji oblici napada;
- 3) djela vezana za sadržaje – dječija pornografija je najčešći sadržaj koji se pojavljuje u ovoj grupi obuhvatajući posjedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovih materijala, njihova proizvodnja radi distribucije i obrada u kompjuterskom sistemu ili na nosiocu podataka;
- 4) djela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primjera djela kompjuterskim sistemima.

U Enciklopediji *cyber* kriminala⁶⁶ navodi se da FBI i Nacionalni centar za kriminal „bijelih kragni“ SAD (National White Collar Crime Center) otkrivaju i prate sljedeće oblike:

- upade u kompjuterske mreže;
- industrijsku špijunažu;
- softversku pirateriju;
- dječiju pornografiju;
- bombardovanje elektronskom poštom;
- „njuškanje“ pasvorda;
- „prerušavanje“ jednog računara da elektronski „liči“ na drugi kako bi se moglo pristupiti sistemu koji je pod restrikcijama;
- krađu kreditnih kartica.

Kompjuterski kriminalitet zavisno od tipa počinjenih djela može biti politički i ekonomski. U politički *cyber* kriminal spadaju:

- *cyber* špijunaža i *cyber* sabotaža,
- haking,
- *cyber* terorizam,
- *cyber* ratovanje.

U ekonomski *cyber* kriminal spadaju⁶⁷:

- *cyber* prevare,
- haking,
- krađa internet vremena i krađa internet usluga,
- piratstvo softvera, mikročipova i BP,
- *cyber* industrijska špijunaža,
- spam,
- proizvodnja i distribucija nedozvoljenih štetnih sadržaja (dječija pornografija, pedofilija, vjerske sekte, širenje rasističkih, nacističkih i sličnih ideja i stavova,...),
- zloupotreba žena i djece,
- manipulacija zabranjenim proizvodima, supstancama i robama,

⁶⁵<http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc>

⁶⁶<http://www.scribd.com/doc/20262442/Encyclopedia-ofCyber-Crime>

⁶⁷<http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29>

- povreda *cyber* privatnost (nadgledanje e-pošte, prislушкиvanje, praćenje e-konferencija, prikačinjanje i analiza špijunkih softvera,...).

Jasno je da veliki broj različitih klasifikacija sam po sebi pokazuje raznovrsnost djela iz opusa kompjuterskog kriminala i kompleksnost njihovih pojavnih oblika.

Ono što je nesporno je da je kompjuterski kriminal više vezan za aktivnosti pojedinaca, a kriminal vezan za kompjuterske mreže više je djelo grupe i to organizovanih, profesionalizovanih, a sve češće i strogo specijalizovanih. Ove grupe su, s jedne strane, „tradicionalne“ grupe organizovanog kriminala koje su se usavršile i osavremenile primjenom informaciono komunikacione tehnologije i pripomile za „izlazak“ na *cyber* scenu. S druge strane, javljaju se i posebne organizovane *cyber* grupe – *cyber* mafija. Ova mafija ima svoja pravila, drugačiji način ponašanja od konvencionalne mafije. Njene aktivnosti su umnogome olakšane specifičnostima okruženja u kom djeluju i oružja koja koriste. Okruženje je virtuelno, oružje je informaciono, a znanje je specijalizovano. Internacionalizam, transnacionalnost, multidimenzionalnost samo su neka od svojstava ovih grupa. Njihova organizaciona formula nije toliko jednostavna, ustaljena i jednoobrazna kao što je to slučaj sa drugim oblicima organizovanog kriminala, što još više utvrđuje sliku njihove posebnosti.⁶⁸

4. PREVENCIJA KOMPJUTERSKOG KRIMINALITETA

Prevencija kompjuterskog kriminaliteta, kao i drugih krivičnih djela koja se mogu svrstati pod ranije iznesene definicije kompjuterskog kriminaliteta, trebala bi se provoditi u skladu sa sljedećim koracima:

- 1) Preuređivanje Krivičnog zakona u dijeli koja se tiču informaciono-komunikacijskih tehnologija, kao i kvalitetnijeg i detaljnijeg pojašnjenja određenih definicija i samih krivičnih djela.
- 2) Veća edukacija pravobranilaca koji bi se specijalizovali za borbu protiv ovog tipa kriminala.
- 3) Povećanje broja policijskih službenika koji bi se specijalizovali u borbi protiv ovog tipa kriminala, njihova edukacija i obuka, kao i nabavka potrebne tehničke opreme.
- 4) Uticaj na svijest građana o novim krivičnim djelima kroz razne informacione aktivnosti.
- 5) Angažovanje poznatih stručnjaka iz oblasti kompjuterskog kriminaliteta i digitalne forenzike, u svim edukacijama, kako stručnih lica, tehničkog osoblja, tako i javnosti.

ZAKLJUČAK

U ovom radu pokušali smo da sagledamo kompleksnost kompjuterskog kriminaliteta. Već prilikom pokušaja definisanja, uočile su se prve teškoće. Naime, ma koliko se svako pojmovno određenje kompjuterskog kriminaliteta na prvi pogled činilo adekvatnim, vrlo brzo se uočavalo da je ovaj oblik kriminalnog djelovanja toliko složen, da je vrlo teško iskazati u jednoj definiciji njegovu specifičnost, sadržajnost i značenje za društvenu zajednicu.

Razmatrajući karakteristike kompjuterskog kriminaliteta, a naročito njegove posljedice, očigledno je da se isti razlikuje od svih drugih oblika kriminalnog djelovanja po stepenu opasnosti u odnosu na napadnuta dobra. Ova konstatacija je još više došla do izražaja kada se shvatilo da mnoge kriminalne aktivnosti potpomognute uticajem oblika kompjuterskog kriminala postaju još opasnije i štetnije.

Ohrabruje činjenica da su mnoge države postale svjesne ove pojave i da su u svom pozitivnom krivičnom zakonodavstvu predvidjele pojavnje oblike kompjuterskog kriminaliteta kao posebna krivična djela. Sa druge strane, ohrabrujuće je i to što se u sve većem broju naučnih i stručnih radova pažnja posvećuje

⁶⁸J. Matijašević, S. Ignjatijević, **Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posljedice**, Univerzitet Privredna akademija, Novi Sad, 2010.

upravo ovom obliku kriminalnog ponašanja. Na taj način dolazi do razotkrivanja mnogih specifičnosti kompjuterskog kriminaliteta, a istovremeno se otvara mogućnost suprotstavljanju njegovim oblicima od strane društvene zajednice.

Sasvim je jasno da se određenoj pojavi društvo adekvatno može suprotstaviti ukoliko sagleda sve njene karakteristike i uđe u sve pore njenih specifičnosti. S obzirom da su načini zloupotrebe kompjuterske tehnologije svakim danom sve savršeniji i komplikovaniji za otkrivanje, i da je vrlo teško ići u korak sa tim kriminalnim aktivnostima, potrebno je i dalje ulagati napore u to da javnost bude svjesna sa kakvim se fenomenom današnje društvo suočava, potrebno je konstantno raditi na što adekvatnijem odgovoru na različita kriminalna djelovanja u ovoj oblasti. Transparentnost i odlučno suprotstavljanje različitim vidovima kriminalnih aktivnosti su dve bitne odrednice u težnji da se različiti oblici kriminaliteta, pa i kompjuterski, svedu u određene, za društvenu zajednicu, podnošljive okvire.

LITERATURA

- [1] B. Banović, Obezbeđenje dokaza u kriminalističkoj obradi dela privrednog kriminaliteta, *Viša škola unutrašnjih poslova*, Beograd, 2002.
- [2] B. Bravar, Pojavne oblike zlorabe računalnika, *Revija za kriminalistiku in kriminologijo*, Ljubljana, 1982
- [3] D. Parker, Computer Abuse, Springfield, 1973.
- [4] Đ. Ignjatović, Pojmovno određenje kompjuterskog kriminaliteta, *Analji Pravnog fakulteta*, Beograd, 1991.
- [5] Ž. Aleksić, M. Škulić, Kriminalistika, *Pravni fakultet Univerziteta u Beogradu i Javno preduzeće „Službeni glasnik“*, Beograd, 2007.
- [6] J. Matijašević, S. Ignjatijević, Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice, *Univerzitet Privredna akademija*, Novi Sad, 2010.
- [7] M. Gačić, Kompuerski kriminal, inostrana iskustva, *13. maj*, Zagreb, 1982.
- [8] S. Petrović, Kompjuterskikriminal, *BezbjednostMUPRS*, BanjaLuka, 1994.

Internet izvori:

- [1] <http://www.justice.gov/criminal/cybercrime/crycoe.htm>
- [2] <http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?lextype=3&search=computer%20crime>
- [3] <http://www.un.org/events/10thcongress/2088h.htm>
- [4] <http://ekonomist.com>
- [5] <http://megatrender.blog.rs/blog/megatrender/megatrender-19/2008/03/06/tipovi-cyber-kriminala>
- [6] <http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29>

KRIMINALISTIČKO-FORENZIČKA OBRADA MJESTA IZVRŠENJA KRIVIČNOG DJELA – UVIĐAJ „ROLE OF DNA SHED LIGHT ON THE WORST FORMS OF VIOLENT DEEDS“

Petar Đukić¹, Dr Borislav Đukić²

¹Visoka škola unutrašnjih poslova, Banja Luka, BiH, petar.djukic96@yahoo.com

²Visoka škola unutrašnjih poslova, Banja Luka, BiH, bobandjukic70@gmail.com

Apstrakt: Uviđaj se preduzima kada je za utvrđivanje neke važne činjenice u postupku potrebno neposredno opažanje. Radi se o čulnom opažanju organa koji vodi krivični postupak o činjecama važnim za konkretni krivičnopravni slučaj. Uviđaj kao radnja dokazivanja mora se preduzeti u zakonskoj formi uz primjenu metoda i sredstava kojima se služe forenzičke nauke u cilju otkrivanja i fiksiranja materijalnih tragova krivičnog djela. Najznačajniji predmet uviđaja je svakako prostor u kom se odigrao sam krivični događaj. Uviđaj se vrši uz pomoć stručne osobe kriminalističko-tehničke ili druge stuke, koja će pomći u pronalaženju, osiguranju ili opisivanju tragova, izvršiti potrebna mjerena i snimanja, sačiniti skicu i fotodokumentaciju ili prikupiti i druge podatke. Cilj rada je da se predstave kriminalističko-forenzičke pravilnosti vršenja uviđaja u praksi (priprema za vršenje uviđaja, tok i sadržaj radnje, materijalni tragovi), ali i da se ukaže na pozitivne zakonske odredbe o uviđaju.

Ključne riječi: uviđaj, čulno opažanje, kriminalistika, forenzika, materijalni tragovi....

UVOD

Uviđaj je radnja dokazivanja koja se sastoji od neposrednog opažanja promjena na licu mjesta krivičnog događaja koje preduzima ovlašćeni organ, tj. uviđaj je sistem intelektualnih, realnih i instrumentalnih djelatnosti koje se primjenjuju na osnovu odredbi Zakona o krivičnom postupku uz primjenu kriminalističko-tehničkih i taktičkih metoda i sredstava koji su usmjereni na pronalaženje, obezbjeđivanje od uništenja i fiksiranje kriminalističkih i pravno relevantnih materijalnih informacija (predmeta, tragova krivičnog djela, situacije nastale krivičnim događajem) za potrebe eventualnog krivičnog postupka [1]. Radi se o neposrednom, čulnom opažanju organa koji vodi krivični postupak o činjenicama važnim za razrješenje cjelokupnog krivičnopravnog slučaja ali i za odlučivanje o nekim akcesornim predmetima krivičnog postupka.

Cilj uviđaja je otkrivanje i prikupljanje materijalnih dokaza ili indicija o postojanju i vrsti krivičnog djela koje mogu poslužiti pronalaženju i identifikaciji učinilaca djela ili o tome da se te činjenice razjasne ili da se utvrde tragovi i posljedice krivičnog djela ili provjeri istinitost drugih dokaza [2].

Predmet uviđaja mogu da budu mjesta, lica i stvari. Sa aspekta ovog rada nužno je istaći koja se to mjesta javljaju kao predmet kriminalističko-forenzičke obrade, odnosno kao predmet samog uviđaja. To su svakako mjesta koja su u Krivičnom zakonu određena kao mjesto izvršenja krivičnog djela. Krivično djelo je učinjeno kako u mjestu gdje je učinilac radio ili je bio dužan raditi, tako i u mjestu gdje je posljedica činjenja ili nečinjenja potpuno ili djelimično nastupila (član 23, stav 1 KZ-a BiH)⁶⁹. Sa druge strane, pored mjesta izvršenja krivičnog djela (u našem krivičnom zakonodavstvu određenog po teoriji ubikviteta), predmet uviđaja je i svako drugo mjesto na kome se mogu pronaći predmeti i tragovi krivičnog djela. Uviđaj se preduzima uz puno poštovanje načela brzine i operativnosti, što znači da ga je neophodno preduzeti što prije kad god je to moguće. Organi koji vrše uviđaj ne smiju dozvoliti da protekne mnogo vremena od izvršenja krivičnog djela do početka vršenja uviđaja. Bitno je i istaći da poštovanje načela brzine ne smije ići na uštrbu načela zakonitosti, metodičnosti, temeljitosti i upornosti.

⁶⁹ Krivični zakon Bosne i Hercegovine (“Službeni glasnik Bosne i Hercegovine”, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15 i 40/15).

Za preuzimanje uviđaja dovoljno je da je ispunjen materijalni uslov predviđen Zakonom o krivičnom postupku Bosne i Hercegovine⁷⁰. Uviđaj se preuzima kada je za utvrđivanje neke važne činjenice u postupku potrebno neposredno opažanje (član 92 ZKP-a BiH). Zakon ne propisuje neki formalni uslov za vršenje uviđaja, kao što je zahtjev, naredba ili rješenje. Vršenje uviđaja u istrazi primarno je u nadležnosti tužioca. Sekundarno, uviđaj mogu vršiti i ovlašćena službena lica nakon obavještavanja tužioca. Ako je tužilac prisutan na licu mjesta u toku vršenja uviđaja od strane ovlašćenih službenih lica, može tražiti da ovlašćeno službeno lice izvrši određene radnje koje on smatra neophodnim. Sve radnje preduzete tokom uviđaja moraju se dokumentovati i detaljno obrazložiti kako u zapisniku, tako i u posebnom službenom izvještaju (član 221 ZKP-a BiH). Uviđaj se vrši uz pomoć stručne osobe kriminalističko-tehničke ili druge struke, koja će pomći u pronalaženju, osiguranju ili opisivanju tragova, izvršiti potrebna mjerena i snimanja, sačiniti skicu i fotodokumentaciju ili prikupiti i druge podatke (član 94, stav 1 ZKP-a BiH). Na uviđaj se može pozvati i vještak, ako bi njegovo prisustvo bilo od koristi za davanje nalaza i mišljenja (član 94, stav 2 ZKP-a BiH).

Dokazna snaga uviđaja je izuzetno velika, a rezultati pribavljeni uviđajem imaju veću vrijednost od dokaza pribaljenih drugim radnjama dokazivama. U prilog tome govori stara latinska izreka „Nulla est maior probatio, quam evidentia rei“ („Nema boljeg dokaza od uviđaja“). Uviđajem se činjenice utvrđuju neposrednim opažanjem organa koji vodi postupak, a ne posrednim putem kao kod drugih dokaznih radnji (npr. saslušanje svjedoka).

Iz svega gore navedenog možemo zaključiti da je uviđaj jedna jedinstvena „kriminalističko-procesna“ radnja čije uslove i formu određuje Zakon o krivičnom postupku, a sadržinu kriminalistika, odnosno sve one nauke koje se primjenjuju da bi se dobili odgovori na pitanja od interesa za neki krivični događaj.

1. OSNOVNE PREPOSTAVKE ZA VRŠENJE UVIĐAJA

1.1. Organizacioni i tehnički uslovi za vršenje uviđaja

Da bi se uviđaj uspješno obavio potrebna je organizaciona uređenost organa koji vrše uviđaj, ali i tehničke predispozicije u smislu posjedovanja odgovarajuće opreme. Simonović i Matijević (2007) predviđaju sljedeće organizacione i tehničke uslove za vršenje uviđaja:

- organizovan efikasan sistem dojave o događaju koji nalaže izlazak na lice mjesta,
- organizovan efikasan sistem veza,
- ustavljena permanentna dežurstva uviđajne ekipe,
- potpuna tehnička oprema (univerzalni neseser, neseser sa foto-opremom, neseser za uviđaje kod saobraćajnih nezgoda...),
- uslovi za preuzimanje eventualnih neophodnih intervencija (prva pomoć, izvlačenje povrijeđenih i njihov brz transport u zdravstvu ustanovu...),
- motorizovane patrole,
- konstantno stručno usavršavanje službenika koji redovno sprovode uviđaj [1].

1.2. Određivanje prostornih granica i obezbjeđenje lica mjesta

Lice mjesta je, u kriminalističko-forenzičkom smislu, svako ono mjesto na kom se mogu pronaći tragovi i predmeti krivičnog djela. Veoma je bitno utvrditi uže i šire prostorne granice lica mjesta. Uži dio lica mjesta je prostor neposrednog događanja krivičnog djela, a širi dio sav preostali prostor u kome se pojavljuju neki tragovi. Isto tako, krivično djelo može da bude izvršeno kako na otvorenom, tako i u zatvorenom prostoru. Od toga da li je u pitanju zatvoren ili otvoren prostor zavisi sama kriminalističko-forenzička obrada (npr. mnogo je lakše obezbijediti zatvoren prostor).

⁷⁰ Zakon o krivičnom postupku Bosne i Hercegovine („Službeni glasnik Bosne i Hercegovine“, br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 i 72/13).

Kao zatvoren prostor moglo bi se odrediti svako mjesto koje je fizički potpuno odvojeno od okoline. Određivanje granica lica mjesta kada je riječ o takvom prostoru bazira se na osnovnom pravilu koje kaže da se lice mjesta prostire na onoj površini na kojoj se nalaze tragovi vezani za kriminalni događaj. Ako je, na primjer, u pitanju soba u kući, moguće je da se krivični događaj odigrao samo u toj sobi, ali je moguće naći trageve i u ostalim prostorijama (hodniku, prilazu kući). U tom slučaju, soba predstavlja uži, a okolne prostorije širi dio lica mjesta.

Ista pravila koja važe kada se utvrđuje prostorna granica lica mjesta kod zatvorenog prostora važe i kada je u pitanju otvoren prostor. Naime, bitna je granica do koje se prostiru materijalni tragovi koji su u vezi sa krivičnim djelom, odnosno događajem. Mjesto gdje se događaj odigrao je uži dio lica mjesta, a granica do koje se prostiru tragovi označava se kao šire lice mjesta. Na primjer, prilikom saobraćajne nezgode, uži dio lica mjesta je mjesto gdje je došlo do kontakta dva vozila ili vozila i pješaka, dok se šira granica prostire sve do mjesta gdje se mogu naći tragovi vezani za tu nezgodu (otpali dijelovi sa vozila, vlažan kolovoz koji je uslovio nezgodu...).

Nakon definitifnog određivanja granica lica mjesta ono se vidno obilježava specijalnim sredstvima (trake, čunjevi). U nedostatku specijalnih sredstava za obilježavanje, mogu se koristiti i priručna sredstva.

Uviđajna ekipa ne može, po prirodi stvari, odmah po izvršenju krivičnog djela izaći na lice mjesta. Tokom vremena potrebnog za to moguće su brojne promjene na licu mjesta izazvane uticajem različitih faktora.

Zbog toga je lice mjesta potrebno na adekvatan način obezbijediti, tj. spriječiti svaku eventualnu promjenu do dolaska uviđajne ekipe. Obezbjedenje lica mjesta obuhvata:

- pružanje prve pomoći povrijedjenim licima,
- otklanjanje neposredne opasnosti od požara ili eksplozije,
- preduzimanje mjera koje imaju za cilj sprječavanje promjena na licu mjesta i očuvanje predmeta i tragova krivičnog djela do dolaska uviđajne ekipe (prekrivanje lica mjesta najlonom u slučaju kiše),
- fiksiranje eventualnih promjena na licu mjesta na odoovarajući način (skica, fotografija),
- pronalaženje svjedoka,
- preduzimanje potrage za učiniocem krivičnog djela ukoliko je to cjelishodno u konkretnom slučaju.

Smatramo da bi trebalo naglasiti šta bi sve trebali uraditi policijski službenici koji se prvi zateknu na mjestu nekog krivičnog događaja prije dolaska uviđajne ekipe:

- zapisati imena svjedoka i drugih osoba koje su bile na licu mjesta kada su policijski službenici došli,
- ustanoviti ključne činjenice (o tome šta se desilo, po mogućnosti napraviti misaonu rekonstrukciju),
- držati potencijalnog osumnjičenog i svjedoček odvojenim,
- poučiti svjedoke da ne raspravljaju međusobno o događaju,
- ne diskutovati sa svjedocima ili drugim licima o događaju,
- zaštiti trageve od uništenja. [3]

2. FAZE UVIĐAJA

2.1. Orijentaciono-informativne aktivnosti koje prethode uvidaju

Radnje koje se preduzimaju u okviru ove faze imaju *informativni* karakter (prikljupljanje relevantnih informacija od ekipe koja je obezbjedivala lice mjesta i od potencijalnih svjedoka), *organizaciono-pripremni* karakter (preduzimanje pripremnih radnji i organizacija sprovođenja uviđaja) i *orientacioni* karakter (ustanavljava se položaj lica mjesta koje će biti obuhvaćeno uviđajem, određuju se tačke sa kojih će se vršiti mjerjenja, skiciranja itd.) [3]. Dakle, da bi sam uviđaj dao što bolje rezultate, veoma je bitno prikupiti što više relevantnih informacija od osoba zatečenih na licu mjesta (pa i od policijskih službenika koji su preduzimali radnje obezbjeđenja lica mjesta) ali i dobro se orijentisati (utvrditi prostorne karakteristike lica mjesta).

2.2. Statička faza uviđaja – pregled lica mjesta i fiksiranje zatečenog stanja

Ova faza uviđaja popularno se naziva i faza uviđaja „sa rukama u džepovima“, jer se u okviru nje ne unose nikakve promjene na licu mjesta. Prvi zadatak uviđajne ekipe po dolasku na lice mjesta jeste da izvrši detaljan vizuelni pregled. U pravilu, prilikom vizuelnog pregleda, na lice mjesta se ne ulazi. Prevashodni cilj pregleda lica mjesta jeste da se uoče tragovi i predmeti krivičnog djela i njihov međusobni raspored, odnosno da se dode do pretpostavke na kojim mjestima bi se mogli nalaziti latentni tragovi. Kad je god to moguće treba izvršiti misaonu rekonstrukciju događaja.

Nakon vizuelnog pregleda lica mjesta obilježavaju se svi tragovi koji su u vezi sa krivičnim djelom ili događajem. Tragovi se obilježavaju specijalnim oznakama (pločice sa brojevima ili slovima). Oznake se stavlju blizu traga, a ako je trag suviše mali uz oznaku se stavlja i strelica usmjerena prema uočenom tragu (npr. ispaljena čaura koja se nalazi u travi) [4]. Isto tako, neophodno je obilježiti i mjesta gdje se nalaze, ili se predpostavlja da se nalaze, nevidljivi (latentni) tragovi krivičnog djela.

Za fiksiranje izgleda lica mjesta koriste se sljedeće metode:

- opisivanje riječima (zapisnik o uviđaju),
- fotografisanje,
- skiciranje,
- makete i kompjutersko modelovanje činjeničnog stanja fiksiranog uviđajem,
- snimanje audio-vizuelnim uređajima.

Zapisnik o uviđaju je procesni dokument koji se obavezno sačinjava, a predstavlja jedan od načina fiksiranja izgleda lica mjesta. Isti treba da potpuno i detaljno prezentuje sve utvrđene relevantne činjenice i stanje na licu mjesta. Mora da bude sastavljen tako da čovjek koji ga čita, a koji nije bio na licu mjesta i nije ranije imao nikakvu predstavu o njemu, može na osnovu zapisnika sebi da predstavi potpunu sliku događaja [5]. Zbog nemogućnosti da se zapisnik o uviđaju sačinjava paralelno sa njegovim vršenjem (što bi bilo idealno), treba ga sastaviti odmah nakon toga, bez ikakvog odlaganja. Pored detaljnog opisa pronađenih tragova i predmeta krivičnog djela, sa kriminalističko-tehničkog stanovišta zapisnik mora da sadrži i detaljan opis terena na kome se događaj odigrao i objekata koji se na njemu nalaze [6].

Lice mjesta fiksira se tzv. uviđajnom fotografijom čiji je osnovni zadatak da što vjernije i preglednije dokumentuje sva zapažanja uviđajne ekipe, odnosno da zabilježi sve ono što je zatečeno na licu mjesta.

Fotografisanje zatečenog stanja lica mjesta treba izvršiti u tri faze i to:

- širi izgled lica mjesta sa okolinom,
- uži izgled lica mjesta iz više pravaca,
- dijelovi lica mjesta. [6]

Fotografisanje se vrši uvijek od šireg ka užem izgledu lica mjesta sve do fotografisanje svakog obilježenog traga. Kada je riječ o operativnoj fotografiji uopšte, za fiksiranje izgleda lica mjesta koriste se panoramska i linearna fotografija. Nužno je napomenuti da se prilikom fotografisanja mora voditi računa o opštim uslovima za dobijanje kvalitetne fotografije (foto-oprema, fotograf...). Od svih fotografija sačinjava se fotoelaborat kao dio tehničke dokumentacije uviđaja.

Nakon što se izgled lica mjesta fiksira zapisnički i fotografski, pristupa se izradi skice slobodnom rukom. U skicu se unose svi obilježeni tragovi i predmeti, njihove dimenzije, te rastojanja između njih. Skica ima određene prednosti u odnosu na zapisnik i fotografiju: *jednostavnost* (za izradu skice dovoljni su papir i olovka), *preglednost* (u skicu se ne unose irelevantne okolnosti), *preciznost* (skica se zasniva na mjerenu). Na osnovu skice sačinjava se situacioni plan lica mjesta, ali u kancelarijskim uslovima, od strane za to stručne osobe.

Kada to važnost slučaja nalaže, lice mjesta se može predstaviti u vidu makete koja se izrađuje na osnovu fotodokumentacije i situacionog plana. Maketama se plastično prikazuje situacija na licu mjesta, svi predmeti izrađeni su u tri dimenzije, a makete se prave u istoj srazmjeri. Paralelno sa razvojem informatike u svijetu se razvija i kompjutersko modelovanje stanja na licu mjesta.

U izuzetno važnim slučajevima ili kada to okolnosti konkretnog slučaja nalažu, tok uviđaja treba da bude fiksiran snimanjem audio-vizuelnim sredstvima. To danas nije nikakav problem s obzirom na dostupnost i kvalitet takvih uređaja.

2.3. Dinamička faza uviđaja

Kad je završena statička faza uviđaja i sve radnje u vezi sa njom, još jedanput se izvrši kontrola za slučaj da je nešto omaškom propušteno i pristupa se sljedećem poslu, dinamičkoj fazi uviđaja, koji za posljedicu ima određene promjene na licu mjesta [4]. Profesor Simonović [5] navodi da se u okviru dinamičke faze uviđaja obavljaju sljedeće radnje:

- *Izuzimanje predmeta i njihovo detaljno analiziranje*. Svi predmeti koji su pronađeni na licu mjesta uzimaju se u ruke zaštićene rukavicama nakon čega se detaljno analiziraju. Ovome treba pristupiti sa znatnom dozom opreza iz razloga što svi pronađeni predmeti mogu biti nosioci nekih drugih tragova. Takve tragove treba potražiti odmah na licu mjesta ako je moguće, a ako ne, to treba svakako učiniti u laboratorijskim uslovima.
- *Izazivanje i fiksiranje latentnih tragova*. Na osnovu misaone rekonstrukcije dolazi se do pretpostavki o mjestima na kojima se nalaze latentni (nevidljivi) tragovi. To npr. mogu da budu predmeti za koje se pretpostavlja da ih je učinilac krivičnog djela dodirivao. Za izazivanje latentnih tragova koriste se različite metode koje se grubo dijele na fizičke (pomoći raznih praškova – argentorat, zlatni prah, magnetni prah) i na hemijske (srebro-nitratom, ninhidrinom, osmijum-tetroksidom...). Izazvani latentni tragovi fiksiraju se fotografiski i pomoću daktiloskopskih folija (crne, bijele, providne).
- *Mulažiranje tragova*. Mulažiraju se reljefni tragovi. To su tragovi koji nastaju pritiskom nekog predmeta na meku podlogu (tragovi obuće na mekanom tlu). Mulažiranje se vrši ulijevanjem određene smjese (albaster gips najčešće) kako bi se dobio odlivak koji će služiti u svrhe kriminalističke identifikacije.
- *Pronalaženje i fiksiranje mikrotragova*. Mikrotragovi su, zapravo, minijaturni makrotragovi koji se ne mogu (ili se jedva mogu) uočiti golim okom, bez upotrebe nekih optičkih pomagala. Da bi se mikrotragovi pronašli potrebno izvršiti misaonu rekonstrukciju događaja i pretpostaviti gdje se oni nalaze, kao i pregledati lice mjesta pomoću nekih optičkih instrumenata (lupa, ultravioletna lampa, pokretni mikroskop i sl.). Za fiksiranje uočenih mikrotragova koriste se sljedeće metode: izuzimanje predmeta nosilaca mikrotragova, struganje (npr. sasušenih tragova krvii), upijanje (pomoću filter papira), korištenje nanelektrisane šipke ili ljepljive trake, usisavanje. Pored toga, svi mikrototragovi fiksiraju se zapisnički, fotografiski i skicom.
- *Pakovanje tragova i predmeta sa lica mjesta*. Vrši se na način da se spriječe sva eventualna oštećenja, kontaminacija ili gubljenje tragova i predmeta krivičnog djela. Koristi se različita ambalaža koja zavisi od vrste, veličine i drugih karakteristika traga ili predmeta (staklene kutije, plastične kutile, polietilenske kese, papirne vrećice, epruvete...). Na ambalaži obavezno treba naznačiti vrstu traga kao i broj kojim je trag obilježen.
- *Obezbjedenje materijala za komparaciju, dodatne analize i vještačenja*.
- *Fiksiranje odoroloških (mirisnih) tragova*. Vrši se radi kasnjeg predočavanja psu tragaču. Npr. pakovanjem nekog predmeta koji je pripadao učiniocu u hermetički zatvorene posude fiksira se mirisni trag.
- *Obavljanje situacionih i drugih vještačenja, rekonstrukcije, kriminalističkog eksperimenta i ostalih potrebnih operativnih i dokaznih radnji*.

Nakon završetka dinamičke faze, potrebno je izvršiti naknadni pregled lica mjesta kako bi uviđajna ekipa bila sigurna da nema tragova i predmeta koji su propušteni.

3. ZNAČAJ UVIĐAJA ZA OTKRIVANJE PRIJAVLJIVANJA FINGIRANIH KRIVIČNIH DJELA

Fingiranje, u kriminalističkom smislu, sastoji se u namjernom prikrivanju neke kriminalne radnje, nekim drugim krivičnim djelom ili sličnim događajem, s ciljem da se zavaraju organi otkrivanja i tako onemogući rasvjetljavanje krivičnog djela i otkrivanje izvršioca [7].

Mjesto kriminalnog događaja je materijalni okvir u kojem je moguće utvrditi vezu između prikrivenog krivičnog djela i djela koje se želi predstaviti, a uviđaj je, najčešće, jedina mogućnost da se to uradi [8]. Fingirana krivična djela razotkrivaju se pronalaženjem negativnih činjenica prilikom vršenja uviđaja. Primjeri negativnih činjenica: pištolj pronađen u desnoj ruci ljevorukog „samoubice“ ukazuje da se radi o fingiranju; nedostatak krvavih mrlja ispod leša kojih bi, prema okolnostima konkretnog slučaja (vrsta

povrede), trebalo biti ukazuje da je leš premješten sa nekog drugog mjesta; u slučaju provale prozor razbijen sa unutrašnje strane ukazuje na fingiranje i sl.

U cilju razotkrivanja fingiranih krivičnih djela treba se voditi pozнатом kriminalističkom maksimom „ko ne sumnja, ne može da otkrije“ i preduzeti određene mjere i radnje kao što su provjera alibija, tajna opservacija, prikupljanje obavještenja i dr.

ZAKLJUČAK

Uviđaj je najpouzdaniji način utvrđivanja činjenica u krivičnom postupku. Pored toga što mora biti preduzet u zakonskoj formi od strane organa koji vodi postupak, prilikom vršenja uviđaja moraju se poštovati principi kriminalistike i forenzičkih nauka uopšte, uz korištenje savremene opreme. Prije svega, da bi se uviđaj uspješno izvršio, neophodno je obezbijediti određene uslove. Prostorne granice lica mjesta moraju biti precizno određene, a svi tragovi i predmeti moraju se sačuvati od uništenja. Prije unošenja bilo kakvih promjena na lice mjesta, njegov izgled treba na valjan način fiksirati – mora se sačiniti fotodokumentacija, situacioni plan lica mjesta i zapisnik o uviđaju koji je procesni akt. Nakon toga, zadatak uviđajne ekipe je da pronađe i fiksira sve relevantne tragove krivičnog djela. Dokazna snaga uviđaja je izuzetno velika, veća od dokazne snage bilo koje druge radnje dokazivanja, jer organ postupka vrši neposredno čulno opažanje na licu mjesta kojim se postiže objektivno sagledavanje situacije.

LITERATURA

- [1] SIMONOVIĆ, B. i MATIJEVIĆ, M.: „*Kriminalistika taktika*“, Internacionalna asocijacija kriminalista, Banja Luka, 2007.
- [2] SIMOVIĆ, M. i SIMOVIĆ, V.: „*Krivično procesno pravo: uvod i opšti dio*“, Pravni fakultet univerziteta u Bihaću, 2013.
- [3] FISHER, B.: „*Techniques of Crime Scene Investigation*“, CRC Press, USA, 2003.
- [4] MAKSIMOVIĆ, R. i TODORIĆ, U.: „*Kriminalistika tehnika*“, Policijska akademija u Beogradu, 1995.
- [5] SIMONOVIĆ, B.: „*Kriminalistika*“, Pravni fakultet u Kragujevcu, Institut za pravne i društvene nauke, Kragujevac, 2004.
- [6] MITROVIĆ, V. i STUPAR, LJ.: „*Kriminalistika tehnika*“, Viša škola unutrašnjih poslova, Beograd, 2002.
- [7] KRIVOKAPIĆ, V., ŽARKOVIĆ, M. i SIMONOVIĆ, B.: „*Kriminalistika taktika*“, Viša škola unutrašnjih poslova, Beograd, 2005.
- [8] KRESOJA, M.: „*Kriminalistika: za osnovno policijsko obrazovanje*“, Yugo-PIRS, Temerin, 2006.

ZAKONI

1. Krivični zakon Bosne i Hercegovine (“Službeni glasnik Bosne i Hercegovine”, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15 i 40/15).
2. Zakon o krivičnom postupku Bosne i Hercegovine (“Službeni glasnik Bosne i Hercegovine”, br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 i 72/13).

ULOGA DNK VJEŠTAČENJA U RASVJETLJAVANJU NAJTEŽIH OBLIKA NASILNIH DELIKATA

Mladen Vuković, mr

Doktorand na Pravnom Fakultetu, Univerzitet u Novom Sadu, zaposlen u MUP RS, Uprava za policijsko obrazovanje, Visoka škola Unutrašnjih poslova, mladen_vukovic1983@yahoo.com

Apstrakt: *Suzbijanje kriminaliteta predstavlja stalni i veoma aktuelan i problematičan dio sveukupne bezbjednosne problematike i stanja u društvu. Najteža krivična djela među kojima su razbojništva i razbojničke krađe, kao tradicionalni oblici nasilnih imovinskih delikata, otkrivaju se najčešće klasičnim metodama i sredstvima, iako se u savremenim ulovima koriste nove metode i vještačenja koje doprinose još efikasnijem otkrivanju i suzbijanju ovih krivičnih djela. Analiza dezoksiribonukleinske kiseline (DNK analiza) predstavlja metodu kriminalističke identifikacije učinioца najtežih nasilnih delikata. U radu će se prezentirati, analizirati i problematizovati primjena D NK vještačenja u otkrivanju i rasvjetljavanju krivičnih djela razbojništva i razbojničkih krađa. Pored toga rad će sadržavati primjer iz kriminalističke prakse Centra javne bezbjednosti Banja Luka, Sektora kriminalističke policije, gdje je na osnovu primjene D NK analize rasvjetljeno teško krivično djelo razbojništva.*

Ključne riječi: D NK, razbojništvo, vještačenje, otkrivanje, dokazivanje

Abstract: *Combating crime is a constant and very current and problematic part of the overall security issues and the situation in the society. The most serious crimes including robbery and robbery, as well as traditional forms of violent property crimes, revealing the most common conventional methods and means, although in contemporary catches using new methods and expertise that contribute to more efficient detection and suppression of these offenses. The analysis of deoxyribonucleic acid (DNA) is a method of identifying crime committed most serious violent offenses. The paper will be presented, analyze and problematize the application of DNA expertise in discovering and disclosing criminal acts of robbery and theft of the band. In addition, work will include an example of the criminal practices of the Public Security Banja Luka, the Criminal Police Department, which is based on the application of DNA analysis elucidated serious crime of robbery.*

Keywords: DNA, robbery, expert analysis, detection, proving.

UVODNA RAZMATRANJA

Identifikacija lica (izvršioca krivičnih djela) na osnovu utvrđivanja D NK profila (na osnovu genetske kompozicije dobijene iz izuzetog biološkog materijala) predstavlja jednu od najnovijih i najsigurnijih metoda kriminalističke identifikacije. U svjedskim okvirima se koristi već oko dvadesetak godina, s tim da je unazad desetak godina koristi u našoj kriminalističkoj praksi. Kriminalističke metode identifikacije na osnovu utvrđivanja D NK profila pružaju izvanredne mogućnosti u otkrivanju i dokazivanju krivičnih djela. Na osnovu D NK analize i komparacije spornih i nespornih uzoraka veoma uspješno su rasvjetljavani najteži oblici nasilnih zločina razbojništva i razbojničkih krađa. Međutim stučna javnost ne bi smjela da izgubi iz vida domene, granice i ograničenja ovih metoda. Opasnosti od kontaminacije biološkog materijala kao i dokazivanje relevantnosti između traga i krivičnog djela predstavlja ozbiljne izazove koje organi unutrašnjih poslova, tužilaštvo, sud i naučna javnost moraju da imaju na umu. Od njih se očekuje da svako u svom domenu bude maksimalno svjestan vrijednosti ali i mogućnosti grešaka u radu sa D NK dokazima i da pruži doprinos njihovom predupređenju. Shodno navedenom u ovom radu će se prezentirati, analizirati i problematizovati primjena D NK vještačenja u otkrivanju i rasvjetljavanju krivičnih djela razbojništva i razbojničkih krađa. Pored toga rad će sadržavati primjer iz kriminalističke prakse Centra javne bezbjednosti Banja Luka, Sektora kriminalističke policije, gdje je na osnovu primjene D NK analize rasvjetljeno teško krivično djelo razbojništva.

1. ANALIZA DEZOKSIRIBONUKLEINSKE KISELINE

Analiza dezoksiribonukleinske kiseline označava skup primijenjenih biohemijskih i molekularno-genetičkih metoda za izdvajanje molekule DNK iz biološkog traga koji može poslužiti kao DNK uzorak, umnožavanje fragmenata određenih genetičkih lokusa iz izdvojenih molekula DNK, elektroforetsko razdvajanje umnoženih DNK fragmenata, detekciju razdvojenih fragmenata, utvrđivanje prisutnih varijanti alela na DNK fragmentu ili biološkom tragu (Simonović, 2002: 574). Članom 117 Zakona o krivičnom postupku Republike Srpske se precizira da će analizu DNK obavljati “institucija koja posjeduje potrebnu stručnost, u smislu osoblja i opreme, da obavlja forenzičku DNK analizu. Na osnovu preporuke o primjeni analize DNK u krivičopravnom sistemu broj (92) 1 Komiteta ministara država članica Savjeta Evrope koja je prihvaćena je na 470. sjednici od 10. februara 1992. godine je određeno da će se zemlje članice zalagati za standardizaciju analize DNK na nacionalnom i na međunarodnom nivou i to kroz međusobnu saradnju, te da će se međunarodna razmjena zaključaka analize DNK vršiti na način da će ona biti moguća samo između država koje prihvataju i ostvaruju uslove određene ovom preporukom, a posebno u skladu sa odgovarajućim međunarodnim pravilima razmjene podataka vezane uz krivične predmete, kao i u skladu sa članom 12 Konvencije o zaštiti podataka. Materijalni uslov za vršenje analize DNK sastoji se u postojanju neophodne potrebe da se takvom analizom odredi identitet ili činjenice da li tragovi materija koji su otkriveni potiču od osumnjičenog, odnosno optuženog ili oštećenog (Primorac, 2009: 205) (član 178). Formalni uslov za ovo vještačenje se u zakonu posebno ne utvrđuje, pa treba smatrati da u tom pogledu važe opšta pravila koja se inače odnose na formalni uslov za određivanje vještačenja (Jekić, Škulić, 2002: 278). U cilju utvrđivanja identiteta osumnjičenog, odnosno optuženog, sa njegovog tijela se mogu uzeti ćelije radi analize DNK, a podaci dobijeni na ovaj način mogu se koristiti i u drugim krivičnim postupcima protiv istog lica (član 179), zbog čega se nalazi tih analiza pohranjuju na jednom mjestu i vode u posebnom registru pri Ministarstvu bezbjednosti BiH (član 180 stav 1). Ovlašćenje da donese pravilnik o načinu prikupljanja i uzimanja uzorka biološkog materijala za potrebe analize DNK u krivičnom postupku, o načinu pakovanja prikupljenog biološkog materijala, čuvanja, obrade i pohranjivanja uzorka i dobijenih rezultata DNK analiza u BiH – ima ministar pravde BiH (član 180 stav 2). On je to učinio donošenjem Pravilnika o načinu prikupljanja i uzimanja uzorka biološkog materijala za potrebe analize dezoksiribonukleinske kiseline u krivičnom postupku. Za DNK analizu u krivičnom postupku prikupljaju se i uzimaju svi dostupni i upotrebljivi uzorci spornog i nespornog biološkog materijala (član 2 Pravilnika).

Postupak analize (član 10 Pravilnika): forenzička DNK analiza iz uzorka biološkog materijala obavlja se u skladu sa molekularno-biološkim postupcima koji su utvrđeni međunarodnim standardima prihvaćenim u BiH, uključujući preporuke Savjeta Evrope i standarde Interpola. Interpol je takođe uspostavio Interpolov DNK protokol (Interpol DNA Gateway), kreiran da bi olakšao uspoređivanje DNK profila između država članica Interpola. Interpol održava bazu podataka DNK profila, a svaka joj država članica (nakon usvajanja povelje kojom se osigurava njena sigurna upotreba) može pristupiti putem Interneta. Baza sadrži više od 69.000 DNK profila koje je pohranilo 45 država članica. Naime DNK analize obavljaju institucije koje u skladu sa članom 177 posjeduju potrebnu stručnost, u smislu osoblja i opreme, da obavljaju forenzičku DNK analizu. Rezultat DNK analiza je DNK profil koji se može numerički predstaviti kao niz parova brojeva, pri čemu svaki par brojeva opisuje oba alela prisutna na određenom genskom lokusu, jedan naslijeden od majke i drugi naslijeden od oca (Marjanović, Primorac, 2011: 231). Numerički zapis DNK profila je posebno koristan u forenzičkoj genetici, jer se dva DNK profila lako mogu uporediti. Poređenje DNK profila se vrši na jednostavan način: da bi dva profila bila podudarna, čitav spisak alela prisutnih na svim analiziranim genskim lokusima mora biti potpuno identičan. Ukoliko je potrebno brzo uporediti veoma veliki broj DNK profila, kao što je slučaj u bazama podataka sa DNK profilima osuđenih učinilaca krivičnih djela, savremene kompjuterske tehnologije se mogu lako primijeniti u ovoj oblasti. Dakle, ako dva analizirana traga potiču od istog lica, tada na svim analiziranim genskim lokusima moraju biti prisutne sve iste varijante (Marjanović, 2011: 136).

Analiza DNK, kao sofisticirana metoda i „novi naučni dokaz“ u forenzičkim naukama traži jasna pravila uzimanja, manipulisanja, čuvanja i raspolaganja uzorcima i podacima do kojih se dođe analizom tih uzorka. Ona je najprecizniji metod identifikacije svakog traga humanog porijekla, pa samim tim i najjači dokaz o identitetu uzorka (Modly, 2001: 22).

Ova metoda se sve više koristi prilikom utvrđivanja identiteta nestalih lica u toku sudsko-medicinskog vještačenja, bilo da je riječ o oružanim sukobima ili masovnim smrtnim posljedicama uslijed terorističkih napada (Primorac, 2001:71). Identifikacija lica na osnovu analize molekula DNK predstavlja metodu vještačenja kojom se istražuje sporni biološki materijal tako što se iz ćelije ekstrahuje DNK kako bi se posebnim metodama ispitali određeni dijelovi njenog lanca sa ciljem da se identificuje genetski materijal pojedinca, koji je individualan i neponovljiv (Primorac&Butorac&Adamović, 2009: 3).

DNK profilisanje je proces koji počinje kada se iz biološkog traga ekstrahuju dijelovi genetskog materijala (DNK), kako bi se utvrdio genetski profil ostavioca, koji se vizuelizuje i prikazuje kao numerička vrijednost, a završava sprovodenjem komparativne analize sa biološkim uzorcima poznatog porijekla (ili drugim biološkim uzorcima nepoznatog porijekla) kako bi se identifikovao ostavilac traga (ili utvrdilo učešće istog lica u izvršenju većeg broja krivičnih djela) (Obradović, 2008: 124). Ova vrsta vještačenja najčešće se naziva metoda utvrđivanja D NK otiska, čime se želi ukazati na njenu preciznost pri izolovanju unikatnih dijelova u okviru DNK lanca i napraviti asocijaciju na klasične metode identifikacije po otiscima prstiju. Kao što ne postoje dva lica koja imaju isti otisak prsta, ne postoje ni dva lica koja imaju isti genetski profil. Metoda je apsolutno pouzdana pri eliminaciji nevinih lica i veoma sigurna pri pozitivnoj identifikaciji izvršilaca. Koristeći se D NK analizom nedavno su neke države, poput Španije, pokrenule međunarodni program s ciljem pronalaženja nestale djece. SAD su pokrenule tzv. „DNA innocence project“ s ciljem oslobođanja lica pogrešno optuženih za izvršenje krivičnog djela, koji je u posljednjih desetak godina oslobođio stotinjak lica od kojih su neka bila osuđena na smrtnu kaznu (Marjanović&Primorac, 2009: 57). Međutim, i pored toga što je D NK vještačenje nova i moćna tehnologija, ona ne može da zamjeni druge metode, na primjer, daktiloskopiju, vještačenje tkanina, tragove oruđa itd. Bez obzira na njenu superiornu diskriminacionu snagu, ona bi kao tehnologija izbora trebalo da bude upotrebljena paralelno sa drugim kriminalističkim metodama.

2. PRIMJER D NK ANALIZE IZ KRIMINALISTIČKE PRAKSE CENTRA JAVNE BEZBJEDNOSTI BANJA LUKA

Dana 10.11.2009. godine oko 07.40 časova u Banja Luci, u naselju Vrbanja, u Ul. Rade Radića broj 30, u prostorijama „Pošte Srpske“, AD Banja Luka, radna jedinica Vrbanja, od strane tri –NN- lica maskirana i naoružana vatrenom oružjem – automatskom puškom i pištoljem, izvršeno je krivično djelo Razbojništvo iz člana 233. stav 2. KZ-a RS nad radnicima Pošte Srpske: M. S., Š. S. i B. A., prilikom čega je otuđen novac u iznosu od 74.050,01 KM.

Navedeno krivično djelo je izvršeno na taj način što su se NN izvršioci, dana 10.11.2009. godine oko 07,40 časova dovezli putničkim vozilom marke „Audi 80“, crvene boje, a na kojem su se nalazile nepripadajuće reg. oznake 486-J-544, ispred objekta Pošte nakon čega su iz vozila izašla dva NN lica, naoružana vatrenom oružjem automatskom puškom i pištoljem, u tamnim kombinezonima, i maskirani u predjelu glave crnim kapama – fantomkama, dok je treće lice ostalo u vozilu. Tom prilikom su dva NN izvršioca prišla ulaznim vratima objekta Pošte Srpske, te s obzirom da su ista bila zaključana, jedan od NN. izvršilaca je udario nogom u predjelu brave vrata, te nasilno otvario ista, nakon čega su oba NN izvršioca ušla u prostorije pošte.

U tom trenutku radnici pošte M. S., Š. S. i B. A su iz šalter sale, iz straha za svoju bezbjednost, utrčali u pomoćnu prostoriju pošte, nakon čega za njima uz povike lezi dole i gde su pare, utrčala i dva NN izvršioca. Ulaskom NN izvršilaca, radnici pošte su legli na pod, prilikom čega je jedan od NN izvršilaca, sa automatskom puškom u ruci, udario nogom radnika pošte B. A. u predjelu stomaka, te uz povike lezi dole i gde su pare radnicu pošte M. S. uhvatio za kosu, nakon čega je izgovorio: " penzije su, znam da ima novca, daj novac". Potom je drugi NN izvršilac stavio pištolj u predjelu glave radniku pošte Š. S. Zatim NN izvršilac naoružan pištoljem prilazi radnoj površini iza šaltera gdje na istoj pronalazi novac u različitim apoenima namjenjen za isplatu penzija, te isti otuđuje nakon čega su dva NN izvršioca uz povike: "lezi dole", trčećim korakom otišla do vozila koje ih je čekalo ispred objekta te u isto sjeli a zatim se udaljili velikom brzinom magistralnim putem u pravcu Čelinca.

Odmah po saznanju radnici CJB SKP Banja Luka su preduzeli niz aktivnosti iz svoje nadležnosti, izašli na lice mjesta i po predhodnoj saglasnosti i ovlaštenju okružnog tužioca OT Banja Luka G. M. pristupili vršenju uviđaja te nakon izvršenog uviđaja isti su pristupili pretresu uže i šire okoline terena koji se nalazi u neposrednoj blizini lica mjesta u cilju pronaalaženja eventualno odbačenih predmeta koji potiču iz navedenog krivičnog djela. Paralelno sa ovim aktivnostima, radnici policije i krim inspektorji drugih organizacionih jedinica CJB Banja Luka, nakon dobijenih početnih saznanja o načinu izvršenja KD i opisu NN izvršilaca, započeli su intenzivnu potragu na lokalitetima za koje se osnovano sumnjalo da se na istima mogu sakriti NN izvršioci. Takođe radnici policije su obavili više informativnih razgovora na terenu o čemu su sačinili službene zabilješke. Tom prilikom radnici CJB SKP Banja Luka pregledom uže i šire okoline lica mjesta, su pronašli predmete i tragove koji bi se mogli dovesti u vezu sa navedenim krivičnim djelom. U mjestu Bijeli Potok, opština Čelinac, radnici policije su pronašli odbačeno i zapaljeno vozilo za koje se osnovano sumnja da je isto korišteno kao sredstvo izvršenja KD tj. vozilo kojim su se NN izvršioci dovezli do objekta „Pošte Srpske“ a zatim se, nakon izvršenog krivičnog djela udaljili u pravcu Čelinca Na vozilu je izvršen uviđaj te su tom prilikom pronađeni predmeti i tragovi koji će biti predmet daljeg vještačenja. Po završetku uviđaja radnici CJB SKP Banja Luka su uzeli izjave na zapisnik od radnika M. S., Š. S, i B. A. koji su se nalazili u prostorijama Pošta Srpske u trenutku izvršenja KD Razbojništvo iz člana 233 stav 2 KZ RS. Na licu mjesta uviđaja na zapaljenom vozilu pronađena je nagorjela fantomka koju je jedan od izvršioca imao na glavi. U skladu sa pravilima kriminalističke struke pomenuti trag je zapakovan u papirnu vrećicu zapečaćen i uz naredbu za DNK vještačenje proslijeđen u Institut za genetički inženjeri i biotehnologiju Sarajevo gdje je po Dr Damiru Marjenoviću izvršena DNK analiza spornog traga prilikom čega je ekstrahovan pun DNK profil nepoznatog muškarca. Koliki je značaj i efikasnost DNK vještačenja vidljivo je u tome što je pomenuti trag fantomka u trenutku izuzimanja bila nagorjela a ista je pronađena u blatu u neposrednoj blizini zapaljenog automobila. Daljim operativnim radom policijski službenici CJB Banja Luka Sektora kriminalističke policije su došli do informacija da je lice B. J. pružio pomoć jednom od izvršioca na taj način što je pod svojim imenom istoga liječio od povreda –opekotina koje je dobio prilikom paljenja vozila. Nakon svih provjera i saslušavanja lica B. J. isti je priznao da je po svojim imenom hospitalizovao lice M. V. i da je njemu i njegovom drugu J. J. nakon izvršenja krivičnog djela razbojništva pružio utočište.

Nakon lišenja slobode M. V. i J. J. od istih je izuzet bris bukalne sluznice te su isti prosleđeni u Institutu za genetički inženjeri i biotehnologiju Sarajevo gdje je po Dr Damiru Marjenoviću izvršena DNK analiza i komparacija sa DNK profilom koji je ekstrahovan iz nagorjele fantomke. Nakon izvršene komparacije nalazom i mišljenjem Dr Damira Marjanovića nesporno je utvrđeno da postoji potpuna podudarnost spornog DNK profila i DNK profila lica M. V.

Nakon podnesenog izvještaja protiv lica V. M. i J. J. od strane sudije za prethodni postupka određen je pritvor, a isti su u sudkom postupku pravosnažno osuđeni na visoke zatvorske kazne. Kako je iz primjera vidljivo u ovom predmetu uz upotrebu savremene metode kriminalističke identifikacije odnosno DNK analize je uspješno riješeno teško nasilničko krivično djelo. Bez DNK analize istraga bi i dalje "takala u mjestu" a izvršioci bi bili na slobodi.

3. ZAKLJUČNA RAZMATRANJA

U našoj kriminalističkoj praksi DNK analiza se vrlo uspješno i efikasno primjenjuje (uz zakonsku regulativu) oko desetak godina. Imajući u vidu prilično veliki broj izvršenih teških naslinih krivičnih djela posljednjih godina u našoj zemlji potrebno je vršiti stalnu edukaciju kriminalističkih tehničara i policijskih službenika o pravilnoj upotrebi DNK analize. Kroz navedene edukacije policijski službenici bi se edukovali o načinu izuzimanja i čuvanja DNK materijala sa lica mjesta, uzimanja DNK uzorka bukalnog brisa od osumnjičenog lica, ko daje naredbu za uzimanje, labaratorije u kojima će se vršiti DNK vještačenje, upotreba baza DNK profila itd. Međutim stučna javnost ne bi smjela da izgubi iz vida domene, granice i ograničenja ovih metoda. Opasnosti od kontaminacije biološkog materijala kao i dokazivanje relevantnosti između traga i krivičnog djela predstavlja ozbiljne izazove koje organi unutrašnjih poslova, tužilaštvo, sud i naučna javnost moraju da imaju na umu. Od njih se očekuje da svako u svom domenu bude maksimalno svjestan vrijednosti ali i mogućnosti grešaka u radu sa DNK dokazima i da pruži doprinos njihovom predupređenju.

Samo ozbiljnim pristupanjem u radu sa DNK dokazima može se povećala efikasnost državnih organa u borbi protiv kriminaliteta kao društveno štetne i negativne pojave, kako u represivnom tako i u preventivnom smislu. Kriminalističke metode identifikacije na osnovu utvrđivanja DNK profila pružaju izvanredne mogućnosti u otkrivanju i dokazivanju krivičnih djela što smo vidjeli i na primjeru kriminalističke prakse Centra javne bezbjednosti Banja Luka, te njihovim uvođenjem u sudsku praksu otvoreno je novo poglavlje savremene kriminalistike.

LITERATURA

- [1] Marjanović D., Primorac D. (2009). *Molekularna forenzična genetika*. Sarajevo.
- [2] Milosavljević M., Milosavljević D., Milosavljević S., (2011). *Forenzičko-kriminalistički aspekti identifikacije (tragova) kostura (leševa) u segmentu forenzičke bioantropologije*. Banja Luka.
- [3] Milosavljević M. (2000). *Osnovi forenzičke biologije*, Sarajevo.
- [4] Modly, D. (1998.), *Kriminalistička metodika*, Sarajevo.
- [5] Modly, D. (2001), *Prikupljanje bioloških neutralnih komparativnih uzoraka humanog porijekla za potrebe vještačenja*, Sarajevo.
- [6] Obradović, D., (2008). *DNK vještačenje sa posebnim osvrtom na njegovu primjenu kod krivičnih djela protiv bezbjednosti javnog saobraćaja*. Beogradb
- [7] Primorac, D. (2001), *Primjena analize DNA u sudskoj medicini i pravosuđu*, Zagreb.
- [8] Primorac, D., Butorac, S. i Adamović, M., (2009). *Analiza DNA u sudskoj medicini i njena primjena u hrvatskom krivičnopravnom sistemu*, Zagreb.

PRAKTIČNA PRIMJENA KRIPTOGRAFIJE U SQL-U KAO NAČINA ZAŠTITE BAZE PODATAKA U SLUČAJU CYBER NAPADA

Mahir Zajmović¹, Hadžib Salkić², Haris Hamidović³

Fakultet informacijskih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez, BiH,
mahir.zajmovic@unvi.edu.ba

Fakultet informacijskih tehnologija, Sveučilište/Univerzitet „Vitez“ Vitez, BiH,
hadzib.salkic@unvi.edu.ba

Stalni sudski vještak IKT struke, Tuzla, Bosna i Hercegovina, mr.
haris.hamidovic@ieee.org

Apstrakt: U ovom radu prikazana je praktična primjena simetričnih kriptografskih algoritama u bazi podataka, korištenje istih kao ugrađenih sistema zaštite SQL Servera u slučaju neželjenih napada od strane neovlaštenih korisnika, prednosti i nedostatci korištenja istih. Testiranje je izvršeno u sistemu za upravljanje bazama podataka Microsoft SQL Server 2014.

Ključne riječi: kriptografija, simetrični algoritmi, baze podataka, Microsoft SQL Server, zaštita

Abstract: This paper describes the practical application of symmetric cryptographic algorithms in the database, use the same as a built-in system of protection of SQL Server in the event of unwanted attacks by unauthorized users, the advantages and disadvantages of using them. Testing was performed in the system for managing databases, Microsoft SQL Server 2014.

Keywords: cryptography, symmetric algorithms, databases, Microsoft SQL Server, protection

1. UVOD

Microsoft SQL Server platformu i servise čine:

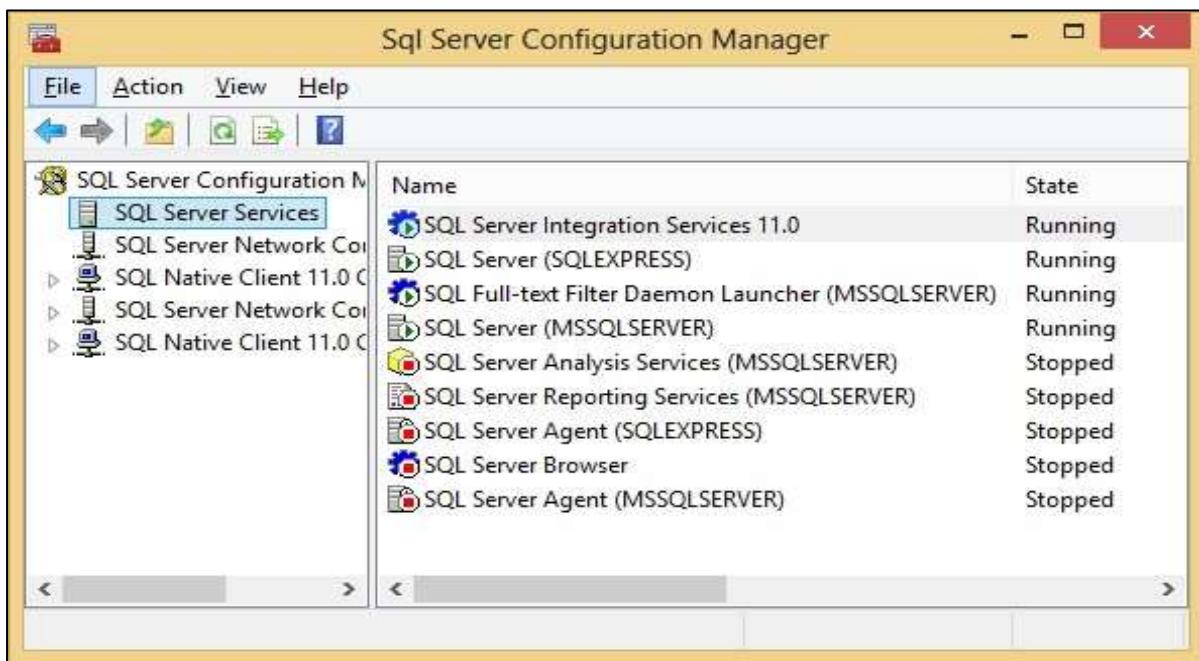
1. Database engine – osnovni servis koji predstavlja relacionu bazu podataka
2. Analysis servis – servis koji služi za analitičko procesiranje podataka, multidimensional upite i analize.
3. Reporting servis – kreiranje izveštaja, integracija sa SharePoint platformom.
4. Integration servis – ETL (Extract Transform & Load) funkcionalnosti za razmjenu i transformaciju podataka.

Ostali servisi i funkcionalnosti: replikacija, full-text pretraga, Data Quality servis i Master Data servis.

Vecina servisa zahtjeva nalog pod kojim će se prijaviti na sistem (lokalni računar ili domena) gdje se instalira. Najčešće se koristi lokalni nalog koji pripada lokalnoj Administrators grupi, a česte su situacije gdje se koristi nalog koji pripada Domain Admin grupi. Obje varijante (posebno druga), su veoma opasne i treba ih izbjegavati. Ako dođe do upada u servis, napadač stiče prava na sistemu koja ima servis čime mu olakšavamo posao.

Prilikom instalacije Microsoft SQL Servera automatski se nude novi različiti nalozi za svaki od njih, a sama instalaciona procedura će napraviti naloge i podesiti minimalni set potrebnih prava kako bi servisi ispravno funkcionisali. Da bi iskoristili ovu mogućnost instalacionog programa, moramo ga pokrenuti u bezbjednosnom kontekstu lokalnog ili domenskog administratora ako želimo da napravi domenske naloge.

Nalozi koje koriste servisi se mogu naknadno promijeniti preko "Sql Server Configuration Manager" alata koji dolazi uz SQL Server ili pomoću Services aplet-a u okviru Administrative tools grupe na Windows računaru.



Slika 1. Sql Server Configuration Manager

2. AUTENTIFIKACIJA I AUTORIZACIJA

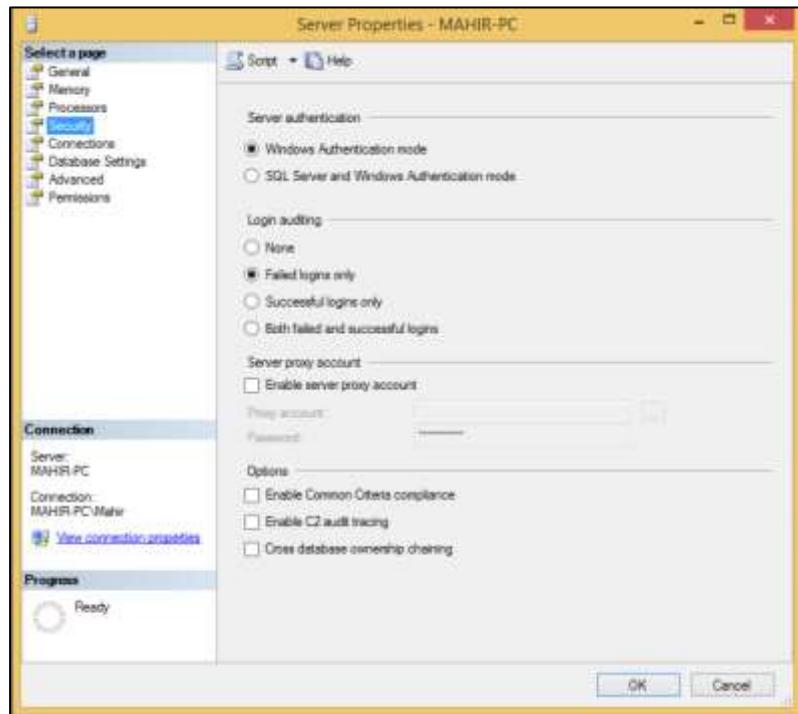
Autentifikacija je proces predstavljanja/identifikacije korisnika nekom sistemu na osnovu koga sistem dozvoljava ili ne dozvoljava pristup svojim resursima.

Autorizacija je proces dodjele prava autentifikovanom korisniku. Određuje koje resurse može koristiti i na koji način.

SQL Server poznaje dva načina autentifikacije:

1. **SQL Server autentifikacija** gdje SQL Server vrši autentifikaciju korisnika upotrebom user name/password para. Mora se koristiti u mrežama bez domena ili za pristup serveru koji je publikovan na javnom Webu direktno preko TCP/IP protokola. Može se naravno koristiti i u mrežama koje imaju domenu ali tada je bolje koristiti drugi način autentifikacije.
2. **Windows autentifikacija** (takođe od ranije poznata po imenima Trusted i Integrated), gdje autentifikaciju vrši Windows domain controller. SQL server administrator određuje koje domenske grupe i korisnici mogu da se autentikuju na SQL server, pa na taj način SQL Server „veruje“ (trust) Windows sistemu autentifikacije. Ovo je preporučljiv vid autentifikacije na SQL Server jer se koriste napredni Windows mehanizmi, smart kartice, domenske polise i slično.

Aktivni način autentifikacije, kao i opcije praćenja logovanja se postavljaju preko Server properties dijaloga.



Slika 2. Server properties dialog

Kod obje vrste autentifikacije korisnici se upisuju u sistemsku tabelu čiji sadržaj možemo vidjeti (ne i mijenjati), preko view-a **sys.syslogins** koji enkapsulira podatke:

```
SELECT * FROM sys.syslogins
```

Kolona „password“ sadrži HASH passworda u slučaju SQL Server naloga, odnosno NULL vrijednost u slučaju naloga koji koristi Windows autentifikaciju. U drugom slučaju password se nalazi u Active Directory bazi, takođe u HASH obliku.

Preporuke:

- Instalirati samo potrebne servise i time smanjiti potencijalnu površinu za napad
- Poslije instalacije zaustaviti servise koji se još uvijek ne koriste u produkciji
- Gdje god je moguće koristiti Windows autentifikaciju
- Ako se mora koristiti SQL Server autentifikacija postaviti polise za kompleksnost šifre
- Izbrisati ili onemogućiti (disable) guest korisnika u svakoj bazi:
`USE ImeBaze
REVOKE CONNECT FROM [guest]`
- Voditi računa o ispravnom korištenju Public role
- Izmjeniti default TCP/IP port (1433)
- Uključiti praćenje logovanja/neuspješnog logovanja na server
- Voditi računa o potencijalno opasnim naredbama i mogućnostima: xp_cmdshell, CLR integracija,...
- Ukloniti zaostale logine iz razvojne faze...
- Onemogućiti SQL Server sa administratorski login;
`ALTER LOGIN [sa] DISABLE`

ili mu promijeniti ime:

```
ALTER LOGIN sa WITH NAME = NovoIme
```

- Redovno primjenjivati ažuriranja i servisne pakete – manualno, nikako automatski.
- Sarađivati sa razvojnim timom i administratorima mreže i domena.

3. KRIPTOGRAFIJA

Microsoft SQL Server posjeduje sve potrebne opcije vezane za kriptografiju koje su jednostavne za korištenje. Također je moguće proširiti postojeće mogućnosti upotrebom extended stored procedura pisanih u C++ programskom jeziku, ali ova opcija će biti uklonjena u slijedećim verzijama SQL Servera. Najbolje je ovo uraditi pomoću CLR (Common Language Runtime) integracije, odnosno integracije sa .NET platformom i .NET programskim jezicima.

3.1. HASH funkcija

HASH je irreverzibilna funkcija koja za isti ulaz različite veličine vraća isti izlaz fiksne dužine. Na primjer, ako se uradi HASH email poruke, nezavisno od njene dužine dobit će se rezultat fiksne dužine – hash (zove se i *digest*).

Ako primaocu pošaljemo poruku i njen kriptovan hash, on može da ponovo uradi hash poruke i usporediti ga sa poslatim. Ako su isti, poruka nije modifikovana. Također se koristi za čuvanje šifara, pa se prilikom logovanja unesena šifra hash-uje i onda upoređuje sa sačuvanim hash-om. Taj sistem koristi SQL Server, Windows security sistem, a također je široko korišten kod developera prilikom implementacije aplikativne bezbjednosti.

Postoji više HASH funkcija, a SQL Server podržava sve koji se standardno koriste.

TSQL programski jezik posjeduje funkciju **HashBytes** koja implementira sve podržane HASH funkcije. Ulazni parametri su tip hash funkcije i string koji treba „heshovati“. Izlaz je tipa varbinary i predstavlja digest zadatog stringa. Podržani HASH algoritmi su: MD2, MD4, MD5, SHA, SHA1, SHA2_256 i SHA2_512.

The screenshot shows the SQL Server Management Studio interface. In the Query Editor window, a T-SQL script is displayed:

```
USE StudentskaSluzba
GO
SELECT
    IDStudenta,
    Prezime,
    Ime,
    HashBytes ('SHA2_512', Jmbg) AS PwdHash
FROM
    tblStudenti
```

The Results pane displays the output of the query:

IDStudenta	Prezime	Ime	PwdHash
1	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
2	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
3	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
4	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
5	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
6	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
7	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540
8	Neznanec	Nikola	0x5CCDFE38CE09C3D000C16B73AFED890F190DEA29540

At the bottom of the Results pane, a message indicates: "Query executed successfully."

Slika 3. Digest šifra kolone „Jmbg“ iz tabele „tblStudenti“

3.2. Transparent Data Encryption (TDE)

TDE je mehanizam gdje SQL Server automatski vrši enkripciju svih fajlova date baze podataka (data i log). Služi kao zaštita od fizičke krađe fajlova koji predstavljaju bazu podataka. Zaštićeni su certifikatom koji se nalazi u certificate skladištu domena ili SQL Servera.

Enkripcija se jednom podesi i poslije toga je transparentna za korisnika. Enkripcija se vrši u realnom vremenu i na raspolaganju su AES_128, AES_192, AES_256 i 3DES simetrični kripto algoritmi - koriste se simetrični algoritmi zbog veće brzine u odnosu na asimetrične.

Ne povećava se značajno veličina fajlova koji se kriptuju, ali se povećava opterećenje procesora zbog potrebe stalne enkripcije i dekripcije blokova podataka prilikom čitanja, izmjene, dodavanja i brisanja podataka.

Backup ovakve “TDE enabled” baze je također kriptovan i ako želimo da uradimo njen Restore na drugom serveru moramo prenijeti i certifikat sa originalnog servera. Ako se kreira Mirror TDE baze, on je također kriptovan. Isto važi ukoliko se uspostavi Log Shipping TDE baze ka jednom ili više target servera.

3.3. Kriptovanje pojedinačnih kolona (podataka) u tabeli

Ovaj mehanizam omogućava kriptovanje podataka na nivou kolone u tabeli SQL Server baze podataka. Fizički, podaci se skladište u kriptovanom obliku u data fajlu baze podataka. Mehanizam je procesno manje zahtjevan od prethodnog TDE jer se ne kriptuje cijela baza (odnosno data i log fajlovi) već tipično samo njen mali dio.

Izuzetno je korisno ako treba zaštiti samo određene informacije – lične podatke, brojeve platnih kartica i tome slično. Postupak je malo složeniji u odnosu na TDE jer se podaci moraju eksplicitno dekriptovati i enkriptovati – respektivno funkcije ENCRYPTBYKEY i DECRYPTBYKEY. Obje funkcije zbog potrebe za brzinom koriste simetrične ključeve, odnosno algoritme: RC2, RC4, DES, 3DES, DESX, AES_128, AES_192, AES_256. Kriptovani podatak se u tabeli čuva u varbinary formatu.

```
/* kreiramo tabelu "Korisnici" */
CREATE TABLE Korisnici
(
    ID           int          NOT NULL PRIMARY KEY,
    KorisnickoIme nvarchar(50) NULL,
    Lozinka      nvarchar(50) NULL,
    LozinkaCrypto nvarchar(max) NULL,
);

/* kreiramo master key za bazu podataka "test"
nije nikako vidljiva i potrebna je jedino ukoliko radimo restore baze
podataka */
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Pa$$word'

/* kreiramo certifikat i koristimo ga da enkriptujemo simetricni kljuc */
CREATE CERTIFICATE CertTest
WITH SUBJECT = 'Certifikat za bazu podataka test',
START_DATE = '2016-03-01 10:00:00.000',
EXPIRY_DATE = '2016-03-30 23:00:00.000';

/* kreiramo simetricni kljuc po algoritmu AES 256 bita */
CREATE SYMMETRIC KEY SymKeyTest WITH ALGORITHM = AES_256
ENCRYPTION BY CERTIFICATE CertTest;

/* otvaramo ključeve kako bi isti bili spremni za koristenje */
OPEN SYMMETRIC KEY SymKeyTest
DECRYPTION BY CERTIFICATE CertTest;

/* koristenjem komande UPDATE setujemo kolonu LozinkaCrypto vrijednoscu iz
kolone Lozinka */
```

```

UPDATE Korisnici
SET LozinkaCrypto = ENCRYPTBYKEY(KEY_GUID('SymKeyTest'),Lozinka);

SELECT * FROM Korisnici;

/* uradimo komparaciju da li je ono sto pise zaista i uradjeno */
SELECT Lozinka, LozinkaCrypto AS 'Sifrovano',
CONVERT(nvarchar, DECRYPTBYKEY(LozinkaCrypto)) AS 'Desifrovano'
FROM Korisnici;

/* dekriptovanje kolone LozinkaCrypto */
UPDATE Korisnici
SET LozinkaCrypto=CONVERT(nvarchar,DECRYPTBYKEY(LozinkaCrypto));

SELECT * FROM Korisnici;

/* brisanje */
DROP SYMMETRIC KEY SymKeyTest
DROP CERTIFICATE CertTest
DROP MASTER KEY

```

ID	KorisnickoIme	Lozinka	LozinkaCrypto
1	mahir	mahir	•サヨウノ恋魔晄
2	jaomin	jaomin	•サヨウノ恋魔晄
3	hadzib	hadzib	•サヨウノ恋魔晄
4	hams	hams	•サヨウノ恋魔晄

Slika 4. Prikaz kolone "Lozinka" u plain text formatu i kriptovanom formatu

4. ZAKLJUČAK

- Prvo obezbjediti operativni sistem, pa potom i SQL Server
- Kontrolisati admin pristup serveru i bazama podataka
- Kriptovati podatke između klijenta i SQL servera ako to zahtjeva polisa firme
- Uvijek kriptovati povjerljive podatke u bazi
- Smanjiti potencijalnu površinu napada isključivanjem servisa i opcija koje nisu potrebne
- Koristiti Windows režim autentifikacije gdje god je moguće
- Raditi redovni audit servera i akcija koje se sprovode nad podacima i objektima

5. LITERATURA

- [1] Zajmović M., Salkić H., Obrodaš I.: „MICROSOFT SQL SERVER 2014 BACKUP ENRIPTION“, Zbornik radova, YU INFO 2016, Društvo za informacione sisteme i računarske mreže Srbije, Beograd, Srbija, 2016. godine
- [2] Milosavljević M.: „Microsoft SQL Server 2012 bezbednost i praktični primeri“, INFOTEH 2012, Elektrotehnički fakultet, Univerzitet u Istočnom Sarajevu, Jahorina, BiH, 2012. godine
- [3] [http://msdn.microsoft.com/enus/library/ms174415\(v=sql.110\).aspx](http://msdn.microsoft.com/enus/library/ms174415(v=sql.110).aspx)
- [4] [http://msdn.microsoft.com/enus/library/ms174361\(v=sql.110\).aspx](http://msdn.microsoft.com/enus/library/ms174361(v=sql.110).aspx)
- [5] [http://msdn.microsoft.com/enus/library/ms143504\(v=sql.110\).aspx](http://msdn.microsoft.com/enus/library/ms143504(v=sql.110).aspx)

VIJESTI IZ SVIJETA CYBER KRIMINALA I FORENZIKE

Animirane mape kiber napada u realnom vremenu u svijetu

Ako redovno pratimo vesti iz domena informacione bezbednosti ubrzo ćemo zaključiti da skoro svakoga dana možemo da pročitamo nove naslove o kiber napadima na različite web sajtove ili računarske mreže. Još 2013. godine statistike su pokazivale da se u svetu dnevno dogodi oko 7.000 DOS napada. Kada se uzme u obzir da se njihov broj od tada konstantno povećava i da pored DOS napada postoje i mnogi drugi, postavlja se pitanje kako prosečan čitalac može da na vizuelan način pojmi ovakva događanja. Neke od kompanija koje se bave zaštitom informacionih sistema odlučilo je da situaciju u kiber prostoru prikažu pomoću animacija. One koje su se odlučile na taj poduhvat kao osnovu za animacije upotrebile su podatke o napadima zabeleženim pomoću njihovih infrastrukture. Naravno, s obzirom na frekvencije napada, nije moguće u realnom vremenu preko klasičnog web portal prikazati sve zabeležene incidente. Na primer, iz jedne od kompanija su tvrdili da njihova mapa prikazuje samo 1% ukupnih zabeleženih napada i da kada bi prikazali sve, korisnički browseri bi se zakočili od preopterećenja.

Ipak, koliki god procenat da prikazuju prilično je interesantno pogledati kako izgledaju maliciozne aktivnosti u kiber prostoru. Izdvojićemo nekoliko najzanimljivijih primera – Kaperski, Fortinet i FireEye. Možda je najinteresantniju animiranu mapu ponudila korporacija Kasperski sa mogućnošću zumiranja i prelaska sa trodimenzionalnog prikaza naše planete oko koje simbolično kruže kiber napadi na dvodimenzionalan prikaz klasične mape .

Posetilac njihovog sajta može da izabere koji tip napada želi da vidi na mapi, pa može da izabere zabeležene bot net aktivnosti ili rezultate sistema za detekciju upada (Intrusion Detection System).





GLOBALNI CYBER RAT

Otkrivena mreža koja je s računa građana ukrala više od 100 milijuna dolara

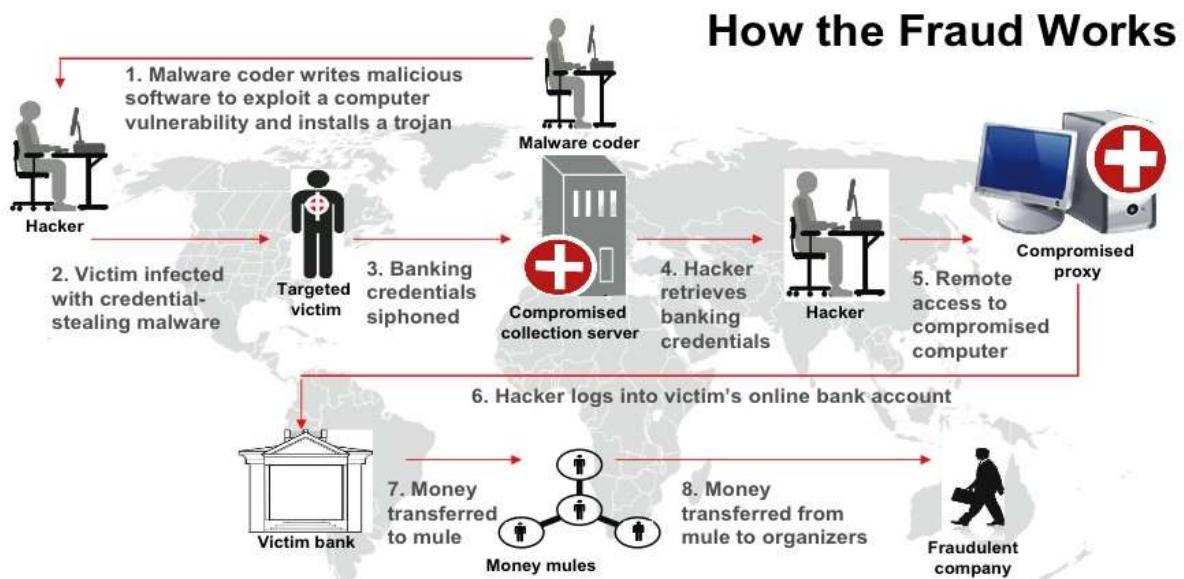
Slika 1. Haker Jevgenij Bogačev



Izvor: dennikn.sk

WASHINGTON - SAD je u ponedjeljak objavio kako je uz pomoć više zemalja uništilo veliku kriminalnu i ucjenjivačku mrežu na internetu koja je od žrtava otela više od sto milijuna dolara. Maligni računalni programi Gameover Zeus i Cryptolocker onesposobljeni su no njihov idejni tvorac ruski bjegunac **Jevgenij Bogačev** na slobodi je i mogao bi uspostaviti novu kriminalnu mrežu u vrlo kratkom roku, upozorilo je američko ministarstvo pravosuđa. Prema podacima kojima SAD raspolaže, posljednja poznata adresa Bogačova je crnomorsko mjesto Anapa u Rusiji. Program Gameover Zeus je ulazio u računala žrtava preko e-mailova, pronalazio je financijske podatke s kojima je praznio njihove bankovne račune. Program Cryptolocker je pak preuzimao i šifrirao podatke s računala žrtava te ih je tek nakon plaćanja otkupnine dešifrirao. U akciji gašenja velike kriminalne mreže sudjelovale su i pravosudne snage Kanade, Francuske, Njemačke, Luksemburga, Nizozemske, Ukrajine i Britanije, a koordinator je bio europski centar za cyber kriminal u Haagu. Programi su napali između 500 tisuća i milijun računala širom svijeta. Zeus je jedan od najuspješnijih računalnih programa za krađu dosad Kriminalna je skupina uz pomoć Cryptolockera samo u prva dva mjeseca od puštanja u optjecaj programa iznudila za dešifriranje podataka 27 milijuna dolara od žrtava Među žrtvama iznude bila je i policijska stanica u Massachusettsu čije su istražni dosjei blokirani šifriranjem. Američko ministarstvo pravosuđa objavilo je da su ukrajinske vlasti u svibnju zaplijenile glavne servere za Gameover Zeus u Kijevu i Donjecku.

Slika 2. Na koji način rade zlonamjerni software za krađu finansijskih podataka



Izvor: www.zdnet.com

HAKERI UKRALI HRVATSKIM TVRTKAMA 2 MIL. KN Sve počinje e-mailom s virusom...

Među žrtvama hakerskih napada u posljednje vrijeme u kojima se “prazne” poslovni računi tvrtki koje za plaćanja koriste internetsko bankarstvo, našao se i Zavod za javno zdravstvo Šibensko-kninske županije, no krađa je spriječena jer su na vrijeme uočili pokušaj i obavijestili banku, piše **Slobodna Dalmacija**.

Slika 3. Krađa novca od strane hakera



Izvor: www.news.com.au

Dogodilo se to pretprošlog ponedjeljka, pred kraj radnog vremena. Haker je s njihova računa nekoliko stotina tisuća kuna uplatio imenom i prezimenom na privatni račun u Njemačkoj, no banka je na vrijeme obavijestena te je transakcija opozvana prije nego je vlasnik računa podignuo novac. O svemu je obavijestena i policija. – Kako je istraga u

tijeku, ne smijem davati izjave o slučaju – kratko je za Hinu rekla **Suzi Vatavuk**, ravnateljica šibenskog Zavoda za javno zdravstvo. Istovjetnim napadima hakeri su od početka godine u Hrvatskoj uspjeli ukrasti ukupno dva milijuna kuna, a još 12 milijuna kuna transakcija banke su uspjele zaustaviti na vrijeme. Riječ je isključivo o poslovnim korisnicima internetskog bankarstva, koji za autorizaciju transakcija koriste USB stick ili čitač kartice. Građani koji koriste tokene za plaćanja nisu ugroženi. Činjenica da napadaju samo poslovne korisnike, međutim, i mana je ovih pokušaja. Kako je riječ o tvrtkama koje kontroliraju promet, haker u pravilu ima jednu priliku za krađu, što znači da će pokušati odjednom prebaciti što veći novčani iznos. Pritom odstupa od jednog od osnovnih pravila ovakvih napada – da se u pravilu kradu iznosi koji nisu bitno veći od uobičajenih isplata s računa, kako se ne bi probudila sumnja kod korisnika ili u baci. Zbog toga se za krađe u pravilu bira kraj radnog vremena, budući da banke mogu u roku od 24 sata blokirati sumnjivu transakciju. Jednom kada novac bude preuzet s računa na koji je prebačen, postupak povrata je prilično komplikiran, i ovisi o kaznenom postupku koji može trajati godinama dok se ne utvrdi tko je lopov. Ključna sigurnosna mjera koja se pri ovakvom načinu plaćanja mora poštovati jest da je uređaj priključen na računalo samo tijekom transakcije, odnosno da se izvadi odmah nakon što je transakcija provedena. Banke tvrde kako nije moguće provesti plaćanje ako je uređaj isključen, pa je i krađa podataka u tom slučaju beskorisna, no pojedini stradali klijenti žale se da su se pridržavali svih uputa, ali da su svejedno opljačkani. Hrvatska narodna banka stoga je od banaka zatražila detaljne izvještaje o krađama, kao i izvješća unutarnjih revizija i voditelja sigurnosti informacijskih sustava banaka, te planove aktivnosti koje su banke poduzele kako bi spriječile nastavak ovakvih krađa. HNB od banaka traži bolju zaštitu, iako ne preciziraju koju. Prije nekoliko godina, HNB je tražio da banke traže dodatnu autorizaciju neuobičajenih transakcija, a sada treba vidjeti što su banke od tada učinile na unaprjeđenju sustava. Banke se brane činjenicom da su napadnuta računala klijenata, a ne sustav banke. Stoga je i mogućnost povrata ukradenog novca mali. No, da banke u svemu malo kasne, pokazuje i činjenica da su nakon prijavljenih upada nadogradile Java platformu na kojoj radi internetsko bankarstvo, te uvele dodatne skočne prozore koji klijente tijekom rada upozoravaju da moraju iskopčati stick ili čitač kartica nakon završetka rada. Otimanje novca u ovoj shemi počinje instaliranjem virusa koji sa zaraženog računala “kupi” podatke poput lozinki, pinova, brojeva računa i sl. Virus se instalira otvaranjem pošte s privicima ili skidanjem sadržaja preko internetskog preglednika, a osim što krade podatke, omogućava i hakeru kontrolu nad kompjutorom. Prva preporuka kako se zaštititi od krađa jest – oprez, i to pri otvaranju mailova i linkova koji stižu od nepoznatih pošiljatelja ili s društvenih mreža, kao i pri skidanju podataka s interneta. Poslodavcima je najpametnije nastojati osigurati da radnici službena računala ne koriste u privatne svrhe, kao i blokirati instaliranje bilo kakvih programa, odnosno to omogućiti samo administratorima. Preporučuje se i da se plaćanja obavljaju jedino preko posebno odvojenih računala za tu svrhu. Jednako je važno i da su sve aplikacije i programi potrebni za rad uredno ažurirani. Naravno, prije svega toga računala treba zaštititi antivirusnim programima.

Slika 4. Kako zaštiti bankovne račune od hakerskih napada



Izvor: <http://www.thisismoney.co.uk/>

'OPREZ, HAKERI BI MOGLI ISKORISTITI HEARTBLEED'
Američka i njemačka vlada upozorile banke

BOSTON - Američka administracija upozorila je u petak banke, infrastrukturne operatore i druge organizacije da budu na oprezu zbog hakera koji bi mogli iskoristiti virus "Heartbleed" kako bi ukrali podatke s internetskih stranica.

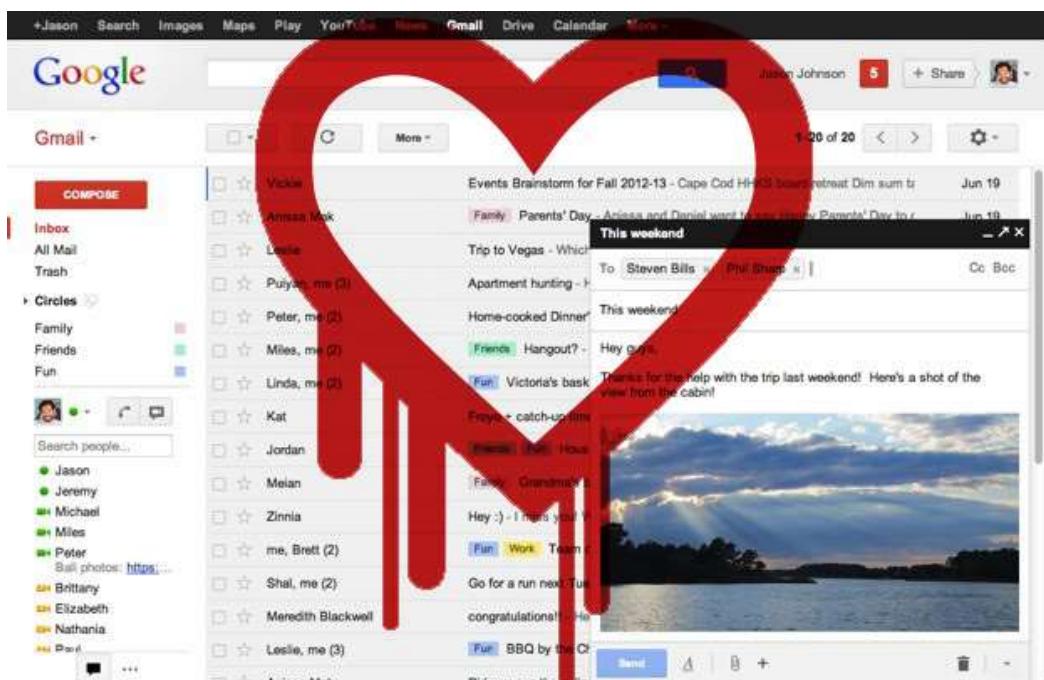
Ministarstvo domovinske sigurnosti, koje radi sa saveznim, državnim i lokalnim vladama na otkrivanju i otklanjanju mogućih prijetnji, zatražilo je od organizacija da prijave bilo kakve napade povezane s Heartbleedom, dok su savezni regulatori savjetovali finansijskim institucijama da identificiraju osjetljive sustave te da učine sve kako bi bili sigurni.

"Iako nije bilo prijavljenih napada ili zlonamjernih incidenata, ...još uvijek je moguće da hakeri to iskoriste", napisao je **Larry Zelvin**, direktor Nacionalnog integracijskog centra za kibernetičku sigurnost i komunikacije ministarstva domovinske sigurnosti, u blogu na internetskoj stranici Bijele kuće.

Njemačka vlada izdala je slično upozorenje.

"Napadač može iskoristiti ranjivost (sustava) i može pročitati sadržaj memorije servera OpenSSL", objavilo je Njemački savezni ured za sigurnost informacija.

Slika 5. Heartbleed virus napada web sajtove



Izvor: www.engadget.com

Ovaj propust postoji već dvije godine, no otkrili su ga tek sada. **Matthew Prince** iz Cloudflare-a, koji je otkrio propust koji postoji već dvije godine, kazao je kako se nadaju da će većinu stranica s greškom popraviti do kraja tjedna. Neke od njih problem su već riješile, što bi značilo da biste na tim stranicama trebali hitno promijeniti lozinku, što je i inače, s vremena na vrijeme, dobra navika.

Slika 6. Matthew Prince



Izvor: www.blog.1and1.com

Iz Facebooka su kazali kako su grešku popravili i prije nego li se vijest proširila te kako nisu zabilježili nikakvu sumnjivu aktivnost no da ipak savjetuju korisnicima da promijene svoje lozinke, a isto su kazali i iz društvene mreže Tumblr. Iz Twittera su pak kazali kako njihov servis nije pogoden tim propustom te da će nastaviti pratiti situaciju.

Iz Googlea su izvijestili kako su riješili problem te kako nema potrebe da korisnici sada nužno mijenjaju lozinke, no kako je zbog ranije ranjivosti možda ipak bolje da to učine. 'Heartbleed' je pogodio Googleovu tražilicu, Gmail, YouTube, no ne i Google Chrome.

Iz Yahooa su kazali kako su počeli raditi na otklanjanju problema čim su za njega saznali te kako još uvijek na tome rade. Bugom su bili pogođeni i popravljeni Yahoo Homepage, Yahoo Search, Yahoo Mail, Yahoo Finance, Yahoo Sports, Yahoo Food, Yahoo Tech i Flickr.

Propust je bio i na stranici za internet kupovinu Amazon iz kojeg su kazali kako bug nije imao utjecaj na njegove servise, no kako je ipak poželjno promijeniti lozinku. Elastic Load Balancing, Amazon EC2, Amazon Linux AMI, Red Hat Enterprise Linux, Ubuntu, AWS OpsWorks, AWS Elastic Beanstalk i Amazon CloudFront su 'pokrpali'.

Iz eBaya i PayPala su pak kazali kako njihovi sustavi nisu imali grešku te kako se korisnici ne trebaju brinuti.

MALOLJETNI HRVAT KRIJE SE IZA PEDOFILSKE FACEBOOK GRUPE Uspjeli su ga razotkriti bosanski hakeri

Dokaz da je Renato M. osnivač ove grupe predstavlja prepiska s M.N.

Slika 7. Renato M.



Izvor: <http://www.opustise.rs/>

Renato M. iz Hrvatske krije se iza Facebook grupe 'Najveće drolje osnovnih i srednjih škola' na kojoj su objavljivane eksplisitne fotografije uz imena i prezimena djevojaka i djevojčica iz zemalja regije - BiH, Hrvatske i Srbije, doznaće Telegraf.rs.

Uz pomoć grupe United Bosnian Hackers Telegraf je došao do podataka prema kojima je osnivač grupe maloljetni Renato M.. On je koristio lažni Facebook profil pod korisničkim imenom Josip M., te je zadnjih par dana namamljivao djevojčice da mu salju svoje provokativne fotografije.

Osim njega, među administratorima grupe našle su se još četiri osobe pod lažnim imenima: Ante I., Kris B.s, Berem Orase i Jovanka Broz.

Dokaz da je Renato M. osnivač ove grupe predstavlja prepiska s M.N. do koje je došla redakcija **Telegrafa**.

- Jučer napravio stranicu. Već 21.000 lajkova. Imam 200 poruka u Inboxu. To mi sve šalju slike - napisao je tijekom prepiske Renato.

Slika 8. Facebook stranice kreirana od strane Renato M.



Izvor: Screenshot

Renato E. (17) se po forumima ističe radikalno desnim stavovima, a predstavlja se kao haker. "Ugasio sam stranicu dok se strasti ne smire. Ali ne mogu mi ništa jer ne kršim zakon", napisao je jučer na uvredljivoj stranici "Najveće drolje osnovnih i srednjih škola" njen administrator - 17-godišnji **Renato E.** iz Novske.

Maloljetnik iz Hrvatske (podaci poznati redakciji) koji je pokrenuo ovu sramotnu Facebook stranicu, koju je do jučer popodne lajkalo više od 70 tisuća ljudi, pod lažnim imenom **Josip M.** na internetu se predstavlja kao član skupine Croatian Revolution Hackers. Kako Jutarnji doznaće, riječ je o tinejdžeru iz okolice Novske koji otprije tri godine s majkom živi u Švedskoj, a odlazak u tu zemlju spasio ga je ponavljanja 7. razreda osnovne škole.

Prema fotografijama koje smo dobili i prema nekim njegovim komentarima na Facebooku, može se zaključiti da je sklon radikalnim desnim skupinama. Na jednoj od fotografija drži dignutu desnicu u zraku, a u nekim svojim komentarima po društvenim mrežama pozdravlja sa "Za dom!".

ADMINISTRATOR PEDOFILSKE GRUPE 'Preimenovat ćemo stranicu da ne vrijedamo drolje'

"Ajde malo odmora na par dana, više mi je pun k... ovih d*olja LoL... Par dana smo off, pozzz", obavijestio je jučer sve korisnike grupe njen administrator. Iako je stranica trenutno ugašena i na njoj administrator više ne objavljuje golišave fotografije maloljetnica iz Hrvatske, Srbije i Bosne i Hercegovine, jučer se pojavilo nekoliko

sličnih Facebook stranica s jednakim nazivom i jednako vulgarnim sadržajem. Iako pokretač stranice tvrdi na nema ničeg spornog u njegovu postupanju jer su se djevojke same fotografirale i postavile to na svoje Facebook profile, Kazneni zakon predviđa kaznena djela protiv časti i ugleda. Obično se progona počinitelja poduzima temeljem privatne tužbe, ali kako je riječ o maloljetnicama, policija i DORH mogu postupati i po službenoj dužnosti. Slična je situacija bila i sa stranicama koje su na jednak način etiketirale djevojke iz Županje i Vinkovaca. Tada su u policiji rekli kako su fotografije djevojaka objavljene na spornoj stranici preuzete s njihovih Facebook profila. Dakle, nisu otuđene neovlaštenim ulaženjem u računala, a nije bila riječ ni o krađi identiteta jer su se uz fotografije pojavljivala stvarna imena osoba.

Slika 9. Renato M. obavljuje slike djevojaka bez njihovog pristanka



Izvor: www.rokaj.ba

BIBLIJOM HAKIRALI EUROPSKE FONDOVE

Grčićev ministarstvo na mukama, pozvani digitalni forenzičari

Slika 10. Hakiranje Europskih fondova



Izvor: <http://www.politikaplus.com/>

Informacije o natječajima s hakirane internetske stranice o strukturnim fondovima EU mogu se naći na novoj adresi.

ZAGREB - Informacije o natječajima s hakirane internetske stranice o strukturnim fondovima EU mogu se naći na adresi www.mrrfeu.hr, izvjestilo je Ministarstvo regionalnoga razvoja i fondova Europske unije. Sve informacije o natječajima „Povećanje gospodarske aktivnosti i konkurentnosti malih i srednjih poduzeća“ i „Shema dodjele bespovratnih sredstava za poslovnu infrastrukturu“ dostupne su na internetskim stranicama www.mrrfeu.hr Ministarstva regionalnoga razvoja i fondova Europske unije, kaže se u priopćenju.

Umjesto informacija o fondovima EU-a, možete pregledati - Bibliju!

Nakon što je u subotu ujutro napadnuta stranica www.strukturnifondovi.hr na kojoj se objavljuju sve informacije o EU fondovima, svim korisnicima omogućen je rad preko stranice Ministarstva na kojoj su poveznice i potrebni obrasci za otvorene natječaje. Obavijest korisnicima objavljena je na naslovni stranice Ministarstva. Stranica www.strukturnifondovi.hr je u rekonstrukciji.

Iz Ministarstva ponovno ističu da je integritet mreže zaštićen te da nijedan korisnik portala ne treba strahovati za sigurnost podataka. Incident se, navode, dogodio u izdvojenoj zoni iz koje nema pristupa mreži Ministarstva regionalnoga razvoja i fondova Europske unije.

Napad na portal prijavljen je nadležnim službama, u tijeku je digitalna forenzika, kaže se u današnjem priopćenju koje je potpisala glasnogovornica Ministarstva regionalnoga razvoja i fondova Europske unije **Ljubica Vuko**

Stranica središnjeg državnog portala za informacije o europskim fondovima hakirana je jučer prijepodne i preusmjerava na stranicu za pretraživanje Biblije.

FBI OTVARA VRATA NAPUŠENIM HAKERIMA? '

Trebamo najbolje, a takvi najčešće puše travu'

Slika 11. Najbolji hakeri često puše travu



Izvor: www.420intel.com

Američka savezna policija FBI u posljednje se vrijeme suočava s velikom dilemom. Prema internom pravilniku ne bi smjela primiti u radni odnos nikoga tko je evidentiran da je unatrag tri godine pušio travu, ali s druge strane upravo se među konzumentima marihuane često kriju najbolji potencijalni agenti koji bi ponajprije radili na borbi protiv cyber kriminala.

Direktor FBI-ja **James Comey** priznao je na jednoj godišnjoj konferenciji da ne zna što učiniti. 'Trebao bih zaposliti najbolje radnike da se bore protiv cyber kriminalaca, a neki od tih klinaca htjeli bi prije razgovora za posao zapaliti joint', otkrio je svoje muke Comey, čije riječi prenosi Wall Street Journal.

Jedan sudionik konferencije direktora je pitao što da kaže svom često napušenom prijatelju koji bi vrlo rado iz hakerskog svijeta prešao u redove saveznih agenata. Comey mu je odgovorio: 'Pa neka se prijavi na natječaj'. Iako to nije izrijekom kazao, ta bi rečenica mogla biti nagovještaj promjene internih pravila o zapošljavanju. Slična, ali ponešto blaža pravila ima i britanska Nacionalna jedinica za borbu protiv cyber kriminala (NCCU).

Računalni ekspert **Richard Clayton** s uglednog Sveučilišta u Cambridgeu, za BBC kaže da bi bilo razborito revidirati ovakve regule. 'Najčešće želite zaposliti mlade hakere, a oni često imaju neke loše navike kao što je pušenje marihuane. No, s vremenom te navike lagano umiru', tvrdi Clayton. 'Ja mislim da FBI i NCCU zapravo imaju veći problem u pronalasku kvalitetnih radnika zbog plaća koje su spremni ponuditi, koje su u usporedbi s iznosima koji se nude u privatnom sektoru izrazito niske', rekao je.

ČUVAJTE KOMPJUTERE

Oprez, internetom kruži zastrašujuće sofisticiran računalni virus

Kada Careto zarazi računalo, počinje prikupljati lozinke, prati promet na mreži i korištenje WiFi-ja, aktiviranje tipki na tipkovnici, razgovore na Skype-u i rad sa podacima, nadzirati što se pojavljuje na ekranu, a može se raširiti na sva računala koja su povezana sa zaraženim

Slika 12. Careto virus

Izvor: pinovytutorial.com

Kako internet sve više napreduje i postaje složeniji, tako napreduju i virusi koji njime haraju, a korisnici osobnih računala upravo su na udaru naj sofisticiranijeg a po svoj prilici i najopasnijeg do sada. Washington Post upotorio je svoje čitatelje na izvještaj Kaspersky labsa, prema kojem internetom kruži vrlo složen računalni virus čiji je autor još uvijek nepoznat. Virus pod nazivom "Careto" kompromitirat će zaraženo računalo kako bi skupio veliki broj informacija, navodi se u izveštaju Kaspersky lab-a, piše Slobodna Dalmacija.

Virus se širi putem mailova koji na prvi pogled deluju autentično (događalo se da je kao pošiljatelj naveden britanski The Guardian ili američki Washington Post), a sadrže link na sumnjiive sajtove koji skeniraju korisnikovo računalo i potom ga pokušavaju zaraziti.

Kada Careto zarazi računalo, počinje prikupljati lozinke, prati promet na mreži i korištenje WiFi-ja, aktiviranje tipki na tipkovnici, razgovore na Skype-u i rad sa podacima, nadzirati što se pojavljuje na ekranu, a može se raširiti na sva računala koja su povezana sa zaraženim. Napada sve operacijske sustave, a Kaspersky labs upozorava da bi se uskoro mogla pojaviti i verzija za Android i iOS. Za razliku od starijih virusa koji su se širili nekontrolirano, Careto ima jasne ciljeve. Premda se na prvi pogled činilo da je napao nasumična računala diljem svijeta, u Kaspersky labu su obradom podataka došli do zaključka da virus najviše napada državne institucije, veleposlanstva, istraživačke organizacije, naftne i razne druge moćne kompanije.

S obzirom na njegovu složenost i specifične "mete", prepostavlja se da je ovako složen software mogla stvoriti samo neka državna obaveštajna agencija, no još nitko sa sigurnošću ne zna tko ga je kreirao i s kojim točno ciljem.

Računalni virusi 'slave' 25 godina: Pročitajte povijest 25 najopasnijih i najpoznatijih

Prvi e-mail virus u povijesti bio je Happy99. Ne zna se otkud je stigao, ali pojavio bi se u vašem Inboxu s nazivom "Sretna Nova 1999.". Čim bi ga otvorili on bi automatski poslao istu poruku svima koje imate u kontaktima, ali nije činio nikakvu štetu, baš kao ni ostali prvotni virusi

Slika 13. Happy99 virus



Izvor: www.slideshare.net

Kompjuterski virusi pojavili su se ekspanzijom interneta i 'oduševljavaju' nas već punih 25 godina! Iako su pozornost dobili prije točno dva desetljeća, pioniri destrukcije naših računala krenuli su u pohod davne 1986. Predstavljamo vam njih 25 za jubilarnih 25 godina.

Sve je krenulo virusom koji zapravo i nije trebao biti virus. Braća Basit i Amjad Farooq Alvi iz Pakistana načinili su zaštitu kojom bi se sprečavalo piratstvo, zbog čega su i ostavili svoj kontakt na poruci koja je upozorila korisnika da ima ilegalne stvari na disku. No, Brain (naziv virusa) se nije nadograđivao i s vremenom se počeo javljati i kad ne bi bilo ilegalnih stvari na disku, nije više mogao razaznati legalno od ilegalnog. Braća su ubrzo povukla svoj program (virus) s tržišta, a danas imaju u Pakistanu telekomunikacijsku tvrtku Brain Telecommunication Limited i vrlo su utjecajni i bogati.

Poslije te 1986. su se sve češće počeli pojavljivati virusi, ali prvi kojeg su zabilježili mediji bio je virus Michelangelo. Ime je dobio jer je mirovao sve do 6. ožujka, dan kad je rođen veliki renesansni umjetnik. Kad bi se Michelangelo 'probudio', 'zarazio' bi disk. Zna se da je stigao s Novog Zelanda, ali se sumnja kako je njegov autor namjerno koristio dan Michelangelova rođenja.

Slika 14. Michelangelo virus

The Most Famous (or Infamous) Viruses and Worms of All Time

MICHELANGELO

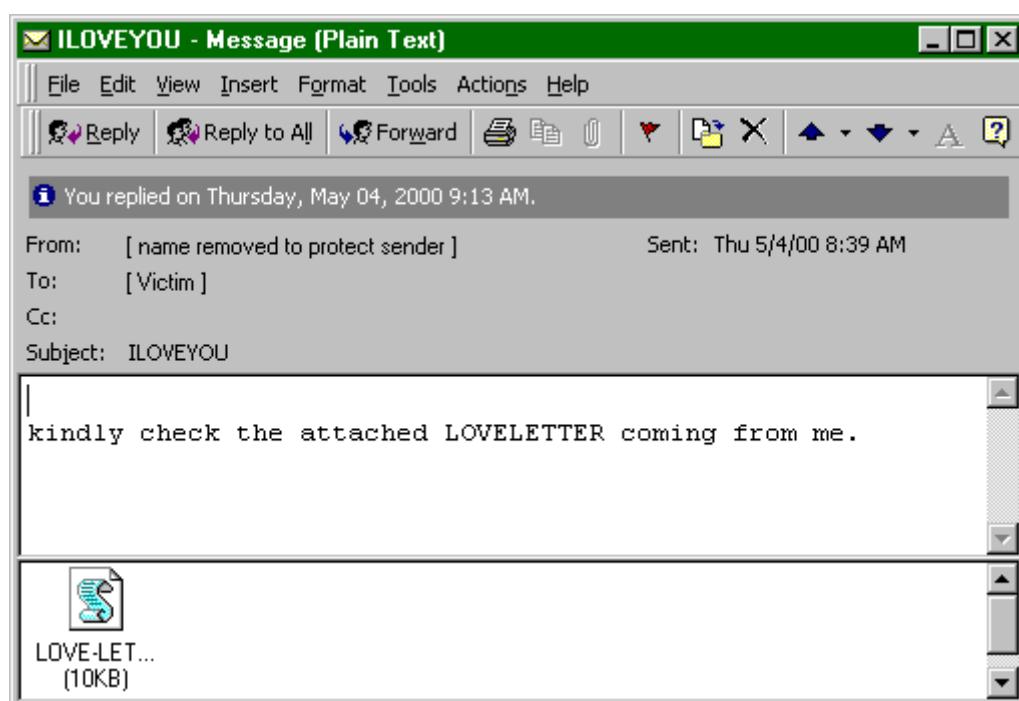
In 1991, the world waited and watched for the Michelangelo virus, a "time bomb" that bombed. Set to deploy on March 6 (Michelangelo's birthday), the virus was designed to overwrite critical drive sectors, but it did little damage in reality.

eWEEK

Izvor: www.ewEEK.com

Ali štetu je zato činilo "ljubavno pismo", virus stigao s Filipina 2000. godine napravio je pravu zbrku u računalnom svijetu. Ovaj virus, odnosno crv kako se nazivaju virusi koji se šire bez pomoći čovjeka, zarazio je milijune računala tako što bi se pojavio u vašem Inboxu s naslovom "Love letter", a kad bi otvorili priloženu datoteku on bi vam zarazio sve na računalu potrebno za normalan rad.

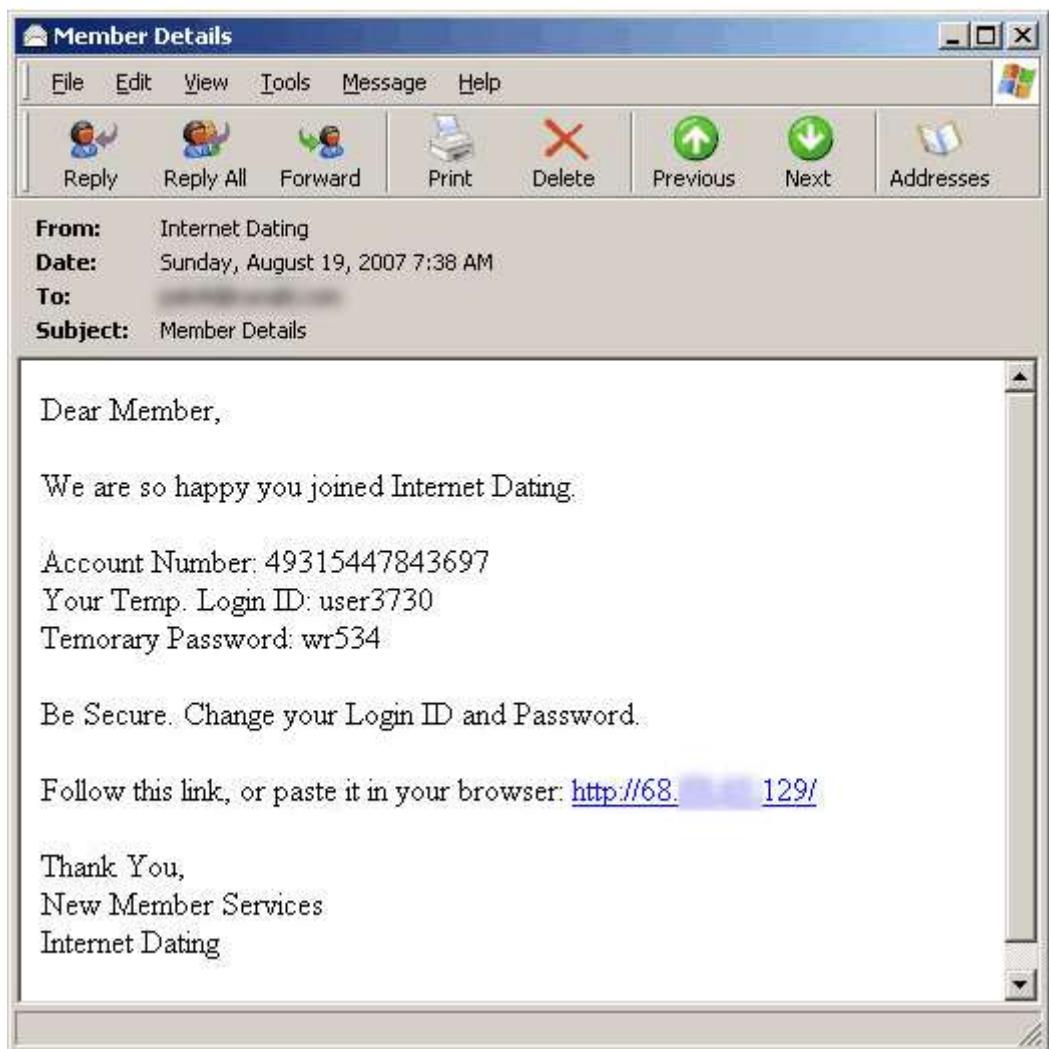
Slika 15. I Love You virus



Taj crv je zapravo bio (r)evolucija i nakon njega su mnogi dobili inspiraciju. Ali svi su oni zapravo služili da vam naštete, to je bila dovoljna satisfakcija svakog tko bi ih pustio u opticaj. Sve do 2003. godine i Fizzera, prvog virusa napravljenog kako bi svom tvorcu donio zaradu. Poanta je bila da vam se 'uvuče' u Inbox i zatim šalje reklame (spam) svima u vašim kontaktima, a zatim svima u kontaktima onog gdje je stigao itd., itd.

Najopasniji virus svih vremena također se širio putem elektroničke pošte. Storm Worm je stvoren 2007. godine na nepoznatoj lokaciji, a zavarao bi vas nazivom "230 mrtvih nakon oluje u Evropi". Kad bi otvorili tu poruku na računalo bi vam stigao 'trojanski konj', vrsta virusa koja se isprva doima kao legalna datoteka, ali čim je instalirate na računalo počne kontrolirati određene programe na računalu i slati vaše informacije onome tko vam je 'trojanca' poslao. Ukratko, Storm Worm je preuzimao kontrolu nad vašim računalom.

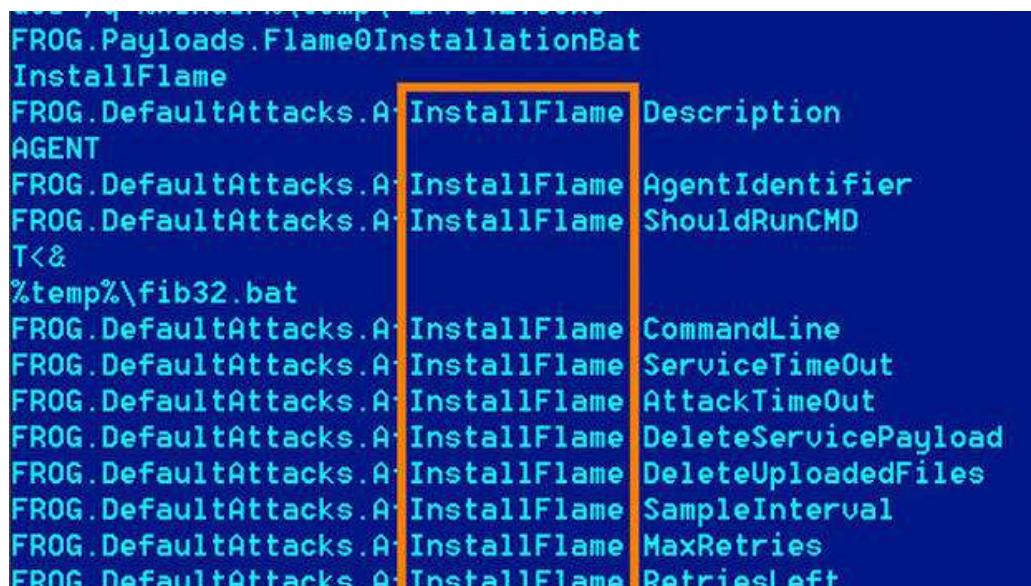
Slika 16. Storm Worm



Izvor: www.grok.lsu.edu

Najmoćniji virus, za koji se vjeruje da ga je načinila Vlada SAD-a ili Izraela, jest izumljen 2010. godine, a naziva se Stuxnet. Njegova je zadaća nadgledati industrijske programe ili datoteke, posebno one koji se koriste za obogaćivanje urana. Smatra se prvim virusom koji se koristi za špijunažu, odnosno kontrolu tržišta, a u što će evoulirati nitko ne zna, iako se mnogi teoretičari zavjera bave raznim crnim predviđanjima.

Slika 17. Stuxnet



```
FROG.Payloads.Flame0InstallationBat
InstallFlame
FROG.DefaultAttacks.A:InstallFlame Description
AGENT
FROG.DefaultAttacks.A:InstallFlame AgentIdentifier
FROG.DefaultAttacks.A:InstallFlame ShouldRunCMD
T<&
%temp%\fib32.bat
FROG.DefaultAttacks.A:InstallFlame CommandLine
FROG.DefaultAttacks.A:InstallFlame ServiceTimeOut
FROG.DefaultAttacks.A:InstallFlame AttackTimeOut
FROG.DefaultAttacks.A:InstallFlame DeleteServicePayload
FROG.DefaultAttacks.A:InstallFlame DeleteUploadedFiles
FROG.DefaultAttacks.A:InstallFlame SampleInterval
FROG.DefaultAttacks.A:InstallFlame MaxRetries
FROG.DefaultAttacks.A:InstallFlame RetriesLeft
```

Izvor: www.cbsnews.com

SAD: SAJBER KRIMINAL KOŠTA KOMPANIJE PO 7,7 MILIONA DOLARA

Sajber kriminal u prosjeku svaku veliku američku kompaniju ove godine košta 15,4 miliona dolara, 19 odsto više nego lani. Troškovi kompanija u javnom i privatnom sektoru zbog sajber kriminala su u punoj ekspanziji širom svijeta, i na godišnjem nivou su povećani za 1,9 odsto, navodi se u šestom godišnjem izvještaju američkog instituta Ponemon. Prosječan godišnji trošak kompanija zbog sajber kriminala za ovu godinu iznosi 7,7 miliona dolara.

Slika 18. Povećani troškovi



Izvor: www.slideshare.net

KAKO DA SIGURNIJE KORISTITE TELEFONE KOJI RADE NA ANDROIDU

Korisnici bi uvijek trebalo da budu na oprezu prilikom korištenja svojih uređaja kako bi izbjegli potencijalne probleme. Googleov Android daleko je najpopularniji mobilni operativni sistem koji zauzima više od 80 odsto tržišta te mobilne uređaje koje pokreće Android koriste stotine miliona ljudi širom svijeta. Većina mobilnih kompanija (osim Applea, Nokije i BlackBerryja) kao primarni operativni sistem koristi upravo Android te je sigurno da će njegova dominacija potrajati još dugo vremena, iako bi konkurenčija trebalo da bude sve jača (polako raste udio Windows Phonea, dio tržišta zauzeće i Firefox OS, ali oni sigurno neće predstavljati opasnost za Google).

Ali, takva popularnost i veliki broj korisnika donosi i određene probleme i opasnosti, a to su ponajviše maliciozni programi i virusi koji bi u budućnosti mogli predstavljati ozbiljne probleme za vlasnike pametnih telefona i tableta koji rade na Androidu te su Cisco i Kaspersky Lab u svojim sigurnosnim izvještajima upozorili kako je 99, odnosno 98 odsto malicioznih programa usmjereno upravo protiv uređaja koji rade na Androidu.

Ipak, za razliku od velikih problema s virusima i malwareom kakve su znali imati korisnici personalnih računara, do sada nije zabilježen virus ili malware koji se proširio na velikom broju telefona ili tableta, a na The Guardianu kažu da bez obzira na to korisnici bi uvijek trebalo da budu na oprezu prilikom korištenja svojih uređaja kako bi izbjegli potencijalne probleme.

Ovo je pet savjeta sa The Guardiana o sigurnijem korištenju mobilnih uređaja koji rade na Androidu:

Oprez prilikom instaliranja aplikacija – aplikacije preuzimajte samo sa Googleove trgovine aplikacija Google Play te izbjegavajte skidanje aplikacija s nepoznatih stranica. Pogotovo pripazite na 'nove verzije' popularnih igara poput Candy Crusha ili Angry Birdsa jer je često riječ o lažnim aplikacijama s prikrivenim malwareom.

Takođe, kada skidate aplikacije sa Google Play obratite pažnju na ocjene i recenzije tih aplikacija te obavezno provjerite šta sve aplikacija zahtijeva (pristup vašim kontaktima, fotografijama i slično).

Pripazite na phishing – osim na lažne aplikacije, pripazite i na phishing i na prevarantske internet stranice putem kojih sajber kriminalci mogu doći do vaših ličnih podataka. Na ovakve stranice možete doći otvaranjem linkova koje šalju kriminalci u e-mailovima ili SMS-ovima, a za koje se čini da ih je poslala npr. vaša banka i u kojima se od vas traži upisivanje ličnih podataka, brojeva bankovnih kartica... Takve su stranice napravljene skoro identično kao i stranice banke tako da korisnici često uopšte nisu svjesni da svoje podatke upisuju na lažne stranice, odnosno da ih daju kriminalcima.

Zaključajte ecran šifrom – s obzirom na to koliko ljudi često gledaju u ekrane svojih telefona, mnogi su lijeni da koriste šifru za otključavanje ekrana jer bi je morali ukucavati 50 i više puta dnevno. Ali, zbog toga bi mogli da imaju velikih problema u slučaju da izgube telefon ili ako ga neko ukrade jer, kako se na telefonima nalaze aplikacije za pristup mailu, društvenim mrežama i brojnim privatnim/važnim podacima, osoba koja se dokopa tuđeg telefona mogla bi da ima pristup svim tim podacima vlasnika telefona. Takođe, korisno je imati uključenu opciju za naknadno lociranje telefona i zaključavanje, odnosno brisanje podataka na daljinu.

Antivirusni softver – iako na pametnim telefonima nije obavezan kao i na računarama, korisnici smartphonea koji žele dodatnu zaštitu na Google Play mogu pronaći aplikacije nekih od najpoznatijih proizvođača antivirusnog softvera poput Avasta, Bitdefendera, Nortona, McAfeeja i drugih kompanija.

Roditeljska kontrola – pametne telefone trebate zaštititi i od djece koja, igrajući se s njima, mogu slučajno izbrisati sadržaj s telefona, skinuti aplikacije, telefonirati i slično, a najbolje rješenje za to jeste korištenjem softvera za roditeljsku kontrolu uređaja. S takvima aplikacijama poput Kids Placea moguće je odrediti ograničenja pri korištenju uređaja i aplikacija i na taj način spriječiti potencijalne neprijatnosti kakve je prošle godine doživio jedan Amerikanac koji se šokirao kada je dobio mail od eBaya u kojem su mu čestitali na kupovini automobila. Naime, automobil nije kupio on, već njegova 14-mjesečna kćer koja se igrala sa njegovim telefonom i – kupila automobil.

Sajber kriminal u prosjeku svaku veliku američku kompaniju ove godine košta 15,4 miliona dolara, 19 odsto više nego lani, kada su oni iznosili 12,7 miliona dolara, prenosi AFP.

Prosječan trošak američkih kompanija u 2015. zbog sajber prestupništva kreće se od 1,9 miliona do 65 miliona dolara na godišnjem nivou.

KINA: UHAPŠENO 15.000 OSOBA ZBOG SAJBER KRIMINALA

Policija u Kini uhapsila je 15.000 osoba osumnjičenih za sajber kriminal tokom pojačane kontrole interneta, saopštili su danas zvaničnici u toj zemlji. Ministarstvo za javnu bezbjednost u Kini saopštilo je da je policija istražila više od 7.400 slučajeva mogućih sajber kriminala, uključujući hakovanje, prevare na globalnj mreži i ilegalnu prodaju ličnih informacija, kao i da je uhapšeno 15.000 osoba. Šestomjesečna specijalna operacija kontrole globalne mreže počela je u julu, ali obuhvata i slučajeve koji su zabilježeni ranije, odnosno do decembra pošle godine.

Peking smatra da je internet virtuelna teritorija kojom moraju da vladaju zakoni i propisi.

Slika 19. Uhapšeni hakeri



Izvor: www.juvenileredemption.org

NAJČEŠĆA ZLOUPOTREBA IDENTITETA NA DRUŠTVENIM MREŽAMA

"Kao što vidite, oko svih nas su različiti uređaji. To znači da ćemo internet sve više da koristimo u svakodnevnom životu. To podrazumijeva veća prijetnje, ali i potrebu za većim brojem obučenih ljudi. Stručnjaci, dalje, imaju ulogu da edukuju širu javnost o svim bezbjednosnim i ostalim prijetnjama na internetu"

Slika 20. Zloupotreba identita kroz društvene mreže



Izvor: www.business-support.it

Najveći broj sajber incidenata u Crnoj Gori odnosi na zloupotrebu identiteta na društvenim mrežama, hakovanje profila, ali ima na bankarske i finansijske prevare, saopšteno je iz Ministarstva za informaciono društvo. Pojedini stručnjaci kazali su za Atlas televiziju, da svijetu, a, ne samo Crnoj Gori fali IT stručnjaka "Ni mi nemamo dovoljno stručnjaka jer se većina omladine usavrša u nekim drugim poljima", kazao je Atlas televiziji Marko Holbl sa Univerziteta u Mariboru. Prema njegovim riječima, IT industrija ubrzano raste. "Kao što vidite, oko svih nas su različiti uređaji. To znači da ćemo internet sve više da koristimo u svakodnevnom životu. To podrazumijeva veća prijetnje, ali i potrebu za većim brojem obučenih ljudi. Stručnjaci, dalje, imaju ulogu da edukuju širu javnost o svim bezbjednosnim i ostalim prijetnjama na internetu", kazao je Holbl.

Stefano Guarino, sa Univerziteta u Rimu, kazao je da oni pokušavaju da prenesu iskustvo i uticu na jačanje svijesti o sajber prijetnjama. "Između ostalog, vaš obrazovni

sistem treba da se i u tom segmentu uskladi sa evropskim standardima”, kazao je Guarino.

On je dodao, da je IT oblast u kojoj izazovima nikad nema kraja.“Svaki put kad osmislimo rješenja, napadi se pojačaju. Najvažnije je da budete ažurirani. Morate da budete u toku sa svim strategijama napada, kako bi ste bili u stanju na njih da odgovorite”, rekao je Guarino.

Projekat Unaprijeđenje Obrazovanja iz oblasti sajber bezbjednosti u Crnoj Gori na kome je jedan od partnera Univerzitet Mediteran je jedan od načina kako budući stručnjaci treba da uče i rade na ovom problemu.

Projekat, koji je podržalo resorno Ministarstvo, ima za cilj da unaprijedi znanje o sajber bezbjednosti unutar organizacija tako da se postojeći resursi optimalno upotrebljavaju radi suzbijanja najvećih i najozbiljnijih prijetnji.

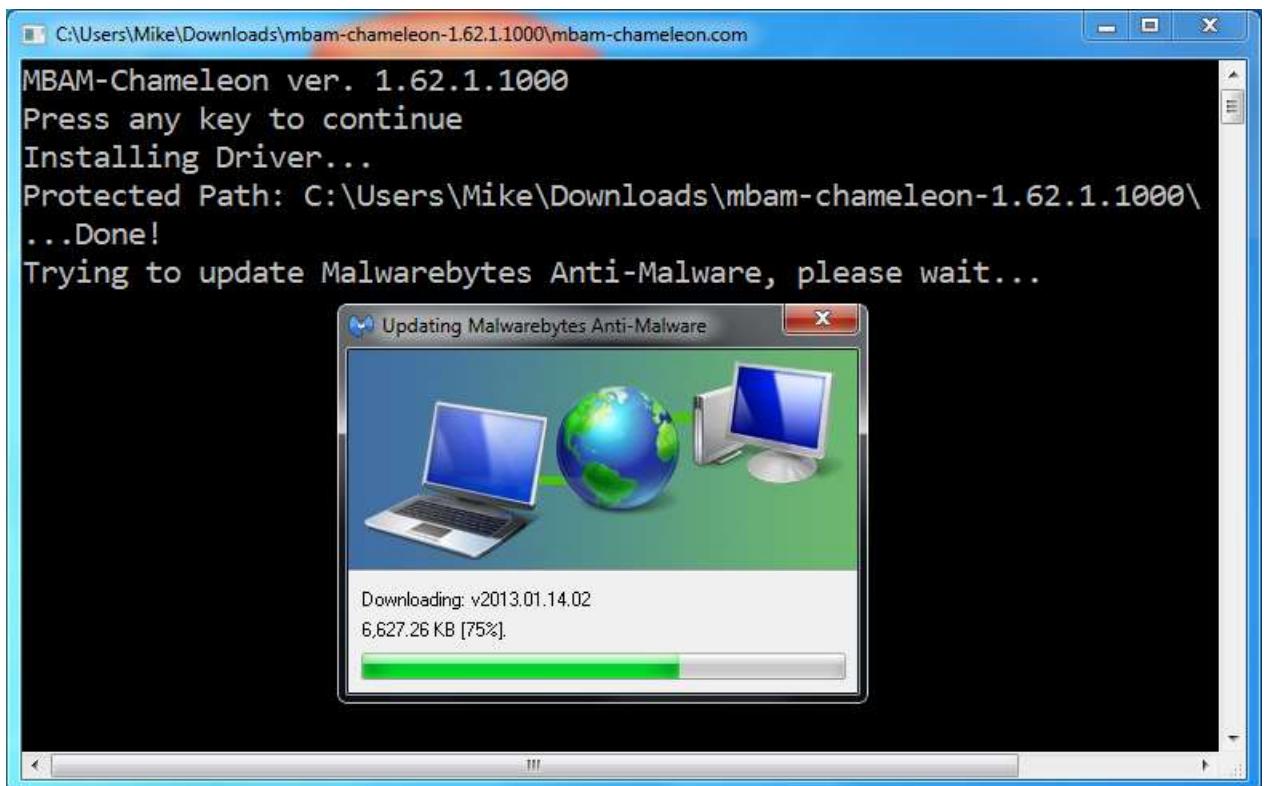
“Svako ponašanje se uči od osnovne škole. Tu treba posvetiti pažnju i edukovati učenike o sajber prostoru. To treba nastaviti u srednjim školama i na univerzitetu”, kazala je Ana Rakočević iz Ministarstva za informaciono društvo

Projekt je finansirala Evropska unija u okviru TEMPUS projekata i traje do kraja 2016 godine.

RAZVIJEN VIRUS KOJI SE ŠIRI BEŽIČNIM MREŽAMA BRZO POPUT PREHLADE!

Malware nazvan Kameleon je samo koncept koga su razvili naučnici kako bi dokazali da postoji mogućnost da se jednog dana ovakvi virusi zaista pojave i napadnu WiFi mreže.

Slika 21. Malware Kameleon



Izvor: www.downloadcrew.com

Naučnici sa univerziteta u Liverpulu napravili su računarski virus koji se širi WiFi mrežama brzo poput prehlade. Na Mashableu kažu da je ovo vjerovatno prvi ovakav oblik virusa koji se, "širi putem vazduha, baš poput prehlade", odnosno čije širenje zavisi od udaljenosti između WiFi mreža. Malware nazvan Kameleon je samo koncept koga su razvili naučnici kako bi dokazali da postoji mogućnost da se jednog dana ovakvi virusi zaista pojave i napadnu WiFi mreže. Takođe, zahvaljujući Kameleonu, istraživači za bezbjednost moći će na vrijeme da se pripreme na potencijalno širenje ovakvih virusa i do tada već pripreme rješenje za njih.

Virus se širi koristeći pristupne tačke putem kojih se korisnici povezuju s internetom (najčešće na javnim mjestima) te se brže širi na područjima na kojima ima više ljudi jer na takvim područjima (kafići i restorani) ima veći broj pristupnih tačaka. Princip rada ovog virusa je sljedeći – kada Kameleon napadne jednu pristupnu tačku, on ne utiče na njen rad, već skuplja podatke svih korisnika koji se povezani s tom pristupnom tačkom te podatke o drugim pristupnim tačkama u blizini s kojima se može povezati i preuzeti kontrolu nad njima. Ono što je posebno zanimljivo jeste da je ovaj virus toliko agresivan da konstantno traži ranjive bežične mreže, a ako nađe na zaštićene pristupne tačke, on ih zaobilazi i jednostavno krene dalje u potragu za ranjivim mrežama.

Osim zbog ovakvog načina širenja, ovaj je virus jako opasan i zato što ne napada individualne računare, već mreže tako da ga je skoro nemoguće otkriti koristeći većinu današnjeg sigurnosnog softvera.

NE ODGOVARAJTE NA SMS PORUKE U KOJIMA VAS OBAVJEŠTAVAJU DA STE DOBILI NA LUTRIJI

Čitateljka Vijesti je juče dobila SMS sa broja +447792029754, u kojoj je pošiljalac na engleskom jeziku obavještava da je osvojila neku nagradu.

Slika 22. Lažne SMS poruke



Izvor: www.thingstoknows.com

Ako dobijete SMS sa nepoznatog broja sa kojeg vas obavještavaju da ste navodno osvojili nagradu na lutriji ili nagardnoj igri u kojoj čak niste ni učestvovali - ne odgovarajte na poruku, više puta su sličan savjet upućivali korisnicima iz telekomunikacionih kompanija koje posluju u Crnoj Gori. Čitateljka Vijesti je juče dobila SMS sa broja +447792029754, u kojoj je pošiljalac na engleskom jeziku obavještava da je osvojila neku nagradu. U poruci je, kako je navela u pismu "Vijestima", navedeno kako bi trebalo da pošalje email na adresu naznačenu u poruci ili da pozove broj telefona sa kojeg je dobila SMS. "Prepostavila sam da je riječ o prevari, pa sam ukucala ovaj broj na Google pretraživač i vidjela o čemu se radi", navela je ona.

Prema Google rezultatima, u pitanju su lažne poruke poslate sa brojeva iz Luksemburga.

Originalan tekst poruke glasi "Congratulations Your Mobile number Has Won You The Sum Of £950,000.00 in Our FreeLotto Promo Ref- FLP14, To Claim email WIN2014@GMX.COM With Your Full Names & No".

U poruci se primalac obavještava kako je navodno osvojio nagradu od 950.000 funti na lutriji i moli se da pošalje poruku na email WIN2014@GMX.COM te da u poruci navede svoje puno ime i prezime.

Slika 23. Alat za hakiranje putem SMS poruka



Izvor: www.hackguideteam4u.blogspot.com

30 GODINA ZATVORA: KAKO JE "PAO" JEDAN OD NAJOPASNIIJIH HAKERI

Ukrajinac je sarađivao sa brojnim hakerima koji su krali te podatke i prodavao ih je navedenom tajnom agentu

Maksim Jastremski je tokom prošle decenije bio jedan od najopasnijih hakera koji se specijalizovao za krađe brojeva kreditnih kartica koje je prodavao kriminalcima putem interneta. Tokom svog djelovanja, on je ukrao podatke o više od 40 miliona kartica te bankama nanio milionsku štetu sve dok nije uhapšen 2008. godine u Turskoj i osuđen na čak 30 godina zatvora.

Slika 24. Maksim Jastremski



Izvor: www.vecernji.hr

Jedan od agenata američke tajne službe (koji je, naravno, ostao anoniman) novinarima CNN-a je opisao detalje vezane za njegovo hapšenje, a zanimljivo je da je on sa Maksimom provodio puno vremena družeći se po gradovima Azije i Bliskog istoka, zajedno su odlazili na plaže, putovali, išli u noćne izlaska po klubovima i slično.

Prvi korak ka njegovom hapšenju napravljen je još 2004. godine kada su agenti tajne službe uhapsili kriminalce koji su u Los Andelesu kupovali stvari po prodavnicama koristeći ukradene kartice. Agenti nisu htjeli da se zadržavaju samo na malim kriminalcima, već su htjeli da dođu do izvora ukradenih kartica pa su sa vođom ove bande postigli dogovor prema kojem će on jednog agenta upoznati sa osobom koja im dobavlja brojeve ukradenih kartica i predstaviti ga kao novog partnera.

Jedan od agenata američke tajne službe novinarima CNN-a je opisao detalje vezane za njegovo hapšenje, a zanimljivo je da je on sa Maksimom provodio puno vremena družeći se po gradovima Azije i Bliskog istoka, zajedno su odlazili na plaže, putovali, išli u noćne izlaska po klubovima i slično

"Tako sam počeo da komuniciram putem instant messengera sa osobama sa jugoistoka Azije", rekao je agent novinarima CNN-a te je dodao kako je, kao dio prevare, morao da nabavi sve potrebne stvari za izradu lažnih kartica – mašine i specijalnu plastiku za izradu samih kartica te, ono najvažnije, brojeve ukradenih kartica. Te brojeve je trebalo da mu da upravo Jastremski koji je u to vrijeme imao najnoviju i najveću bazu ukradenih kreditnih kartica.

Ukrajinac je sarađivao sa brojnim hakerima koji su krali te podatke i prodavao ih je navedenom tajnom agentu. Nakon nekog vremena konstantnog dopisivanja, došlo je vrijeme da se agent i ovaj Ukrajinac, koji je u hakerskim krugovima bio poznat pod nadimkom "Maksic" upoznaju te su se više puta nalazili u gradovima na jugoistoku Azije i na Bliskom istoku. Druženje sa jednim od najvećih hakera agent je opisao kao posao i neku vrstu prijateljstva jer su oni dane provodili kupajući se na plaži, surfujući, izlazeći u noćne klubove, putujući i slično.

Ali, kada je agent od Jastremskija skupio dovoljno informacija, "priateljstvo" je završilo te je njihove planove o izlasku u turske noćne klubove prekinula policija koja je upala u hotel i uhapsila ih (agent je uhapšen kako niko ne bi posumnjao da je riječ o tajnom agentu, a poslije je odmah oslobođen).

Tokom cijelog vremena druženja sa Maksicem i sličnim hakerima i kriminalcima, agent je rekao da se ni u jednom trenutku nije osjećao ugroženim i kako uopšte nije imao utisak da je riječ o nekim velikim mafijašima koji su odgovorni za krađe miliona dolara:

"Činili su se kao obični ljudi kakve bi sreli na ulici ili u podzemnoj. Niko od njih nije izgledao kao veliki mafijaš".

Maksim Jastremski je u Turskoj osuđen zbog prevara sa kreditnim karticama te trenutno služi 30-godišnju zatvorsku kaznu.

TUĐE LIČNE PODATKE JE MOGUĆE DOBITI BUKVALNO ZA SITNIŠ, ČAK I ZA 3 DOLARA

Istraživanje pokazuje da je cijena za koju se mogu dobiti finansijske informacije o korisnicima jako pala u odnosu na ranije godine. Želite bankovni račun sa 300.000 dolara na njemu? Mogli biste da ga dobijete za samo 300 dolara, kažu istraživači hakerskog podzemlja.

Za taj iznos, piše BBC, možete da dobijete tuđe podatke o bankovnom računu, te korisničko ime i lozinku, što će vam omogućiti nesmetan pristup tuđem novcu.

Istraživanje o crnom tržištu podataka su radili Džo Stjuart iz Dell SecureWorks i Dejvid Šer, nezavisni istraživač. Oni su pratili ruske i druge forume na kojima se okupljaju oni koji trguju finansijskim podacima.

Stjuart kaže da je cijena za koju se mogu dobiti finansijske informacije o korisnicima jako pala u odnosu na ranije godine. Kompletan dosije o finansijama i drugim

informacijama danas se može dobiti za samo 25 dolara, ako je u pitanju američka žrtva, dok je cijena iste usluge za žrtvu iz Britanije, 30 do 40 dolara.

Prije dvije godine, jedan takav dosije, koji se hakerskom žargonu naziva Fullz, mogao se dobiti za 60 dolara.

Tipičan Fullz sadrži sljedeće podatke o žrtvi: puno ime i prezime, adresu, telefonske brojeve, e-mail adrese sa lozinkama, datum rođenja, podatke o osiguranju, socijalnom, te dodatno može da sadrži podatke o bankovnom računu, kreditnoj kartici, uključujući i PIN kodove.

Pošto se broj onih koji dolaze do podataka korisnika toliko raširio, hakeri, kaže Stjuart, neke od ovih informacija kupcima daju i besplatno, kako bi kupac mogao da ih provjeri, a potom ostale informacije prodaju na veliko. U tom slučaju, podaci za Mastercard ili američke Visa kartice koštaju oko 4 dolara, dok je cijena za britanske ili evropske nešto viša i iznosi sedam do osam dolara.

Razlog zašto podaci ukradeni od žrtava u Americi koštaju manje od onih u Britaniji, odnosno Evropi, leži u činjenici da je za kriminalce teže i skuplje da ukradene podatke prenesu iz SAD, gdje se oni nalaze i ta procedura obično zahtijeva uključivanje posrednika.

Kriminalci godinama postaju i sve sofisticiraniji u svojim ponudama. Ranije su nudili popis brojeva kreditnih kartica, a sada ciljaju na lokacije na kojima se čuva širom spektar ličnih podataka korisnika, kaže Stjuart.

Osim toga, i način na koji potencijalnim kupcima nude ukradene podatke je postao napredniji, pa danas oni postavljaju i web stranice koje pretražuju objekte koji će im omogućiti da dobiju pristupne podatke korisnika.

Stjuart napominje i da bi hakeri, rastom popularnosti virtuelne valute bitcoin, mogli da u narednom periodu promijene fokus i usmjere se na vlasnike bitcoin računa

Stjuart navodi da kriminalci takve servise predstavljaju kao uslužu pretrage zahvaljujući kojoj korisnici pokušavaju da dobiju informaciju o određenim bankama gdje im je najpraktičnije da dođu do gotovine. Hakeri potom pokušavaju da iskoriste propuste u sistemima i tako pristupaju informacijama o kreditnim karticama i drugim podacima.

Za DDoS napad, hakeri traže 3 do 5 dolara po satu, cijena za dan je 90 do 100 dolara, dok za napad koji traje nedjelju dana, treba izdvojiti 400 do 600 dolara.

Na tržištu svoju cijenu imaju i kompromitujući računari (botovi), pa tako 1.000 botova košta 20 dolara, 5.000 košta 90 dolara, dok biste za 250 dolara mogli da dobijete čak 15.000 botova.

Stjuart napominje i da bi hakeri, rastom popularnosti virtualne valute bitcoin, mogli da u narednom periodu promijene fokus i usmjere se na vlasnike bitcoin računa.

„Mnogi bitcoin korisnici ne znaju mnogo o sigurnosti i mnogi koriste jednostavnu kombinaciju korisničkog imena i lozinke, što hakeri mogu lako da provale“, kaže Stjuart.

Za kriminalca je pravo blago ako uspije da ukrade bitcoin digitalni novčanik nekog korisnika, jer vrlo lako može da raspolaže virtualnim novcem i unovči ga gdje želi.

OSMORO UHAPŠENO ZBOG "SAJBER" PLJAČKE BANKE

Britanska policija je danas uhapsila osam osoba optuženih da su provalili u sistem dvije banke i ukrali 1.2 miliona funti

Slika 25. Krađa novca iz banke hakerskim napadima



Izvor: www.newslinksandbundles.blogspot.com

Britanska policija saopštila je danas da je uhapsila osam osoba osumnjičenih da su iz "Barklija" ukrali 1,3 miliona funti (dva miliona dolara) tako što su "provalili" u kompjuterski sistem te banke. Ta grupa je optužena da je na kompjuterski sistem banke instalirala jedan uređaj koji im je omogućio da izvrše "sajber" pljačku. Riječ je o muškarcima, između 24 i 27 godina, koje trenutno policija ispituje, prenijela je agencija AP. Prilikom pretresa više stanova u širem području Londona, policija je pronašla novac, nakit i na hiljade kreditnih kartica. Ova grupa je uhapšena pošto nije uspjela da, na isti način, prošle nedjelje opljačka i banku "Santander".

Otkriveni su pošto je lažni inženjer pokušao da u ekspozituri španske banke "Santander" instalira specijalni "miš", koji se inače koristi za istovremenu kontrolu više kompjutera.

Detektivi su naveli da su na taj način oni mogli da "iz daljine preuzmu kontrolu nad kompjuterom banke".

POVRATAK CISPA-E: POČETAK KRAJA PRIVATNOSTI NA INTERNETU?

"Sajber sigurnost je veliki problem, ali CISPA pokušava da riješi taj problem napadom na slobodu interneta".

Predstavnički dom Kongresa u SAD-u ponovno je izglasao CISPA-u koja po mnogima označava početak kraja privatnosti na internetu

Početkom prošle godine ulice brojnih svjetskih gradova bile su prepune demonstranata koji su političkim elitama i korporacijama poručile da ne žele nikakve zakone kojima će gušiti njihovu privatnost u svrhu borbe protiv sajber terorizma ili piraterije. Tadašnji pritisak je uspio i vremenom su predlozi zakona poput SOPA-e, CISPA-e i ACTA-e odbačeni, ali je sada jasno da je, makar kada je CISPA u pitanju, odbacivanje njegovog izglasavanja bilo samo privremeno - juče je Predstavnički dom američkog Kongresa izglasao ovaj predlog zakona koga još mora da potvrdi Senat i potpiše Barak Obama da bi CISPA i zvanično postala zakon.

Slika 26. Cyber Intelligence Sharing and Protection Act



Izvor: www.shocklee.com

Kako prenosi Huffington Post, CISPA (Cyber Intelligence Sharing and Protection Act) je zakon za zaštitu od sajber terorizma i drugih oblika sajber napada, ali će taj zakon omogućiti privatnim kompanijama da sa drugim korporacijama i američkom vladom dijeli lične podatke svojih korisnika – čak i u slučajevima u kojima su se te kompanije ugovorom obavezale da to neće raditi.

Dakle, CISPA bi bila iznad svih ostalih zakona i kompanije koje su se ugovorom obavezale da neće dijeliti privatne podatke svojih korisnika (poput npr. e-mailova i drugih privatnih informacija), biće oslobođene odgovornosti i potencijalnih civilnih tužbi zbog kršenja tih ugovora.

Zanimljivo je da je jedan delegat Kongresa kao jedan od argumenata zbog kojih bi trebalo izglasati CISPA-u pomenuo i nedavni teroristički napad u Bostonu – Majk Mekaul rekao je da su u tom napadu upotrijebljene prave bombe, a kada je u pitanju sajber prostor to su digitalne bombe i upravo zbog toga "ovaj zakon treba donijeti po hitnom postupku".

Mekaul je dodao da, kada digitalne bombe napadnu SAD, to će biti krivica Kongresa koji nije na vrijeme izglasao ovaj zakon sa kojim bi trebalo da spriječe sajber napade na američku infrastrukturu i institucije.

Kao i prošle godine, organizacije za zaštitu privatnosti smatraju ovaj zakon napadom na privatnost korisnika jer će njegovim donošenjem privatne korporacije i vlada imati

pristup svim ličnim i privatnim podacima korisnika koje će moći međusobno razmjenjivati.

Poslije SOPA, PIPA i ACTA, stiže još kontroverzniji zakon: CISPA >>>

Pirati predlažu alternativu za ACTA, CISPA, SIPA i PIPA >>>

Organizacija Electronic Frontier Foundation (EFF) tražila je da se u ovaj zakon ubaci i amandman prema kojem će privatne kompanije s korisnicima moći da sastavljaju pravno primjenjive ugovore o privatnosti, ali u Predstavničkom domu uopšte nisu glasali o njihovom amandmanu.

Ako na kraju Senat prihvati ovaj zakon u trenutnom obliku, potpisivanje ovakvih ugovora o privatnosti i zaštiti podataka između kompanija i korisnika neće imati previše smisla jer, ako kompanija prekrši taj ugovor, neće biti nikakvih sankcija, a za nadzor i dijeljenje tih (privatnih) podataka neće biti potreban sudski nalog.

Novinar The Guardana cijelu situaciju oko CISPA-a sveo je na rečenicu: "Sajber sigurnost je veliki problem, ali CISPA pokušava da riješi taj problem napadom na slobodu interneta" i dodao da će protiv ovog zakona biti svi oni kojima je stalno do njihove privatnosti u digitalnom

**NASLJEDNICA KGB-A RAZVIJA SISTEM ZAŠTITE OD SAJBER
NAPADA**

U martu 2012. hakeri su napali sajtove agencije "RIA Novosti" i "Gazetu", u novembru 2011. su zaraženi sajtovi agencije "Interfaks", "Komsomolske pravde"...

Rusija će uskoro imati sistem na državnom nivou za upozoravanje, otkrivanje i likvidaciju kompjuterskih napada na svoje informativne sisteme, pišu Novosti.m Vladimir Putin je potpisao ukaz kojim je zadužio Federalnu službu bezbjednosti, nasljednicu KGB da stvori "zaštitni zid" protiv sajber-napadača. Cilj je da se zaštite informativni sistemi i informativne-telekomunikacione mreže na teritoriji Rusije, ali i diplomatska predstavnštva Rusije u inostranstvu.U novom sistemu zaštite od kompjuterskih napada, pišu Novosti, osim državnih organa će biti uključeni i vlasnici informativnih resursa, od sajtova da banaka podataka, kao i operatori veza i kompanije koje imaju licence da se bave zaštitom u ovoj oblasti.

Ruski krivični zakon predviđa kazne do sedam godina zatvora za ulazak u zaštićene informativne sisteme. Sredinom januara ove godine poznata ruska kompanija "Laboratorija Kasperskog", koja se bavi pravljenjem anti-virusnih sistema, saopštila je da je otkrila veliku sajber-špijunsku mrežu koja je od 2007. godine sprovodila operaciju "Crveni oktobar". Napadani su kompjuteri, mobilni telefoni i korporativne mreže, između ostalog, i na teritoriji bivšeg SSSR-a. Glavni cilj im je bio da uđu u sisteme vladinih i diplomatskih struktura kao i kompanija i naučnih instituta.

Problemi sa upadima u ruske kompjuterske sisteme nisu rijetkost. U martu 2012. hakeri su napali sajtove agencije "RIA Novosti" i "Gazetu", u novembru 2011. su zaraženi sajtori agencije "Interfaks", "Komsomolske pravde" i još nekih listova. Od hakera nisu mogli da se odbrane ni u Ruskim željeznicama kao i glavnoj upravi Ministarstva za vanredne situacije Rusije, pišu Novosti.

Rusi kao prijetnja

U štabu NATO u Briselu, smatraju da im je glavna opasnost na ovom polju prijeti od Rusije, Kine i Irana. NATO je prošle godine napravio i simulaciju sajber sukoba gdje je iscenario kompjuterski napad na Mađarsku i Estoniju.

IVO SU INTERNET STRANICE KOJE NE SMIJETE OTVARATI

Nikada nemojte vjerovati neprovjerenom kontaktu, davati povjerljive informacije i šifre putem interneta... S obzirom na to da su korisnici interneta već odavno daleko oprezniji sa sumnjivim stranicama i mailovima, hakeri su pronašli nove načine za prevare. Istraživanje kompanije MacAfee pokazalo je da su prevare na internetu i hakovanje u porastu. S obzirom na to, ABC News donosi pet stranica koje je dobro izbjegavati.

1. Nepoznate mobilne aplikacije

U porastu su napadi na aplikacije za Android, a najpopularnije prevare su one koje stižu od "vaše banke" ili one aplikacije koje traže da doplatite za noviju, nadograđenu verziju.

2. Lažni službenici

Među novijim prevarama su i lažni službenici koji žrtve kontaktiraju putem maila ili tekstualnih poruka. U poruci vam nude pomoći u "lječenju" vašeg računara zajedno s linkom na koji bi trebalo da kliknete. Klik na poveznicu zapravo omogućava ulaz hakerima u vaš računar.

3. Pornografske stranice

Tokom surfanja je moguće da slučajno kliknete na prozor koji može da odjednom iskoči i tako se nađete na stranici s pornografskim sadržajem.

4. Prevare s računima

Ovdje je riječ o porukama, mailovima i telefonskim pozivima iz "vaše banke", a traže vaše podatke radi uklanjanja određenog problema.

5. Spamovi

Iako su korisnici već naviknuti na neželjenu poštu, istraživanja su pokazala da Amerikanci najčešće kliknu na mailove u kojima se pominju lijekovi.

Nikada nemojte vjerovati neprovjerenom kontaktu, davati povjerljive informacije i šifre putem interneta, i budite oprezni prema mailovima nepoznatih pošiljalaca i ne otvarajte linkove koje vam oni šalju.

SAJBER KRIMINAL U AUSTRIJI U ZABRINJAVAĆEM PORASTU

Kriminalne bande sve više koriste mogućnosti pametnih telefona, čiji udio na tržištu značajno raste, za sopstveno bogaćenje. Sajber kriminal se u Austriji u značajnom je porastu, pokazuje izvještaj Savezne kriminalističke službe (BK), predstavljen u Beču.

Sa nešto više od 10.000 prijavljenih slučajeva se broj prekršaja prošle godine u poređenju sa 2011. gotovo više nego udvostručio. BK procjenjuje da je tačan broj sajber krivičnih djela daleko veći, i ukazuje da su "pametni telefoni" sve češća meta kriminalnih napada, piše Tanjug a prenosi portal Gde investirati.

Prošle godine je prijavljeno ukupno 10.231 krivično djelo iz oblasti sajber kriminala, što je gotovo udvostručenje u poređenju sa 2011, kada je podnijeta 4.831 prijava. Stopa riješenih slučajeva iznosila je oko 25 odsto, što je smanjenje za oko 20 procenata u poređenju sa 2011, proizilazi iz izvještaja.

BK ističe da su uzroci za smanjenje stope sve veća profesionalizacija kriminalnih bandi, koje su organizovane i međunarodno umrežene, kao i zbog sve učestalije upotrebe programa koji nanose štetu računarima. Istovremeno je rad policije otežan zbog upotrebe sloga za anomimizaciju korisnika, kao i novih tehnologija.

Udio pametnih telefona u Austriji je porastao do 2012. na 60 odsto, a pored uspostavljanje telefonskih razgovora ova vrsta mobilnih korisnicima otvara mogućnosti i za sve škakljivije zadatke kao što su tele-benking i elektronska plaćanja. Kriminalne bande sve više koriste mogućnosti pametnih telefona za sopstveno bogaćenje.

Inače, osumnjičeni za krivična djela iz oblasti sajber kriminala su između 25 i 40 godina starosti, i u 76 odsto slučajeva su iz Austrije. Takođe, izvještaj pokazuje da je prošle godine zabilježen i blagi porast kod dečije pornografije. Prema statistici BK, broj prijava iz ove kategorije porastao je sa 502 na 543.

Trend je da broj internet sajtova sa sadržajem dječije pornografije opada, ali da se ovakva vrsta materijala pojačano razmjenjuje preko foruma i četova u socijalnim mrežama. Ministarstvo unutrašnjih poslova Austrije počelo je prošle godine primjenu strategije borbe protiv sajber kriminala. Glavni dio strategije je uspostavljanje centra za borbu protiv sajber kriminala.

STROŽE KAZNE ZA SAJBER KRIMINAL U EU

Prema postignutom dogovoru, maksimalna kazna za djela vezana za ilegalni pristup informacionim sistemima trebala bi da bude najmanje dvije godine zatvora.

Evropski parlament prihvatio je predlog povećanja kazni za sajber kriminal unutar zemalja članica Evropske unije. Prema postignutom dogovoru, maksimalna kazna za djela vezana za ilegalni pristup informacionim sistemima trebala bi da bude najmanje dvije godine zatvora, prenosi portal bug.hr. Najviša kazna za kompjuterske napade na kritičnu infrastrukturu, kao što su elektrane, saobraćajnice ili vladine mreže, trebala bi da bude pet godina ili više.

Takođe, povećavaju se kazne za ilegalno presretanje komunikacije ili proizvodnju i prodaju alata koji to omogućavaju, a firme koje iznajmljuju botnetove ili hakere za krađu podataka bitće odgovorne za svaki prekršaj koji je napravljen tom prilikom.

Vlade zemalja Evropske unije imaju sada dvije godine za primjenu ovih odluka u konkretnim nacionalnim zakonima.

SAD: OSAM HAKERA OPTUŽENO ZA KRAĐU 45 MILIONA DOLARA

Hekeri su koordinisane akcije izveli 22. XII prošle i 19. i 20. II ove godine, tako što su najprije upali u bazu podataka bankovnih kartica, a zatim opljačkali bankomate širom svijeta

Grupa sajber pljačkaša banaka je u dva navrata krajem prošle i početkom ove godine, za samo nekoliko sati, sa računa u 26 zemalja ukrala 45 miliona dolara, a u vezi sa ovim slučajem danas je u Njujorku za zavjeru i pranje novca optuženo osam hakera.

Državni tužilac u Bruklincu Loreta Linč je, čitajući optužnicu protiv članova njujorske hakerske ćelije, ovaj slučaj uporedila sa čuvenom pljačkom Lufthanze s kraja 1970-ih, ovjekovječene u filmu Martina Skorsetza "Dobri momci", javio je AP.

Hekeri su koordinisane akcije izveli 22. decembra prošle i 19. i 20. februara ove godine, tako što su najprije upali u bazu podataka bankovnih kartica, a zatim opljačkali bankomate širom svijeta prethodno uklonivši limite za podizanje gotovog novca i koristeći lažne kartice. U vezi sa ovim slučajem u SAD je ranije ove godine uhapšeno sedam osoba kojima prijete zatvorske kazne od 10 godina, a njihov vođa Alberto Jusi Lajud-Pena je ubijen krajem aprila u Dominikanskoj Republici.

Grupa je uhvaćena pošto je jedan osumnjičeni viđen na snimcima bezbjednosnih kamera sa rancem punim novca, dok su se drugi fotografisali sa svežnjevima novčanica na Menhetnu.

Američki istražitelji nastavljaju da rade na ovom slučaju, a za sada je poznato da su hapšenja sprovedena i u drugim zemljama, ali se i dalje ne zna ko su glavni organizatori, niti gdje se nalaze.

Hakerski napadi prerasli u ozbiljan problem

"Potrebno podići svijest kako građana tako i nadležnih institucija o tome koliki je značaj uspostavljanja stabilne infrastrukture kojom ćemo zaštititi sajber prostor"

Za razliku od hakerskih napada iza koji su prije 15 godina uglavnom stajali tinejdžeri, danas je sajber kriminal mnogo ozbiljnija pojava motivisana ne samo sticanjem finansijske dobiti, a ozbiljne posljedice zbog toga mogu trpjeti pojedinci, preduzeća, ali i Vlade, poručila je ministarka odbrane Milica Pejanović – Đurišić.

Slika 27. Milica Pejanović Đurišić



Izvor: www.kodeks.me

Ona je na konferenciji "Sajber bezbjednost" u organizaciji kompanije Microsoft navela da smo u današnje vrijeme svjedoci sve većeg broja sajber napada, pa se često osjetljivi lični i poslovni podaci mogu naći na otvorenim mrežama.

"Podaci pokazuju i da u vremenu ozbiljne krize sajber kriminal predstavlja aktivnost čiji obim ima dvocifreni rast, kao što je to u ostalom i slučaj sa svim ostalim nelegalnim

aktivnostima. U tim uslovima i efekti sajber kriminala postaju sve ozbiljniji za pojedince, preduzeća, pa i za Vlade. Zato je potrebno podići svijest kako građana tako i nadležnih institucija o tome koliki je značaj uspostavljanja stabilne infrastrukture kojom ćemo zaštititi sajber prostor", kazala je Pejanović – Đurišić.

I Vlada Crne Gore, kako je navela, suočava se sa potrebom dodatnog angažmana u pravcu uspostavljanja dobrog zakonodavnog okriva sa ciljem postizanja veće bezbjednosti. Ona je dodala da je jasno da nacionalne strategije i politike sajber odbrane ne mogu ni izdaleka biti dovoljne imajući u vidu činjenicu da je riječ o izazovima koji imaju globalni karakter.

"Ministarstvo odbrane je u prethodnom periodu sa NATO partnerima dinamiziralo saradnju na polju sajber odbrane polazeći od usvojenog strategijskog koncepta fokusiranog na razvijanje sposobnosti država članica da koordinirano preveniraju, detektuju, odbrane se i oporave od eventualnih sajber napada", kazala je ona i dodala da je program "Nauka za mir i bezbjednost "namjenski osmišljen za Crnu Goru, BiH i Makedoniju.

Pejanović – Đurišić je istakla i da se Crna Gora suočava sa problemom finasiranja projekata koji zahtjevaju i visok nivo ekspertske znanja.

Generalni direktor Microsofta za 24 zemlje centralne i istočne Evrope Takijo Hirano naveo je da je sajber bezbjednost postala veoma važna tema u poslednjih šest mjeseci u agendama mnogih Vlada. Kako je kazao i svijest o tom problemu podignuta je na veći nivo u prethodnih par godina.

Direktor te kompanije za Crnu Goru Oliver Obradović dodao je da je u vremenu kada se trči za informacijama i kada je Internet ušao u svaku oblast ljudskog djelovanja prirodno je da postoje pojedinci i organizovane grupe koji žele da informatičke resurse stave u funkciju nelegalnog sticanja protivpravne koristi, širenja informacija, bespravno korišćenje autorskih prava intelektualne svojine.

Slika 28. Oliver Obradović



Izvor: www.tehnika-informatika.com

"Internet je idealno mjesto za njihovu komunikaciju i kolaboraciju i tehnike kojim se služe na internetu omogućavaju im relativno bezbjednu komunikaciju. Pravi efikasan način odgovora na prijetnje visokotehnološkog kriminala je dobar regulatorni okvir, adkevatni institucionalni i tehnički kapaciteti, međunarodna saradnja, a naročito bolja saradnja državnih organa i privatnog i javnog sektora", istakao je Obradović.

Ministar za informaciono društvo i telekomunikacije Vujica Lazović kazao je da se države trude da izgrade nacionalne odbrambene mehanizmem i intenziviraju regionalnu i međunarodnu sradnju u toj oblasti.

On je naveo i da je Crna Gora donijela niz zakona i regulativa kojom se uređuje funkcionisanje, poslovanje i bezbjednosti sajber prostora. U okviru tog ministarstva osnovan je i Odsjek za borbu protiv računarskog kriminala i da su do sada učestvovali u rješavanju brojnih incidenata.

ETIČKI HAKERI SVE TRAŽENIJI: ZNAJU SVE KAO ZLONAMJERNI, ALI SU IM MOTIVI DRUGAČIJI

Etički hakeri prikupljaju informacije o ranjivosti sistema. Dostavljaju ih kompaniji koja ih je unajmila, s predlogom mjera zaštite. Institucije, mediji i banke često su meta hakerskih napada. Da li su podaci kojima raspolažu bezbjedni kao i lični podaci građana brinu takozvani etički hakeri. U Bosni i Hercegovini njihove usluge su sve više tražene. Ko su etički hakeri i šta je njihov posao, istraživala je reporterka Al Jazeere Ljiljana Smiljanić.

Etički, ili hakeri s bijelim šeširom, prikupljaju informacije o ranjivosti sistema. Dostavljaju ih kompaniji koja ih je unajmila, s predlogom mjera zaštite. Mogu testirati

izvana ili u kompaniji, pojašnjava Zoran Đurić, predsjednik udruženja koje se bavi tom problematikom.

Mogu, ali i ne moraju znati ništa o sistemu kompanije koja ih je angažovala. I to nisu jedini načini prikupljanja informacija.

Drugačiji motivi

"Pokušaj da se preko korisnika informacionog sistema dođe do osjetljive informacije, kao što je korisničko ime i lozinka za pristup informacionom sistemu, kao što su neke druge osjetljive informacije, pa da ih onda možda u nekoj drugoj fazi, nekog tehničkog napada koristi etički haker da bi došao do neke druge ili treće osjetljive informacije", kaže Đurić, prvi čovjek Udruženje za reviziju, kontrolu i sigurnost informacionih sistema Republike Srpske (RS).

Etički hakeri koriste isto oružje kao i oni koji nisu dobromanjerni. Motivi su im drugačiji.

U nekim zemljama regiona, poput Slovenije, Hrvatske i Srbije, usluge etičkih hakera su godinama u upotrebi. Bosna i Hercegovina još nije dostigla taj nivo, ali je interes sve veći.

Većina institucija sa kojima su reporteri Al Džazire bili u kontaktu su ili zainteresovane, ili planiraju da u narednih godinu dana izvrše takve vrste testiranja, s obzirom da odnedavno u BiH postoji i regulativa koja podržava takvu vrstu testiranja. Sve regulative koje su prisutne u posljednje vrijeme većinom su bazirane na preporukama ISO 27.000 standarda za upravljanje sigurnošću informacijama“, rekao je Đurić.

Banke najranjivije

Kreditne kartice i elektronsko bankarstvo učinili su banke najranjivim na napade hakera. Upravo zato najviše banke u Bosni i Hercegovini koriste usluge etičkih hakera.

Na taj način štite i svoje poslovne podatke, ali i lične podatke svojih klijenata. Sve banke uglavnom imaju svoje timove ljudi koji brinu o bezbjednosti sistema.

"Predstavlja osnovu za optimizaciju ulaganja u IT strukturu i sve druge mjere zaštite informacionog sistema. Zatim, povećanje svjesnosti i budnosti zaposlenih banke, fokusiranje stalnih edukacija po pitanju informacione bezbjednosti na određenu

problematiku i ranjivosti, koje su otkrivene...", kaže Zoran Antić, IN menadžer Hypo Alpe Adria Bank.

Ipak, bankari upozoravaju da su prva linija odbrane sami korisnici. Ukoliko građani ne čuvaju svoje kreditne kartice, pin kodove, lozinke... stručnjaci ne mogu mnogo uraditi.

NI CRNA GORA NIJE IMUNA NA SAJBER KRIMINAL, MOŽETE POSTATI NAPADAČ, A DA TO I NE ZNATE

Uskoro bi trebalo da bude usvojena Strategija o sajber bezbjednosti i aktiviran specijalni broj putem kojeg ćete moći da prijavite prevare.

Kancelarija kao i svaka druga. U njoj sjede članovi CIRT tima Ministarstva za informaciono društvo, čiji je zadatak borba protiv sajber kriminala.

"Izuzetno atraktivno područje za kriminal",

U sajber svijetu, procjenjuje se da je svake sekunde 14 ljudi prevareno, a neka istraživanja pokazuju da je šteta od sajber kriminala na godišnjem nivou čak 414 milijardi eura. I Crna Gora je dio toga.

Adis Balota iz MIDT podsjeća da je CIRT timu prijavljena takozvana phishing prevara na e-bankingu - kada se na internetu pojavio lažni sajt Prve banke, registrovan u inostranstvu.

POJAVIO SE LAŽNI SAJT PRVE BANKE

"Imali smo i zahtjev od CIRT tima iz Indije, gdje se na teritoriji Crne Gore, gdje je registrovan .me domen, nalazi preko 20 lažnih sajtova e-bankinga njihovih banaka koje su registrirane u Indiji", kaže Balota.

Pomagali su i u slučaju krađe profila jedne naše javne ličnosti na Facebooku, kada su direktno sa ljudima iz te kompanije rješvali problem.

Crna Gora od Facebooka tražila podatke o dva korisnika >>>

Članovi tima sjećaju se i hakerskog napada na sajt Vlade.

Ana Rakočević iz CIRT Crna Gora kaže da su napadači bili uglavnom kosovski hakeri. Reakcija tima je, kaže bila brza.

"Pratili smo fajlove i vidjeli sa kojih adresa dolaze napadi".

Balota kaže da je, više nego u bilo kojoj drugoj sferi života, kada je sajber kriminal u pitanju, izuzetno bitna brza reakcija.

CIRT Crna Gora je ove godine imala 25 slučajeva. Jedan od najvećih je slučaj dječaka iz podgoričkog naselja Blok 5. Sve je počelo kada su im kolege iz Hrvatske javile da se iz Crne Gore napada njihov bankarski sistem. Slučaj je riješen u saradnji sa tužilaštvom, kada su blokirane sporne IP adrese.

Tom akcijom je, kaže Balota, spriječena pronađenja oko 26.000 eura.

Crnogorski hakeri su klinci

Dječak iz Bloka 5 nije ni znao šta radi - njegov računar je bio zaražen trojancem i postao je zombi, što je omogućilo hakerskoj grupi da preuzme komandu nad njegovim računaram.

Taj slučaj pokazuje čega sve ima u internet svijetu i otvara pitanje kako da se ponašamo u sajber prostoru.

"Isto kao u fizičkom, uz malo veću dozu opreznosti", kaže Balota.

Na internetu ostavljajte što manje ličnih podataka, preko interneta nikad ne plaćajte karticom preko koje primate platu. Za online kupovinu uvijek otvorite drugi račun...

U MIDT kažu da bi uskoro trebalo da bude usvojena Strategija o sajber bezbjednosti i aktiviran specijalni broj putem kojeg ćete moći da prijavite prevare.