CYBER KRIMINAL I ZAŠTITA PRIVATNOSTI U CYBER SVIJETU

CYBER CRIMINAL AND PRIVACY PROTECTION IN THE CYBER WORLD

Stručni članak

Mirsada Karahmetović dipl. pravnik[*]
Kenan Mujić dipl. ing. elektrotehnike[*]
Vahidin Đaltur mr. sci. IT [*]

Sažetak

U radu je prikazan značaj i uloga borbe protiv cyber kriminala. Također su opisani primjeri i pravila nastanka i medote zaštite odnosno prevencije ove od vrste kriminala. Cyber kriminal ili kompjuterski orjentisan kriminal, je kriminal koji uključuje kompjutere i lokalnu ili globalnu mrežu. Svaki kompjuter može biti korišten u u činjenju krivičnog djela ili može biti meta počinioca. Cyber kriminal se može definisati kao: " krivična djela koja su počinjena protiv pojedinca ili grupe pojedinaca sa s kriminalnim motivom da namjerno naštete ugledu žrtve ili nanesu fizičku ili mentalnu štetu ili gubitak, žrtvi direktno ili indirektno, koristeći moderne telekomunikacijske mreže kao što su internet i mreže mobilnihih (Bluetooth/SMS/MMS,NFC) telefona. Cyber kriminal može biti prijetnja za ličnu ili nacionalnu finansijku sigurnost.

Problemi oko ovih vrsta krivičnih dijela postali su značajni, naručito oni koji se tiču hakiranja, kršenja autorskih prava, ilegalnog masovnog nadzora, seksualnog iznuđivanja, dječje pornografije i odgajanja djece.

Ključne riječi: sajber, kriminal, računar, mreže, sigurnos, napad, zaštita.

Abstract

This paper shows the importance and role of fighting cybercrime. Examples and rules for the emergence and methods of protection and prevention of this type of crime are also described. Cybercrime, or computer-

[*] *e-mail: karahmetovic.mirsada@gmail.com*
[*] *e-mail: kenan.mujic@hotmail.com*
[*] *e-mail: vahidin.djaltur@gmail.com*

oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target of the offender. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones networks (Bluetooth/SMS/MMS,NFC)".

Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those regarding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming

Key words: cyber, crime, computer, network, security, offence, protection.

1. UVOD

Razvojem kompjuterskih sistema i kompjuterskih mreža te naglim razvojem „pametnih telefona“ (eng. smartphone) od 2010. godine kreiran je razvijan novi način činjenja krivičnih djela putem kompjuterskih sistema, koja krivična djela sve učestalije nazivamo jednim pojmom – cyber kriminal. Pojam „cyber“ je engleska riječ koja predstavlja prefiks koji se koristi za nešto što za svoju osnovu ima elektroniku, a koristi se za virtuelne pojmove i stvari koji su vezani za kompjutersku mrežu i sisteme mobilnih telefona.

Države članice Vijeća Evrope i ostale države potpisnice, dana 23.01.2001. godine u Budimpešti, usvojile su Evropsku konvenciju o kompjuterskom kriminalu a Bosna i Hercegovina je dana 25.03.2006. godine je donijela Odluku o ratifikaciji ove Konvencije. Cilj ove Konvencije je da realizira vijeće jedinstvo između svojih članova i intenziviranje saradnje sa drugim državama članicama Konvencije u borbi protiv cyber kriminala i potrebu za zaštitom legitimnih interesa povezanih sa razvojem kompjuterskih tehnologija, sprečavanje zloupotrebe kompjuterskih sistema, mreža i podataka, te brža i efikasnija borba protiv krivičnih djela počinjenih u cyber prostoru, olakšavajući njihovo otkrivanje, istragu i gonjenje kako na unutrašnjem tako i međunarodnom nivou.

Konvencija razlikuje četiri vrste krivičnih djela počinjenih u cyber prostoru, i to:

- djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema, u koja se ubrajaju: nedozvoljeni pristup kompjuterskim sistemima, povreda integriteta podataka, povreda

integriteta sistema i zloupotreba;
- kompjuterska djela, u koja se ubrajaju kompjutersko falsificiranje i kompjuterska prevara;
- djela vezana za sadržaj, u koja se ubrajaju djela koja se odnose na dječiju pornografiju;
- djela u vezi sa napadom na intelektualnu svojinu i odnosna prava.

Cilj Konvencije je da države potpisnice uvrste prethodno navedena krivična djela u nacionalna krivična zakonodavstva, ukoliko to već nisu učinile.

Konvencija je naročito važna zbog brzine djelovanja strana u postupku.
- Jedna država potpisnica Konvencije može tražiti od druge države potpisnice brzo čuvanje pohranjenih podataka putem kompjuterskog sistema koji se nalaze na teritoriji te druge strane, a uvezi kojih strana koja traži pomoć ima namjeru da podnese zahtjev za pomoć u cilju pretraživanja ili nekog sličnog pristupa, zapljene ili na drugi način distribuisanja navedenih podataka,
- Jedna država potpisnica može tražiti od druge brzu distribuciju čuvanih podataka,
- Jedna država potpisnica može tražiti od druge da pretraži ili na neki drugi način pristupi, zaplijeni ili na drugi način pribavi podatke i pohranjene podatke putem kompjuterskog sistema distribuira drugoj strani.

Države potpisnice, pa tako i Bosna i Hercegovina su odredile kontakt tačku u ovakvim vidovima međunarodne pomoći i sradnje, koja će biti dostupna za saradnju 24 sata na dan i 7 dana u sedmici, a u cilju osiguranja trenutne pomoći u istragama koje se tiču krivičnih djela povezanih sa kompjuterskim sistemima. Kontakt tačka u Bosni i Hercegovini je ovlaštena službena osoba iz Federalne uprave policije Federacije Bosne i Hercegovine i ovlaštena službena osoba iz Ministarstva unutrašnjih poslova Republike Srpske.

Međutim, važno je napomenuti da tačka za kontakt služi da bi se procedura zbog hitnosti ubrzala, ali ovaj način saradnje ne isključuje oficijelnost zamolbe, odnosno, molba za pružanje pravne pomoći mora biti sačinjena formalno. Nakon kratkog izlaganja o međunarodnoj saradnji, mehanizmima u borbi protiv cyber kriminala, te spoznaje da države sistemski rade na suzbijanju, otkrivanju i kažnjavanju počinitelja krivičnih djela putem kompjuterskih sistema, važno je i preventivno djelovati i zaštiti se od Cyber napada.

2. ZAŠTITITA OD OVOG OBLIKA KRIMINALA TE ZAŠTITA VLASTITE PRIVATNOSTI

Nemoguće je apsolutno zaštiti svoju privatnost u cyber svijetu, jer telefon, računar, ili bilo koji drugi elektronički uređaj su potencijalni pristupi privatnom životu korisnika istih, ali se rizik pristupu informcijama može itekako smanjiti ukoliko se poduzmu određene mjere zaštite podataka. Da bismo osigurali naš računar, podatke koji se nalaze u njemu i sve ono što radimo koristeći internet, neophodno je poduzeti određene mjere zaštite od mogućih cyber upada u naš računar, pokušaja preuzimanja podataka ili kontrole nad uređajem od strane raznih vrsta specijaliziranih i dobro obučenih cyber kriminalaca.

Postoje određene mjere i metode predostrožnosti koje se mogu napraviti u cilju zaštite od cyber kriminala. Neke od njih se realizuju na sl. način:

1. Korištenje anivirusnog paketa koji obuhvata kompletnu uslugu internet sigurnosti, kako bi se zaštitili od virusa i ostalih prijetnji. Malware je zajednički naziv za štetne programe koje cyber-kriminalci koriste kako bi pristupili tuđim kompjuterima. Takvi programi su obično skriveni u prilozima ili besplatnom sadržaju. Antivirusni program je potrebno redovno ažurirati i svake sedmice skenirati cijeli kompjuter.
2. Koristiti jake šifre koje nije lako pogoditi, ne treba ponavljati istu šifru na različitim stranicama, te ih mijenjati s vremena na vrijeme. Kada se bira šifra ne treba koristiti neku riječ ili datum koji imaju veze sa nama lično, već generisane šifre, a u tome nam može pomoći *password generator*. Kako se ne bi desilo da zaboravimo svoju šifru, *lastpass* vrlo lako može pohraniti i sačuvati šifru za bilo koju stranicu. To će smanjiti šansu da neko pogodi našu šifru te ukrade naš identitet, zloupotrijebi informacije i slično.
3. Zaštititi svoje lične informacije na društvenim mrežama pomoću postavki za privatnost. Lični podaci koji su lako dostupni cyber kriminalcima mogu biti iskorišteni protiv nas, tako da, što manje informacija dijelimo sa svijetom, to je bolje sa aspekta sigurnosti. Treba voditi računa o sadržaju koji se objavljuje, jer sve što se jednom objavi, zauvijek ostaje na internetu.
4. Također je vrlo važno voditi računa o tome koje stranice posjećujemo i na kojim sajtovima pravitmo svoje korisničke račune. Ukoliko posjećujete online casina, trebalo bi pratiti savjete stručnjaka koji stranice detaljno pregledaju i ocijene da li su sigurne i pouzdane.
5. Zaštita kućne mreže *(home network)* sa jakom šifrom, kao i VPN. VPN *(virtual private network)* će šifrirati sav promet ostavljajući naše uređaje dok ne stigne na odredište. Čak i ako haker uspije doći u našu

komunikacijsku liniju, oni neće opstruirati ništa osim šifriranog prometa.

6. Oprezno surfati internetom i paziti kakav sadržaj se preuzima. Pripaziti se lažne e-poruke *(phishing)* finansijskih institucija u kojima se od nas traži da potvrdimo podatke o računu. Takve e-poruke prijavite institucijama od kojih navodno dolaze, kako bismo pomogli u razotkrivanju prevaranta. Finansijske institucije nikada od svojih korisnika ne traže potvrdite putem e-poruka.
7. Razgovarati sa svojom djecom o prihvatljivom načinu upotrebe interneta i pratiti njihovu online aktivnost. Usmjeriti ih ka prikladnim internetskim stranicama. Osigurajti im da znaju da vam se mogu obratiti ukoliko dožive bilo kakvo neugodno iskustvo online, poput uznemiravanja ili uhođenja.
8. Ukoliko smatrate da ste žrtva cyber krimnala, morate upozoriti lokalnu policiju o onome šta vam se dešava. Iako vam se čini da zločin možda i nije toliko ozbiljan, ipak ga prijavite jer time možete pomoći u preveniranju iskorištavanja ljudi u budućnosti. (Mitnick, 2018)

3. ZAŠTITA ŠIFRE OD HAKIRANJA

Da bismo zaštitili svoje online račune, prije svega moramo imati jaku šifru. Kratka definicija hakiranja bi bila sticanje neovlaštenog pristupa podacima u sistemu ili računaru. Nije neobično da većina ljudi, pa čak i ozbiljnih kompanija imaju kratke i jednostavne maksimalno personalizovane šifre koje su jednostavne za pamćenje, te nije ni čudo što se dešavaju neovlašteni upadi i hakiranja.

U 21. vijeku imamo mogućnost da se zaštitimo od neovlaštenih upada u naše korisničke račune. Najjednostavniji način zaštite je kreiranjem jake i kompleksne čifre koja se sastoji od malih, velikih slova i brojeva.

Možda zvuči komplikovano, ali postoji automatski i ručni način kreiranja šifri.

Kada je riječ o automatskom načinu kreiranja šifri, postoji nekoliko digitalnih menadžera šifri, kao što je naprimjer "KeePass password Safe" i drugi, koji funkcionišu po principu ne samo da čuvaju našu šifru sigurnom, nego i generiraju nove i jake šifre za bilo koji drugi račun ili web lokaciju kada vam zatreba.

Međutim, i kod korištenja menadžera šifri postoje određeni rizici. Naprimjer, menadžer šifri koristi master šifru koju ste vi prethodno generirali za pristup svim ostalim šiframa, te ukoliko neko zarazi naš kompjuter ili nekim slučajem dođe u posjed naše master šifre, u tom slučaju ima pristup i svim ostalim šiframa. Najbolji način i u ovom slučaju je da naša master šifra bude jaka odnosno treba da se sastoji od najmanje 20 karaktera, brojeva, slova i drugih slučajnih karaktera, kako bi se mogućnost razbijanja ovakve

šifre svela na minimum.

Također treba imati na umu pravilo da, ukoliko želimo jaku šifru, nikada je ne smijemo koristiti za dva različita računa, jer će i u ovoj situaciji osoba koja uspije razbiti našu šifru imati pristup i drugim računima ukoliko koristitmo istu šifru (npr. ista nam je šifra za facebook račun, instagram, email, mobilno bankarstvo...).

Čak i kada imamo jaku šifru nismo apsolutno zaštićeni, jer postoje mnogi besplatni programi koje može bilo ko preuzeti a koji služe za razbijanje šifri. Međutim, kreiranjem jake i dugačke šifre, proces razbijanja šifre je dugotrajan te je velika vjerovatnoća da će i hakeri nakon više desetina sati provedenih na razbijanju tako jake šifre i odustati. Dakle, vjerovatnoća da se apsolutno zaštitimo je mala, ali je uz jaku šifru znatno manja mogućnost za neovlašteni pristup našim računima odnosno proboja naše šifre. Na svu sreću, neke web lokacije, kao što je internet bankarstvo ili email adresa, blokiraju račune nakon tri neuspjela pokušaja ukucavanja šifre, što hakerima otežava put do našeg računa. (Mitnick, 2018)

Kao što šifrom štitite svoje online račune, isto tako morate zaštiti svoje elektronske uređaje, kao što su mobiteli, iPad-i, laptopi, računari. Neophodno je zaštiti kako svoje kućne, tako i službene elektroničke uređaje.

Npr. pozvali smo društvo na kućnu zabavu, a ostao nam je uključen računar, dovoljno je da neko od znatiželjnih gostiju sjedne za računar i na taj način uđe u našu privatnost, kao što su razni folderi, privatne fotografije ili još gore, naše šifre za online račune. Ista je situacija i na poslu, pozvali smo npr. konkurenciju na sastanak, dovoljan je samo jedan mali tren nepažnje da uđu u naše projekte, finansijske konstrukcije ili da pogledaju našu elektronsku poštu. Dakle, neophodna je zaštita šifrom, i to na način da se naš elektronički uređaj automatski zaključava nakon nekoliko sekundi nekorištenja, ili još kreativniji način je da uparimo svoj kompjuter sa mobitelom putem bluetooth, te kada se udaljimo sa mobitelom od kompjutera, isti se automatski zaključava. Isto se može postići i sa uređajima koji koriste bluetooth kao što su narukvice ili smart satovi koji funkcionišu po istom principu, tj. kada se udaljimo iz dometa uređaja, isti se automatski zaključava.

Što se tiče mobilnih uređaja, postoje tri načina zaštite od neželjenog pristupa, i to putem šifre, zatim vizuelnog otključavanja, te biometrijski način otključavanja otiskom prsta ili prepoznavanjem lica ili skeniranjem zjenice oka.

Kada je u pitanju otključavanje telefona putem šifre, nikada ne koristiti automatsku šifru koju nam sistem nudi (najčešće četiri nule), potrebno je da sami kreiramo šifru tako što ćemo ući u postavke telefona i ručno kreirati šifru koju ćemo samo mi znati i koja će sadržavati više od četiri cifre, po mogućnosti kombinacija slova i brojeva. Preporučuje se da šifra sadrži

sedam ili više cifri, kombinacija slova i brojeva, obzirom da pametni telefoni uglavnom imaju opciju koja na tastaturi za zaključavanje nudi oboje, slovne i brojčane tipke na istom displeju što je jednostavnije za disponiranje i sačinjavanje kombinacije šifre.

Druga opcija otključavanja je vizuelna tzv. Android lock patterns. Radi se o devet tačkica na displeju koje je potrebno spojiti na način koji mi želimo tj. koji podesimo i na taj način generiramo šifru. Međutim, ova šifra nije nasigurnije rješenje, jer ljudski mozak funkcioniše na način da sebi olakša korištenje, te većina korisnika ovog vida šifre spajajući ponuđene kombinacije tačkica unesu svoje prvo slovo imena, ili neke vrlo svojstvene simbole, što hakerima olakšava posao za pristup našem telefonu i podacima.

Treći način otključavanja je biometrijski. Pametni telefoni u posljednje vrijeme nude opciju otključavanja otiskom prsta ili prepoznavanja lica. Međutim, ovo je dosta nesiguran način zaštite telefona naročito kada uzmemo u obzir činjenicu da postoje vrlo jednostavni stari metodi za pobjedu nad ovim načinom zaštite. To uključuje snimanje otiska prsta pomoću dječijeg pudera i selotejpa. Takođe kada je riječ o otključavanju putem prepoznavanja lica, vrlo je jednostavno otključati telefon pomoću fotografije visoke rezolucije.

Dakle, biometrija je sama po sebi ranjiva na napade. Idealno bi bilo kada bi biometriju koristili kao jedan od autentifikacijskih faktora. Dakle koristimo biometriju (otisak prsta ili prepoznavanje lica) a potom unesemo pin ili šifru, te će jedino na taj način naš mobilni telefon biti siguran.

Samsung electronics već neko vrijeme nudi razvijeniju i mnogo sigurniju opciju otključavanja mobilnih telefona tako što kombinira skenerinja lice i skeniranje zjenica očiju, što postavlja ovu metodu otključavanja uređaja na sasvim novi i bolji level sigurnosti. Iako se ova metoda otključavanja odvija velikom brzinom tj. ispod pola sekunde, korisnici i dalje preferiraju najbržu metodu otključavanja uređaja koja se dešava gotovo trenutno (zavisi od kvaliteta, brenda, serije i cijene uređaja).

Za zaštitu svog email računa, takođe treba koristiti složeniju šifru. Međutim, najbolji način zaštite šifre je takozvani 2FA (two factor authentication) to jeste dva faktora autentifikacije. To u prijevodu znači da kada želimo da pristupimo svojoj elektronskoj pošti navodi se šifra i poduzima se barem još jedan korak kao što je na primjer odgovor na neko sigurnosno pitanje koji odgovor samo mi znamo, na primjer ime naše drugarice iz školske klupe i slično (ovo se pokazalo nepouzdanim jer osoba koja nas dovoljno dobro poznaje može ostvariti pristup).

Ukoliko imamo gmail račun, da bismo pristupili istom, nakon unesene šifre, na naš mobilni telefon (koji smo prethodno povezali sa gmail računom) će stići sms poruka sa kodom koji je neophodno unijeti za nastavak pristupu email-u. Na taj način će se smanjiti mogućnost neovlaštenog upada u naš

Email račun, jer se pretpostavlja da samo mi imamo pristup našem telefonu i kodu koji nam je poslan putem sms poruke. Tako da, ukoliko se želimo logirati sa nekog novog uređaja, obavezno uz sebe moramo imati mobilni telefon. (Mitnick, 2018)

4. VPN ZAŠTITA (VIRTUAL PRIVATE NETWORK)

VPN (skraćenica od engleskog “Virtual Private Network”) je mrežna tehnologija koja preko javne mreže (npr. Internet) ili privatne mreže u vlasništvu pružatelja usluge izrađuje sigurnu vezu. VPN tehnologiju za zaštićeno i daljinsko spajanje na privatne mreže upotrebljavaju razne vrste organizacija i pojedinaca, od velikih kompanija pa do državnih agencija.

Na internetu su dostupne desetine pružatelja VPN usluga kod kojih se možemo spojiti na provajder za mjesečnu naknadu od samo 5-10 $ kako bismo osigurali svoje lične podatke i online aktivnosti. Osim toga, većina operativnih sistema ima integrisanu podršku za VPN-ove, a također postoje i besplatni VPN-ovi (i/ili besplatne verzije komercijalnih VPN-ova. Između lažnih WiFi mreža, hakiranja preko interneta i napada raznim vrstama prevara – javne mreže su postale opasno i varljivo mjesto za prosječnog korisnika. Iako je VPN tehnologija prvobitno osmišljena kako bi omogućila zaposlenicima korporacija da se sigurno spoje na mreže svojih radnih mjesta kada nisu u uredu, VPN veze se sada koriste najviše za skrivanje internet aktivnosti, pružajući time privatnost i zaobilaženje cenzure, izbjegavanje hakera na javnim Wi-Fi mežama te za varanje web stranica da korisnik dolazi s neke druge lokacije kako bi se izbjegla ograničenja korisnika iz određenih država ili regija. No, VPN servisi nisu legalni u svim državama svijeta.

Princip rada VPN-a

Isto kao što *firewall* štiti podatke na našem računaru, VPN štiti naše podatke online. Iako je VPN tehnički mreža širokog područja (WAN), ulaz u njega nudi isti nivo sigurnosti, izgled i funkcionalnost kao i privatna mreža. VPN-ovi mogu biti ili daljinskog pristupa ili od mjesta do mjesta.

Kada surfamo bez VPN-a, zapravo se spajamo na provajder svog pružatelja pristupa internetu (ISP-a), a koji nas zatim spaja s web stranicom koju želimo. To znači da sva internetska aktivnost prolazi kroz njegove provajdere i ISP je može pratiti.

Prilikom surfanja putem VPN-a naš promet prolazi kroz VPN provajder koristeći šifrirani “tunel”. To znači da niko nema pristup njemu osim nas i provajdera VPN-a. Svejedno, postoji i razlika između privatnosti i anonimnosti. Upotreba VPN-a nas ne čini anonimnima zato što naš pružatelj

VPN usluge zna ko smo i može vidjeti našu online aktivnost. Ipak, to štiti našu privatnost od našeg ISP-a, škole, fakulteta i čak i naše vlade. Kako bismo potvrdili da je pružatelj VPN usluge uistinu zaštitio našu privatnost, veoma je važno odabrati pružatelja koji ne bilježi podatke. Ako pružatelj VPN usluge zadržava podatke u upotrebi, vlasti ih uvijek mogu tražiti, pregledavati ili ih pregledati na silu, što znači da naši podaci više neće biti privatni.

Treba imati na umu da čak i ako se naš pružatelj obveže da neće bilježiti bilo kakve podatke, i dalje može pratiti našu online aktivnost u stvarnom vremenu kada to bude potrebno, npr. zbog tehničkih razloga poput rješavanja problema. Iako većina pružatelja VPN usluga s tom politikom također obećava da neće pratiti ni našu aktivnost u stvarnom vremenu, u većini država je legalno da organi vlasti prisile pružatelja VPN usluga da počne čuvati podatke o upotrebi pojedinačnog korisnika bez obavijesti korisniku. Ipak, ako nismo u bijegu od vlasti zbog ilegalnih online aktivnosti, vjerovatno nemamo nikakvog razloga za brigu.

Osim odabira pružatelja VPN usluga koji ne bilježi nikakve podatke, vjerovatno želimo osigurati i da pružatelj kojega ste odabrali koristi dijeljene IP adrese, što znači da puno istih korisnika upotrebljava istu IP adresu. To trećoj strani drastično otežava zadatak pripisivanja neke uočene online aktivnosti baš nama.

5. KO SVE MOŽE PRISTUPITI E-MAIL POŠTI

Vjerovatno ste do sada primijetili da se u gornjem desnom uglu našeg e mail računa nalaze neke reklame. Te reklame nisu slučajne. One su bazirane na našoj prethodnoj e mail korespodenciji. To znači da, ukoliko smo sa nekim razmijenili poruku da npr. putujete u neku zemlju ili grad, počet će vam stizati reklame hotela iz te zemlje ili grada, booking ponude, ponude avio kompanija i sl, ili ste pomenuli neki kozmetički tretman koji želimo uraditi, stizat će vam reklame raznih kozmetičkih salona, preparata za uljepšavanje i slično. To znači da naša korespodencija nije sigurna, da uvijek postoji neko ko može pročitati našu poštu. Sva elektronska komunikacija se odvija preko servera te se prilikom tranzita poruke sa računa na račun, ključne riječi skeniraju te na osnovu toga i baziraju reklame koje vam se pojavljuju u desnom uglu poštanskog prozora.

Ovakva praksa nije ograničena samo na našu privatnu elektronsku poštu. Ukoliko pošaljemo elektronsku poštu putem poslovne mreže, telekomunikacioni odjel naše kompanije također može pregledati i pohranjivati našu komunikaciju. Odluka je na telekomunikacinom odjelu naše kompanije ili njihovih nadređenih, da li će dopustiti označenoj elektronskoj pošti da prođe kroz njihove servere i mreže, ili da uključe

agencije za provedbu zakona. Naime, razlog za ovakav vid praćenja može biti zaštita elektronske pošte koja sadrži poslovne tajne ili neki drugi sporan sadržaj. Ova praksa također uključuje i pregledanje pošte u cilju otkrivanja štetnog sadržaja. Ukoliko uposlenici našeg telekomunikacionog odjela pregledaju i arhiviraju našu elektronsku poštu, trebali bi nas o tome obavijestiti svaki puta kada to urade, iako većina kompanija to ne čini. Dakle, svaki puta kada pišemo elektronsku poruku, čak i ako poruku izbrišemo iz dolaznog sadučića, važno je imati na umu da postoji šansa da će kopija tih riječi i slika bti skenirana i postojat će, možda ne zauvijek, ali sigurno duži period na serveru. Neke kompanije imaju politiku kratkog pohranjivanja, ali sigurnije je zaključiti da većina kompanija čuvaju elektronske pošiljke duži vremenski period. Sada kada znamo da i naš poslodavac možda čita našu elektronsku poštu, najmanje što možemo uraditi je da mu taj posao otežamo. Svaki puta kada se konektuje,o na internet, pojavljuje se IP adresa (Internet protocol adress) te konekcije. Ovo može predstavljati problem ukoliko želimo biti nevidljivi na mreži: možemo promijeniti ime (ili ne dati taj podatak uopšte), ali naša IP adresa i dalje otkriva gdje se tačno nalazimo u svijetu, kojeg pružaoca internet usluga koristimo kao i identitet osobe koja plaća račune internet usluge (koja može ali i ne mora biti mi). Svi dijelovi ovih informacija uključeni su u metapodatke elektronske pošiljke i kasnije mogu biti korišteni za našu identifikaciju. Bilo koja komunikacija, bilo elektronska ili ne, može biti korištena za našu identifikaciju putem adrese Internog Protokola (IP) koja je dodijeljena našem ruteru, bilo da smo kod kuće, na poslu ili kod prijatelja. Međutim, IP adrese u elektronskoj pošti mogu biti krivotvorene. Neko može koristiti proxy odnosno zamjensku adresu- ne njegovu stvarnu IP adresu nego tuđu, tako da elektronska pošta izgleda kao da je došla sa druge lokacije. Cilj korištenja proxy je da se izbjegne odavanje stvarne IP adrese pošiljaoca elektronske pošte, tako što će neko naprimjer koristiti proxy iz Njemačke kako bi spriječio otkrivanje informacije da elektronska pošta zapravo dolazi iz Francuske. Da bismo sakrili našu IP adresu i na taj način ostali anonimni možemo koristiti uslugu anonimnih email servisa kao što su Anonymous Email – TorGuard, GuerrilaMail, Secure Mail, The Anonymous Email. Ova usluga jednostavno mijenja elektronske adrese pošiljaoca prije nego što pošalje poruku namjeravanom primaocu. Svrha ovakvih servisa je, kako oni navode, "borba za privatnost i odbrana od napada na privatnost". Drugi način da sakrijemo našu IP adresu je da koristimo Tor ruter. Tor je razvijen u Američkom mornaričkom istraživačkom laboratoriju 2004. godine kao način da vojno osoblje provodi istraživanja bez otkrivanja njihove fizičke lokacije, poslije čega je Tor program doživio ekspanziju na način da ga svako može koristiti. Tor je osmišljen za upotrebu od strane osoba koje žive u strogim režimima i kao način izbjegavanja cenzure popularnih medija

i usluga, kao i za prevenciju praćenja koji sadržaj pretražujete.Tor je i dalje besplatan i može gakoristiti bilo ko i bilo kada. (Mitnick, William, 2011).

Princip rada Tor-a

Nakon što instaliramo Tor na svom elektroničkom uređaju pokreće se uobičajeni način pristupa web stranici. Obično kada smo na mreži, otvaramo Internet pretraživač i ukucavamo ime stranice koju želimo posjetiti.

Kada koristimo Tor, direktna linija između nas i našeg cilja odnosno stranice koju posjećujemo je prikrivena dodatnim čvorovima i svakih nekoliko sekundi lanac čvorova koji nas povezuje sa bilo kojom stranicom, mijenja se bez da mi to i primjetimo. Varijacije čvorova koje nas povezuju sa stranicom su kao slojevi. Drugim riječima, ukoliko neko pokuša da nas nađe putem stranice koju smo gledali neće uspjeti jer se put konstantno mijenja. Ukoliko se naša tačka ulaska i izlaska ne povežu, naša konekcija smatra se anonimnom. Kada koristimo Tor, naš zahtjev za otvaranje stranice, nije poslan direktno serveru željene stranice nego drugom Tor čvoru. I da bi stvari bile još komplikovanije, taj čvoj prosljeđuje zahtjev drugom čvoru koji nas povezuje sa željenom stranicom. Dakle postoji ulazni čvor i izlazni čvor. Ukoliko tražimo nekoga ko je posjećivao našu web stranicu, samo bih mogao vidjeti IP adresu i informacije iz izlaznog čvora koji je posljedni u lancu, ali ne i prvi ulazni čvor. Tor se može podesiti da koristi izlazne čvorove određene države.

Da bismo koristili Tor, potreban nam je modifikovan Firefox pretraživač sa ToR stranice (www.torproject.org). Potrebno je uvijek tražiti legitimni Tor pretraživač za naš operativni sistem sa Tor web stranice. Za android operativne sisteme Orbot je legitimna besplatna Tor aplikacija sa Google Play-a koja djeluje dvostrano – šifrira naš promet i zamračuje našu IP adresu. Na iOS operativnim sistemima (iPad, iPhone), Onion browser je legitimna aplikacija sa iTunes prodavnice.

Kada znamo da je Tor siguran web pretraživač, iako nema i vlastiti server za elektronsku poštu?! Tor je posjedovao server za elektronsku poštu putem kojeg se odvijala email korespodencija, međutim, agencije za sprovedbu zakona su zaplijenili taj server te na taj način pristupili svim šifriranim elektronskim porukama pohranjenim u Tor pošti. Iz ovoga možemo zaključiti, da nikada ne možemo biti apsolutno zaštićeni u digitalnom svijetu. Iako Tor koristi posebnu mrežu pomoću koje možemo pristupiti interentu, pretraživanje je dosta sporije u odnosu na klasični način. Međutim, pored mogućnosti da surfamo internetom, na Toru možemo pronaći stranice koje inače nije moguće pronaći – nazivaju se Dark Web (tamna mreža). Neke od ovih sakrivenih stranica često nude prodaju predmeta i usluge koje mogu biti nezakonite. Potrebno je istaći međutim, da

Tor ima nekoliko slabosti: nemamo kontrolu nad izlaznim čvorovima koji mogu biti pod kontrolom vlade ili agencija za provedbu zakona, i dalje možemo biti otkriveni, Tor je jako spor. Obzirom na navedeno, ukoliko i dalje odlučimo da koristimo Tor, ne bismo trebali da ga pokrenemo sa istog uređaja koji koristimo za surfanje. Drugim riječima, koristite laptop za surfanje internetom, a sasvim drugi uređaj za Tor iz razloga ukoliko bi neko kompromitovao naš laptop, ne može otkriti Tor koji koritite sa drugog uređaja.

Ovo je važno znati kako bismo sačuvali naš nalog anonimnim i kako naša IP adresa ne bi bila povezana sa Torom. (Mitnick, William, 2002).

6. ZAŠTITA PRIVATNOG/ OBIČNOG KORISNIKA SMARTFONA

Pametni telefoni su toliko postali sastavni dio našeg svakodnevnog funkcionisanja da ne čudi i veliko interesovanje cyber kriminalaca za njih. Treba imati na umu da svaki pametni telefon predstavlja zaseban kompjuter, koji se također može koristiti kao server. Da bi bili na korak ispred hakera i cyber kriminalaca, korisnici treba da vode računa da je operativni sistem njihovih telefona ažuriran i da sve sigurnosne zakrpe preuzimaju odmah nakon što ih proizvođači objave. Za one kojima je potrebna dodatna sigurnost, vrijedi razmišljati i o korištenju dodatne zaštite. Virtualne privatne mreže (Virtual Private Networks) dobar su način da se uređaji zaštite i osiguraju da informacije o bankarskim transakcijama, kreditnim karticama i drugim privatnim podacima ne stignu u krive ruke zbog toga što se telefon koristi preko neosiguranih WiFi mreža i nepouzdanih internet servera. (www.kaspersky.com)

7. SAVJETI GRAĐANIMA PRILIKOM DAVANJA LIČNIH PODATAKA NA INTERNETU

Krađa podataka i identiteta su izuzetno uobičajeni događaji, pa je prvi i glavni savjet odgovorno ponašanje i briga o čuvanju privatnosti ličnih podataka. Nikako ne treba olako davati lične podatke, posebno ne na internetu jer su načini na koje naši podaci mogu biti zloupotrijebljeni gotovo zastrašujući. Posljedice mogu biti ne samo gubitak novca, ili narušavanje ličnog ugleda i reputacije, već se osoba kojoj su ukradeni lični podaci ukradeni može naći odgovornom za dugove koje je neko drugi napravio, ili čak za prestup ili kriminalno djelo prilikom čijeg vršenja je korišten njen identitet. Pored toga, treba stalno voditi računa kako se ponašamo na internetu - nikada ne treba koristiti istu lozinku za nekoliko web lokacija ili usluga. Postoje brojni programi koji pomažu kreiranje jakih lozinki i

omogućavaju jednostavno upravljanje njima.

Finalno, da bi bili sigurni od phishinga, uvijek provjerite internet adresu stranice koja vam traži podatke ili e- mail adresu pošiljaoca, prije nego što kliknete na bilo šta. (www.kaspersky.com)

8. OPASNOSTI KOJE POSTOJE U 2019., A KOJE NISMO IMALI U 2018. GODINI

Tokom 2018. godine, gledano u brojkama, više od 30 posto personalnih računara bilo je izloženo najmanje jednom napadu zlućudnim softverom koji je na njih došao s Interneta. Prema našim podacima, 765. 538 računara prošle godine je napadnuto enkriptorima, a čak 5.638.828 ličnih računara bilo je žrtva softverskih alata koji služe za rudarenje kriptovaluta. Rješenja kompanije Kaspersky blokirala su zlućudan softver kojem je svrha bila krađa novca putem aplikacija za online banking na čak 830.135 uređaja.

Ove godine, nastavio se trend napada na aplikacije za online banking, i vrtoglavo raste. Kako smo i očekivali, ovu godinu obilježila je značajna promjena u formatu prijetnji Zločinci u posljednje vrijeme sve više eksperimentiraju s novim, sofisticiranim metodama napada, koje je puno teže otkriti. Usmjerili su se na osnovniju infrastrukturu, traže i iskorištavaju ranjivosti u mrežnom hardveru, senzorima i drugim uređajima koji se temelje na tehnologijama Interneta stvari. Cyber kriminalci stalno potvrđuju svoju domišljatosti i kreativnost kada su u pitanju napadi, nalazeći nove i sve opasnije načine da se domognu naših podataka i imovine, pa je zato veoma važno kako da softverski osiguramo svoje uređaje pouzdanim rješenjem, tako i da prilagodimo svoje ponašanje i vodimo računa da se ne dovedemo u situaciju u kojoj bi neko mogao da zloupotrijebi našu otvorenost. Oprez i svijest o opasnostima su uvijek najbolji recept za sigurnost. (www.kaspersky.com)

9. NAJČEŠĆA SIGURNOSNA PITANJA U PODIZANJU NIVOA SIGURNOSTI IT SISTEMA U KOMPANIJAMA

Većina kompanija danas prolazi kroz proces takozvane “digitalne transformacije“ tj. integracije digitalne tehnologije u sve oblasti poslovanja. To temeljno mijenja način na koji posluju, komuniciraju i sarađuju sa svojim korisnicima, partnerima, ali i sopstvenim zaposlenima.

Izdvojeni finansijski budžet potreban za ovaj proces se nekako nađe i pokrije, ono što zabrinjava je nedovoljan broj stručnjaka za cyber sigurnost. Čak 48 posto firmi su ukazale na nedostatak stručnjaka u ovoj oblasti. To znači da ovaj proces često povećava izloženost kompanije raznim sigurnosnim izazovima i rizicima, koje ne treba zanemariti.

Pri tome, hakeri koji pronalaze neku hardversku ili softversku slabost IT sistema koji kompanija koristi, samo su jedan dio problema. Izazovi po sigurnost mnogo češće dolaze zbog ljudskog faktora: neoprezni ili nedovoljno obučeni/trenirani zaposlenici; neažurirani programi; neadekvatno određena ograničenja pristupa osjetljivim podacima ili neadekvatna zaštita endpoint uređaja u kompanijama. Redovni treninzi svih zaposlenih koji dolaze u kontakt sa tim sistemima, bez obzira na funkciju koju obavljaju, i podizanje svijesti o rizičnom ponašanju postaju neophodni u organizacijama svih veličina. Naravno, neophodno je eliminisati i mogućnost neautorizovanog pristupa postavkama IT sistema, a to se može postići samo primjenom adekvatnih, sveobuhvatnih rješenja za cyber-zaštitu i adekvatnim postavkama sigurnosti. Jedino tako se na najmanjoj mogućoj tački smanjuje mogućnost kompromitacije sigurnosti. (www.kaspersky.com)

10. ZAKLJUČAK

Svakim danom tehnologija napreduje i prevazilazi dosadašnje granice i tehnološke limite. U zadnjih 10 godina možemo svjedočiti ogromnom razvoju i ekspanziji tehnologije u oblasti računara, interneta i pametnih telefona koji danas u suštini džepni komjuteri. Preko 90% posto svjetske komunikacije na daljinu, se odvija preko elektročkih uređaja. Gotovo sve bankovne transakcije odvijaju se putem interneta preko moćnih servera. Svaki elektronički uređaj koji posjeduje procesor ili mikroprocesor i pri tome je povezan sa internetom ili uređajem koji je povezan na internet, može biti dostupan trećem licu odnosno stručnjaku u oblasti hakiranja. Hakiranje u suštini predstavlja ilegalni pristup uređajima, bankovnim računima, privatnim osobnim ili državnim podacima itd. Razvojem tehnologije uporedo je tekao razvoj i umjeće hakiranja.

Danas su cyber napadi sve češći jer je Svijet preplavljen elektrnočkim uređajima i težnjom ka digitalizaciji svega što je moguće digitalizirati, što hakerima daje mnoge mogućnosti i nove ideje za izvršenje ovog kriminala. Konstantno se vodi borba između hakera i ostatka svijeta u zaštiti informacija te se konstantno razvijaju novi sistemi i programski paketi koji bi nas zaštili od ilegalnih upada i napada hakera. Koliko brzo se širi razvoj cyber kriminala nam govori i podatak i se skoro svi programi koji služe za zažtitu od istog obnavljaju i po više puta na dnevnoj bazi.

LITERATURA

1. Mitnick, K., 2018. The Art of Invisibility. Hachette Book Group USA
2. Mitnick, K., William, L. S., 2011. Ghost in the Wires. Sorward by Steve Wozniak.

11. Mitnick, K., William, L. S., 2002. The Art od Deception. Sorward by Steve Wozniak.
12. https://www.kaspersky.com/

PRILOG

U prilogu su dati neki od statističkih podataka za cyber kriminal.