UNIVERZITET U SARAJEVU

FAKULTET POLITIČKIH NAUKA

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

CYBER PRIJETNJA U KONTEKSTU OSTALIH SIGURNOSNIH RIZIKA I IZAZOVA

-magistarski rad-

Kandidat:

Nedžad Borčilo

Mentor:

Prof.dr. Selmo Cikotić

Sarajevo, 2023. godine.

FAKULTET POLITIČKIH NAUKA
UNIVERZITET U SARAJEVU
MCMXLIX

ODSJEK SIGURNOSNE I MIROVNE STUDIJE

CYBER PRIJETNJA U KONTEKSTU OSTALIH SIGURNOSNIH RIZIKA I IZAZOVA

-magistarski rad-

Kandidat:

Nedžad Borčilo

Mentor:

Prof.dr. Selmo Cikotić

Sarajevo, 2023. godine.

S A D R Ž A J

UVOD

Svijet je postao globalizirani fenomen. Događaji na jednom kraju svijeta utječu na drugi zahvaljujući tehnološkom razvoju i postojanju mreže, odnosno Interneta. Internet je postao sredstvo za prenošenje informacija broj jedan. Teško da postoji osoba na svijetu koja ne koristi Internet za istraživanje, razmjenu poruka i mnoge druge svrhe. Sama upotreba Interneta predstavlja rizik za zaštitu ličnih podataka, jer je već svima jasno da sve što ukucamo u pretraživač ili sve što objavimo ostavlja svoj digitalni trag zauvijek. Internet je, kako je nekada bio, vrlo koristan, postepeno zloupotrebljavan. Kibernetički rizik je svugdje i svi smo mi potencijalni ciljevi.

Naglašavamo da svaka nacionalna država ima svoj sistem nacionalne sigurnosti, ona je organizirana prema potrebama svoje države, svaka nacionalna država ima svoje povjerljive podatke, podatke o svojim građanima i drugima. Sve nacionalne države moraju i trebaju voditi brigu o zaštiti ovih podataka kako ne bi došli u pogrešne "ruke" i ne bi bili zloupotrijebljeni. Ali u kojoj je mjeri ovaj sistem funkcionalan, jedno je od ključnih pitanja u ovom članku.

Predmet istraživanja je upoznavanje sa dostignućima i efektima rada državnih policijskih organa FUP, SIPA, MUP, MS, MO i Ministarstvo saobraćaja i komunikacija. U studiji se govori o načinima na koje ove službe rade, o njihovim dobrim i uspješnim, ali i o lošim ili loše provedenim aktivnostima na polju prevencije i represije na polju cyber napada i prijetnji. Unutar određenog predmeta istraživanja potrebno je objasniti tipični model predmeta istraživanja koji se sastoji od nekoliko faktora: prirodnih i socijalnih uslova, predmeta - tema, interesa i ciljeva, zatim djelovanja društvenih aktera, metoda, načina i sredstava djelovanja , skup rezultata i radnji. Osnova pristupa razvoju standardnog modela predmeta istraživanja je da je predmet istraživanja svih društvenih nauka društvo sa različitih aspekata, a problem kibernetičke sigurnosti i problem nefunkcionalnog sistema kibernetičke sigurnosti veliki deficit, za stanovništvo, vladine agencije, bankarske sisteme i društvo u cjelini.

Strateški cilj Bosne i Hercegovine je ulazak u EU kroz pristupne pregovore, te je cilj da se postane punopravni član. Broj povezanih uređaja je eksponencijalno rastao, kao i broj aktivnih korisnika interneta i ovo označava pozitivan razvoj u bosanskohercegovačkom društvu. Cyber prostor nudi mnoge mogućnosti kao što su pružiti pomoć rastućim ekonomijama i građanima, pomoći u zatvaranju jaza između bogatih i siromašnih, razvoj

sposobnosti neophodnih za zaštitu, uzimajući u obzir izloženost i rastuće prijetnje u mreži. Međutim, kako se navodi u izvještaju Evropske komisije o napretku Bosne i Hercegovine, još 2016: „Bosna i Hercegovina nema sveobuhvatan strateški pristup problemu prijetnje u oblasti cyber kriminala i cyber sigurnosti, prijetnje kibernetičke sigurnosti, postojeće sposobnosti i sposobnosti za borbu protiv kibernetičkog kriminala, te timove koji sprečavaju i štite cyber incidente i sigurnosne prijetnje javnim informacionim sistemima (CERT/CSIRT)“. Postojeće ljudske i materijalne sposobnosti i organizacione sposobnosti nisu dovoljne da obezbjede potreban nivo sigurnosti u cyber prostoru Bosne i Hercegovine. Različiti nivoi vlasti imaju različit stepen pripravnosti, koji vodi do toga da je neujednačen rezultat koji se odnosi na nivo zaštite korisnika u javnom i privatnom sektoru. Sve ovo podriva ukupni nivo zaštite u cyber prostoru, ranjivost na prijetnje i napade i nekompetentnost za pravovremeno djelovanje, saradnju i koordinaciju sa ostatkom regiona i svijeta.

I. METODOLOŠKI OKVIR RADA

1. Problem istraživanja

Pravne norme, koje se odnose na aspekte zaštite kompjuterskih sistema, se moraju fokusirati na ovlasti i odgovornosti zemalja domaćina – provajdera, internet usluga, za nadzor sadržaja i usluga, a potom i ovlasti za reagovanje i sankcionisanje. Ovaj napor je najveći pravni izazov međunarodne zajednice, a ujedno i najveći doprinos borbi protiv terorizma na globalnom nivou – posebno s obzirom na terorističke zloupotrebe interneta koji su danas globalnih razmjera.

Internet kao informaciona mreža omogućava dvosmjernu komunikaciju i predstavlja nivo korišćenja informacione infrastrukture u ofanzivne svrhe srazmjerno nivou izloženosti terorističkih organizacija napadima protivterorističkih snaga. Može se očekivati da terorističke organizacije često ne uspijevaju postići prednost vođenu faktorima iznenađenja, ali ovu taktiku možemo prilagoditi i primijeniti u antiterorističkoj strategiji.

2. Predmet istraživanja

Postojeće znanje o ovom predmetu uključuje znanje empirijske i teorijske prirode, tj. ono je hipotetičke prirode. Dakle, postoje naučna saznanja koja su zabilježena, ali kao takva nisu provjerena. Cilj stranih entiteta je pomoći nacionalnim vladinim strukturama da stvore jedinstvenu agenciju koja će se baviti zaštitom svih vrsta institucionalnih podataka na mrežama, odnosno internetu. Kao jedinstvena država i kao zemlja kandidat za članstvo u EU, Bosna i Hercegovina mora ispuniti zadatak koji je EU postavila na polju sigurnosti cyber prostora, biti svjesna sigurnosne transformacije i globalizacije sigurnosnih prijetnji, te tako razviti novi sigurnosni sistem koja će sada uključivati cyber sobu. Policijske službe i druge vladine agencije takođe trebaju uložiti više napora i resursa u računarske stručnjake kako bi postigli najviši mogući nivo državne zaštite podataka i omogućili državi da se brani od cyber prijetnji. Važno je utvrditi nedostatke u pravilima i ispraviti ih ili opravdati novim izmjenama.

2.1. Kategorijalno pojmovni aparat

Cyber prijetnja

Cyber prijetnjom se smatra svaka prijetnja koja je usmjerena putem online infrastrukture a koja može imati dalekosežne posljedice na cjelokupno društvo, odnosno državu. Cyber prijetnje se još smatraju i novim načinima prijetnji, odnosno modernim prijetnjama koje su sve više zastupljene ogromnim rastom online infrastrukture.[1]

Cyber sigurnost

Cyber sigurnost je specifična vrsta informacione sigurnosti koja se odnosi na način na koji organizacije štite digitalne informacije, kao što su mreže, programi, uređaji, serveri i drugi digitalni podaci. Iako je ovo samo jedan aspekt informacione sigurnosti, njemu se posvećuje najviše pažnje jer su sajber prijetnje zastupljenije od fizičkih prijetnji.[2]

E-commerce

Kako se danas sve više ljudi odlučuje koristiti internet za kupovinu koja je otvorena mogućnost krađe podataka o računu. Preporučljivo je da kupujete online samo preko sajtova koji nude pravu zaštita i sigurnost. Nikada ne kupujte robu na mreži ostavljajući svoj kreditni broj karticu i njen datum isteka bez enkripcije (prilikom kupovine treba jasno vidjeti etiketu tzv. (slika katanca) što ukazuje da radi u sigurnoj vezi i da vaši podaci neće biti dostupni neovlašćenim licima. Ako kupujete online, redovno provjeravajte njihove račune.

Krađa identiteta

Krađa identiteta kroz zloupotrebu informacionih tehnologija je, sa širenjem upotrebe interneta, je postala jedna od najčešćih aktivnosti počinitelja. Upotreba informacija tehnologije, od strane korisnika koji nisu dovoljno svjesni opasnosti koje ih čekaju korištenje ličnih podataka koji čine njihov identitet na internetu, dovelo je do stvaranja velike količine ličnih podataka koji su lako dostupni počiniocima krivičnih djela, koji ih kasnije, po pravilu, zloupotrebljavaju.

[1] https://duplico.io/cyber-prijetnje-ranjivosti-i-rizici-razlike-i-definicije/ (5.3.2022.)
[2] https://duplico.io/informacijska-sigurnost-i-cyber-sigurnost/ (5.3.2022.)

Sigurnosne prijetnje u cyber kriminalu

Sigurnosne prijetnje podrazumijevaju proces, odnosno djelovanje, koje za cilj ima da se ugrozi sigurnost pojedinca, grupe, organizacije, države, te da im se oteža i/ili onemogući ostvarivanje strateških i drugih ciljeva, a sve to uz pomoć informacionih tehnologija.

Sigurnosne provjere

Cyber sigurnosne provjere predstavljaju proces pomoću kojega treba da se dobije uvid u tajne podatke, a provode ga organi koji imaju ovlasti da dođu do takvih podataka. Kao i svake druge provjere, sigurnosne provjere moraju imati zakonski osnov za provjeravanjem istih.

Visoko tehnički kriminal

Visokotehnološki kriminal obuhvata skup krivičnih djela gdje su kao predmet izvršenja i kao sredstva za izvršenje krivičnog djela su računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Ova definicija uključuje veliki broj zloupotreba informacionih tehnologija, kao i oblast zloupotreba u radio-difuznim tehnologijama. Tako se razlikuju krivična djela gdje se računari pojavljuju kao sredstvo izvršenja (Computer Related Crime) i kao objekat izvršenja (Computer Crime), kao i krivična djela u čijem se načinu izvršenja pojavljuju elementi nezakonitog korištenja interneta.[3] Broj i vrste krivičnih djela iz oblasti visokotehnološkog kriminala, kao i ekonomska šteta koja je rezultat izvršenja ovih zločina, veoma je teško procijeniti. Međutim, broj počinjenih krivičnih djela i privredna šteta koja je do sada registrovana iz godine u godinu se konstantno povećava.

Zaštita podataka

U cilju zaštite podataka od neovlaštenog pristupa, preporučuje se korištenje tzv. BIOS-a, lozinka i lozinka screensaver. Ako imate povjerljive informacije na svom računaru, postoje i metoda šifriranja cijelog tvrdog diska u realnom vremenu (ovi podaci će uvijek biti pohranjeni na disk kao šifrirani). Najsigurniji način zaštite podataka od neovlaštenih osoba je osigurati da te osobe ne čine pristup vašem računaru. Međutim, ako podatke šaljete putem e-pošte, ne možete biti potpuno sigurni da će samo osoba kojoj su upućeni imati pristup ovim podacima. U ovim u nekim slučajevima se preporučuje korištenje enkripcije. Jedan od najpoznatijih kriptografskih programa je Pretty Good to Privac, poznatiji kao PGP, ali postoji mnogo

[3] http://mup.ks.gov.ba/sites/mup.ks.gov.ba/files/zastitimo_se_od_cyber_kriminala1_1.pdf (Pristupljeno 53.2022.)

sličnih programa koje možete pronađeno na internetu. Uz pomoć ovih programa moguće je obezbijediti e-poštu, hard disk, folder sa podacima, pa čak i jedan Word dokument.

Zlonamjerni softver

Zlonamjerni softver je vrsta softvera dizajnirana da se infiltrira u kompjuterski sistem, bez informacija i saglasnosti njegovog vlasnika. Ovo je opšti pojam koji koriste stručnjaci za opisivanje različitih oblika neprijateljskog, nametljivog ili dosadnog softvera ili programski kod. Termin "računarski virus" je pojam koji obuhvata sve vrste zlonamjernog softvera. Odluku o tome da li će se softver smatrati zlonamjernim, tj. zlonamjeran, zasnovan je na njegovoj namjeri kreatora, a ne na njegove funkcije.

Ova grupa uključuje:

• kompjuterski virusi

• crvi

• Trojanci

• špijunski softver

• modificirani softver za oglašavanje (nepošteni reklamni softver)

• softver kreiran za potrebe visokotehnološkog kriminala, kao što je pristup na mreži računi (crimeware)

• softver kreiran za dobijanje administratorskog pristupa sistemu (rootkit), kao i drugi zlonamjernog i neželjenog softvera.

3. Sistem hipoteza

3.1. Generalna hipoteza

Bez cjelovitog i funkcionalnog odgovora na cyber prijetnje sistem sigurnosti moderne države ne može dati potpuni odgovor ni na mnoštvo drugih sigurnosnih prijetnji.

3.2. Posebne- pojedinačne hipoteze

Ph.1. Uvoditi cyber sigurnost kao obavezan program obuke uposlenika operatora ključnih usluga i baza podataka od kritičnog značaja, kao i uposlenika institucija javne uprave.

Cyber sigurnost se neće unaprijeđivati ukoliko se ne institucionalizira kao obavezan sadržaj obuke svih pripadnika sistema sigurnosti koji imaju dodira sa mrežama i napravama konektovanim na mrežu.

Ph. 2. Cyber sigurnost se može eventualno izgrađivati i realizirati u okviru procesa obrazovanja, medija, društvenih mreža i drugih formi obrazovanja i obuke.

Ph. 3. Ažurno informisanje donosioca odluka o cyber sigurnosti o svim relevantnim informacijama podiže nivo funkcioniranja ukupnog sistema sigurnosti.

4. Način istraživanja

Metode istraživanja

U ovom radu su korištene sljedeće metode:

- istraživanja,
- analiza,
- apstrakcija,
- dedukcija,
- indukcija,
- sinteza,

- opis,
- uporedne i povijesne metode i metode predviđanja.

Ciljevi istraživanja

Ciljevi istraživanja u radu su naučnog i društvenog karaktera.

Naučni cilj će u mnogome doprinijeti cjelokupnom sektoru sigurnosti kroz svoje pojašnjavanje i definisanje pojma cyber sigurnost kako sa teorijskog, tako i sa svih praktičnih staništa cyber prostora i jačanja sigurnosti u njemu.

Društveni cilj ovog istraživanja je usmjeren na namjeru da se podigne opšta svijest svih pripadnika sistema sigurnosti, ali i svih drugih korisnika interneta u državnim institucijama i društvenoj zajednici, o potencijalnim cyber prijetnjama koje su prisutne na mrežama i o mogućim metodama, namjerama i postupcima zaštite od njih.

Vremensko određenje odnosi se na period od samog nastanka cyber prijetnji do danas.

GLAVA I

INFORMACIJSKA TEHNOLOGIJA

Komunikacione i informacione tehnologije su oblast nauke i tehnologije koja obuhvata proučavanje komunikacionih i informacionih tehnologija i sistema i njihove primjene u svim oblastima ljudskog života i djelatnosti.[4] Kao i drugi tehnički smjerovi, komunikacijska i informatička tehnologija povezuje matematiku, fiziku i druge prirodne nauke s jedne strane, te praktične rezultate s druge strane. Možemo reći da je područje komunikacionih i informacionih tehnologija danas toliko široko i interdisciplinarno da je veoma malo ljudskih aktivnosti u koje nisu prodrle komunikacijske i informatičke tehnologije i značajno doprinijele njihovom razvoju.

Rastuća potražnja za efikasnim komunikacionim i informacionim sistemima u razvijenim društvima zahtijeva kontinuirani razvoj novih metoda i tehnologija za prijenos, obradu, skladištenje i zaštitu informacija. Kontinuirani brzi razvoj, kontinuirano usavršavanje, nova znanja i ostvarena postignuća nužno zahtijevaju odgovarajući obrazovni proces.

Danas je oblast komunikacija i informacionih tehnologija toliko široka i interdisciplinarna, da je malo ljudskih aktivnosti koje nisu obuhvatile komunikacijske i informatičke tehnologije, te značajno doprinijele njihovom razvoju.[5] Jedna od karakteristika komunikacijske i informacione tehnologije je da se ona veoma brzo razvija. Razvoj mikroelektronike i kompjuterske tehnologije omogućio je razvoj u oblasti informacionih i telekomunikacionih tehnologija, te tako postao jedan od najperspektivnijih djelatnosti u privredi.[6]

Prijenos informacija putem slike, zvuka ili podataka jedan je od najvažnijih preduslova za razvoj modernog društva. Tehnologije kao što su Internet, World Wide Web, e-trgovina, mobilne komunikacije i digitalna televizija ubrzano se razvijaju i integrišu radna i životna okruženja koja se stalno mijenjaju.[7]

[4] https://vpsle.edu.rs/wp-content/uploads/2018/01/INFORMACIONE-TEHNOLOGIJE.pdf
[5] https://repozitorij.efst.unist.hr/islandora/object/efst%3A2553/datastream/PDF/view
[6] http://www.lecad.unze.ba/nastava/INFORMATIKA/Info1 Informacione%20Tehnologije%20i%20Razvoj/Info1_1do2-Prezen.pdf
[7] Tiganj, Dž., Komunikativne mogućnosti starih i novih medija, Magistarski rad,

Internet mreže možemo posmatrati kao jedan fenomen koji se svakodnevno sve više širi i unaprijeđuje. Ove mreže su promijenile način na koji komuniciramo, naše dnevne aktivnosti, te na neki način možemo reći da su promijenile i svijet. Internet mreže se smatraju jednim vidom alata, te zbog toga možemo reći da mogu biti prijetnja.

Cyber prijetnje koje se mogu odnositi na pojedinca, institucije, firme, te čak i na nacionalnu sigurnost, a pri tome mogu izazvati negativne posljedice mogu nastati iz različitog korištenja društvenih mreža, koji su glavni alati razmjene informacija na internetu.

Negativne posljedice nastaju prilikom korištenja društvenih medija, a posebno kada se društvenim mrežama koriste osobe koje imaju doticaja s osjetljivim sigurnosnim informacijama. Podložnost cyber napadima preko društvenih mreža ovisi o tome na koji se način koristi društvenim mrežama, ko se njima koristi i zbog kojih razloga.

Kada napadači iskoriste ranjivosti u kodiranju kako bi dobili pristup poslužitelju ili bazi podataka, ove vrste prijetnji kibernetičkih napada poznate su kao napadi sloja aplikacije. Korisnici Interneta vjeruju da će osjetljivi i osobni podaci koje podijele na web-stranici biti sigurni i privatni. Napadi temeljeni na web-u mogu ugroziti privatne informacije kao što su korisnikova kreditna kartica, medicinske informacije, privatne slike i chat-ovi, što dovodi do potencijalno teških posljedica. Web aplikacije posebno su osjetljive na kibernetičke napade jer često zahtijevaju visoku razinu dostupnosti. Budući da te aplikacije moraju biti javno dostupne, ne mogu se zaštititi iza vatrozida. Mnoge aplikacije imaju pristup, bilo izravno ili neizravno, vrlo poželjnim podacima o kupcima. Napadač traži ranjivosti kako bi mogao ukrasti te informacije ili ih proslijediti.[8]

Mobilni uređaji kao rizik

Baš kao što broj mobilnih uređaja koje koristimo svakodnevno raste, tako raste i količina naših podataka pohranjenih na njima. Zbog toga u u budućnosti možemo očekivati rast broja hakerskih napada povezanih s korištenjem i zloupotrebom mobilnih uređaja. Veoma je bitno osigurati svaki uređaj koji se koristi, a jedan od načina za smanjenje ovog tipa rizika jeste omogućavanje pristupa putem osigurane web-aplikacijske infrastrukture koja cyber sigurnošću upravlja u stvarnom vremenu.

[8] Acunetix. What Is a Web Application Attack and how to Defend Against It. Preuzeto sa: https://www.acunetix.com/websitesecurity/web-application-attack

Napadi povezani s IoT uređajima

Svi znamo kako funkcioniše tržište, posebno kada je riječ o novim tehnologijama. Glavni cilj jeste da se u ovoj utrci najnovije tehnologije i proizvodi implementiraju što brže, dok se na sigurnost u tim momentima baš i ne misli. Zbog toga i ne čudi što je rastući trend interneta stvari, osim inovacija, donio i podosta sigurnosnih propusta, a nesigurna bežična komunikacija, nešifrirani lični podaci, neprovjerene nadogradnje upravljačkog softvera, ranjiv web-interfejs samo su neki od njih. Kompromitovani IoT uređaji, poput routera i NAS servera, mogu cyber kriminalcima omogućiti pristup komunikaciji i podacima, poslužiti kao ulazna tačka za dalje napade ili djelovati kao DDoS napadački dronovi. S druge strane, proizvodi za kućnu automatizaciju te nosivi uređaji mogu se iskoristiti za krađu ličnih i drugih podataka koji bi mogli biti korisni hakerima.[9]

Napadi temeljeni na informacijskom sistemu

Napade temeljene na sistemu možemo kategorizirati pod sintaksne napade (engl. syntactic attacks) koji koriste softver poput virusa kako bi ometao ili oštetio računalni sistem ili mrežu. Njegov cilj je napasti korisnike uzrokujući proizvodnju grešaka i nepredvidivih rezultata u računalnom sistemu. Sintaksni napadi ponekad se grupiraju pod pojmom zlonamjernih softvera ili malware. Ti napadi mogu uključivati viruse, crve (engl. worms) i trojanske konje. Jedan od čestih načina prijenosa takvih napada je e-pošta.[10]

Svakodnevno se bilježi porast cyber napada na kritične infrastrukture. Prethodno se smatralo da je rizik ovih napada na kritične infrastrukture nizak zbog potrebe za specijalističkim znanjem i zbog nepostojanja odgovarajućih internetskih veza. Međusobna povezanost mnogih digitalnih tehnologija i važnih ili kritičnih infrastrukturnih sustava dovela je do stvaranja novih ranjivosti s dalekosežnim posljedicama (Spremić, Šimunić, 2018) .

Kao što smo već rekli, živimo u vremenu velikih i čestih cyber napada, gdje napadači ne biraju institucije. Zbog sve veće količine podataka u optjecaju i svakodnevnog korištenja informacijske tehnologije, cyber napadi se događaju sve češće te su posljedice sve opasnije za institucije kao što su državne institucije, banke, bolnice, aerodromi i drugo podložne cyber napadima i prijetnjama. Cilj napada na ove institucije leži u tome da se napravi neki vid štete

[9] https://www.asadria.com/it-sigurnost-i-nadolazeci-trendovi-sta-mozemo-ocekivati-u-2020-godini/
[10] M. Bhardwaj, G.P. Singh. Types of Hacking Attack and their Counter Measure. 2011;1(1)

kao što je nedostupnost sistema, krađa podataka i slično, kako bi se omeo rad istih. Cyber napadi omogućuju napadaču da dobije pristup tajnim informacijama i sistemu institucija kako bi ostvario svoj cilj. Digitalizacijom i razvojem novih tehnologija povećala se vjerojatnost cyber napada u kritičnim infrastrukturama zbog korištenja informacijskih sustava. u. Brzina i način odgovora na cyber napade od ključne su važnosti za sve institucije. Cyber napadi na kritične infrastrukture institucija imaju loš utjecaj na samu instituciju i mogu izazvati velike posljedice i stoga je bitno posvetiti posebnu pažnju pronalasku rješenja za rizike kojima su one izložene. Zaštita svih institucija je veoma važna za čitavo društvo.

Cyber sigurnost

Cyber sigurnost je specifična vrsta informacione sigurnosti koja se odnosi na način na koji organizacije štite digitalne informacije, kao što su mreže, programi, uređaji, serveri i drugi digitalni podaci. Iako je ovo samo jedan aspekt informacione sigurnosti, njemu se posvećuje najviše pažnje jer su cyber prijetnje zastupljenije od fizičkih prijetnji. Zlonamjerni softver, hakiranje od strane kriminalaca i insajderske greške su među glavnim razlozima kršenja, i savršeno je logično dati prednost odbrani kako bi se ublažili ovi rizici. Ova aktivnost se može definisati kao zaštita računara, servera, mobilnih uređaja, elektronskih sistema, mreža i podataka od zlonamjernih napada koji ciljaju niz uređaja od pojedinaca do korporativnih organizacija. Ne može se reći da su cyber sigurnost i fizička sigurnost potpuno odvojene ili različite. Međutim, ako je laptop ukraden, na primjer, trebale bi postojati komplementarne mjere kibernetičke sigurnosti kako bi se zaštitila organizacija od dopuštanja da podaci i prava pristupa padnu u pogrešne ruke. Napadi su podijeljeni u različite kategorije kao što su: sigurnost mreže, sigurnost aplikacija, sigurnost informacija, operativna sigurnost i oporavak od katastrofe, imajući na umu kontinuitet poslovanja. Sigurnost mreže i aplikacija fokusira se na zaštitu računarskih mreža i softvera i uređaja od prijetnji i ranjivosti.[11]

Oporavak od katastrofe bavi se odgovorom organizacije na potencijalni gubitak i oporavak podataka i operativnom sposobnošću organizacije da nastavi sa normalnim radom nakon napada. Poznavanje definicije kibernetičke sigurnosti nije dovoljno bez detaljnijeg razumijevanja različitih vrsta napada. Napadi se mogu podijeliti u četiri logične cjeline, kao što su: cyber kriminal (fokusiran na ekonomsku dobit), cyber napad (prvenstveno politički) i

[11]Helmbrecht, U., Purser, S., Klæstrup, R., "Cyber Security: Future, challenges and opportunities". European network and information Security agency (eniSa), Heraklin, 2011.

cyber terorizam. Većina ovih napada se izvodi uz pomoć nekih medija, kao što su zlonamjerni softver uključujući viruse, špijunski softver, ransomware adware, botne, itd.

Napadi su poznati kao SQL injekcija, phishing, dos (uskraćivanje usluge) itd. Prema svim dostupnim izvještajima, cyber prijetnje su naglo porasle posljednjih godina i rastu iz dana u dan. Vlasnici preduzeća danas nemaju potrebno tehničko znanje i stručnost da zaštite svoje poslovanje od unutrašnjih i eksternih cyber pretnji. Ne samo velike kompanije, već i male kompanije su navodno ranjive na cyber napade. Kako kompanije postaju digitalne, prošla su vremena kada su se vlasnici preduzeća mogli obratiti IT odjelu svaki put kada se pojavi prijetnja, ovo je postalo poslovno pitanje, zbog čega bi kompanije trebale implementirati odgovarajuće sigurnosne protokole kako bi zaštitile svoje poslovanje od uzroka cyber prijetnji. Cyber bezbjednost je praksa zaštite povjerljivih informacija i podataka kompanije od neovlašćenog pristupa primenom više bezbjednosnih protokola. Cyber sigurnost se odnosi na zaštitu podataka i informacija od ovlaštenog elektronskog pristupa. Jednostavno rečeno, internet sigurnost štiti vaše vrijedne podatke u elektronskom obliku. To je podskup informacione sigurnosti koji se bavi sigurnošću vaše IT infrastrukture kako bi osigurao njenu konstatntu sigurnost. Mala preduzeća su ranjivija na cyber prijetnje jer potencijalni hakeri znaju da malim preduzećima nedostaju resursi jer su veće kompanije investirale u bezbjednosne tehnologije i strategije. Procedure i politike digitalne kibernetičke sigurnosti se brzo mijenjaju, tako da kompanije moraju biti u toku s najnovijim mjerama kibernetičke sigurnosti kako bi bolje zaštitile svoj cyber prostor od cyber prijetnji. Neki od najčešćih cyber napada uključuju phishing, kršenje podataka, mamce i još mnogo toga.[12]

1.1. Oružje kompjuterskog kriminala

Za razliku od ostalih oblika kriminaliteta, kompjuterski kriminal još uvijek ne predstavlja potpunu fenomenološku kategoriju, pa ga je nemoguće definirati jednom i preciznom konceptualnom definicijom. Kompjuterski kriminal je krivično djelo koje ima za cilj sigurnost informacionih (računarskih, kompjuterskih) sistema, traženje određene koristi za sebe ili druge, ili nanošenje određene štete drugima. Nadalje, prema nekim definicijama,

[12]Heijden, R., Dietzel, S., Leinmuller, T. i Kargl, F. (2019). Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. IEEE Communications Surveys & Tutorials 21(1).

kompjuterski kriminal je definiran kao zloupotreba kompjutera u smislu bilo kojeg događaja vezanog za korištenje kompjuterske tehnologije u kojem žrtva trpi ili može pretrpjeti gubitak, a počinitelj djeluje s ciljem sticanja prednosti.

Evropska konvencija o cyber kriminalu definiše četiri kategorije krivičnih djela: krivična djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema (nezakonit pristup, presretanje, ometanje podataka, korištenje opreme, programa), krivična djela povezana s računarom (falsifikovanje i krađa), zločini u vezi sa sadržajem (najčešće u obliku dječije pornografije, uključujući posjedovanje, distribuciju, prijenos, skladištenje ili stavljanje na raspolaganje takvih materijala), djela povezana s kršenjem autorskih prava. U tom smislu, cyber kriminal se može podijeliti na: politički (cyber špijunaža, hakovanje, cyber sabotaža, cyber terorizam, cyber ratovanje), ekonomski (cyber prevara, hakovanje, krađa internetskih usluga i vremena, piratski softver, mikročipovi i baze podataka, cyber industrijski špijunaža, lažne internet aukcije), proizvodnja i distribucija nelegalnog i štetnog sadržaja (dječija pornografija, pedofilija, vjerske sekte, širenje rasističkih i nacionalističkih ideja i stavova, zlostavljanje žena i djece, trgovina ljudskim organima, oružjem i drogama) i internet kršenja privatnosti (praćenje e-pošte, neželjena pošta, prisluškivanje i snimanje). Zlonamjerni softver je generički naziv za zlonamjerne programe koje cyber kriminalci koriste za pristup tuđim računarima. Takvi programi su često skriveni u prilozima ili besplatnim sadržajima. Koriste se za mnoge nezakonite radnje, kao što su krađa ličnih podataka, brisanje ili oštećenje podataka, kreiranje botneta (mreža zaraženih računara) i zaobilaženje sigurnosnih programa. Postoji mnogo različitih zlonamjernih programa, ovaj put ćemo se pozabaviti virusima, trojancima, špijunskim softverom, adwareom i scarewareom. Virus je reproducibilan program koji obično donosi zlonamjerne programe koji mogu oštetiti datoteke i programe na vašem računalu. Nadalje, virusi se koriste za praćenje svega što radite na svom računalu i omogućavaju neovlašteni i potencijalno štetan pristup vašem osobnom računalu. Većina korisnika interneta svjesna je opasnosti koje nose virusi i mogu biti zaštićeni raznim antivirusnim programima i zaštitnim zidovima. Međutim, ljudi koji stvaraju virus stalno pronalaze nove načine za širenje virusa na vaš računar. Stoga morate biti vrlo oprezni kada radite na internetu, preuzimate razne sadržaje itd. Na internetu ste često preplavljeni zahtjevima za preuzimanje svih vrsta sadržaja, uključujući pozadine, screensaver i widgete. Ako se odlučite za preuzimanje ovakvog sadržaja, morate znati da u ovom slučaju vjerojatno preuzimate trojanca. Kao što ime govori, trojanac je zlonamjerni program koji oponaša nešto

što nije i sadrži skriveni program čija je svrha nanošenje štete.[13] Na taj način trojanci mogu učiniti različite vrste štete vašem računaru: obrisati ili prepisati podatke na vašem računaru, evidentirati pritiske na tastere za pristup vašim ličnim podacima, onemogućiti firewall i antivirusne programe i instalirati druge viruse. Špijunski softver je program koji "prati" vašu aktivnost na Internetu, dok je adver program koji instalira iskačuće prozore i reklame na vaš računar.

Mnogi poznati virusi rade na oba. Junkware je u najboljem slučaju bezopasan – može prikupiti informacije o vašim navikama surfanja i prikazati reklame (adware) koje odgovaraju vašim interesima. Uprkos tome, to je napad na privatnost koji može značajno usporiti vaš računar. U najgorem slučaju, špijunski softver može biti zlonamjeran, skenirajući vaš tvrdi disk u potrazi za ličnim podacima, kao što su bankovni podaci i lozinke, i propuštajući ih kriminalcima. Takođe, može pokušati da sruši instalirane antivirusne i antišpijunske programe.

Scareware je zlonamjerni program koji generiše iskačuće prozore slične Windows porukama, a zatim oponaša antivirusni ili antišpijunski program, aplikaciju vatrozida ili čistač baze podataka. Svrha ovakvih poruka je da ubijede korisnika da na njegovom računaru ima mnogo zaraženih fajlova. Korisniku se tada savjetuje da kupi određeno softversko rješenje koje će riješiti njegov problem. Zapravo, problem uopće ne postoji, a preporučeni program bi mogao biti pravi zlonamjerni softver. Ako korisnik vjeruje ovim porukama, ne samo da će izgubiti novac trošenjem na beskorisni program, već će njegovi lični povjerljivi podaci vjerovatno završiti u rukama pravih kriminalaca.

Prilikom korištenja društvenih mreža važno je naglasiti da se identitet osobe na društvenoj mreži ne može smatrati njenim identitetom u smislu tačnosti ličnih podataka. Tačnije rečeno, utvrđivanje i provjera tačnog identiteta lica sredstvima i sredstvima kriminalne tehnologije moguće je samo provjerom lične karte izdate od strane nadležnog organa ili druge javne isprave koja sadrži fotografiju i potpis lica. Na društvenim mrežama postoje milioni registrovanih korisnika sa velikim brojem profila sa istim ličnim podacima, od kojih samo jedan može biti "pravi", a ostali su "lažni" profili. Ovo je posebno uobičajeno kada su u pitanju poznate ličnosti u sportu ili šou biznisu, pa je fenomen gotovo nemoguće kontrolisati.

[13]Finnemore, Martha and Sikkink, Kathryn. 1998. “International norm dynamics and political change, international organization”, Harvard Kennedy School, Cambridge.

Osim toga, veliki broj korisnika društvenih mreža ima otvoren veliki broj vlastitih profila na istoj društvenoj mreži, pa je nemoguće znati da li se radi o "pravom" ili "lažnom" profilu.

Neophodno je imati na umu da prilikom kreiranja profila na društvenoj mreži korisnik prihvata uslove korišćenja društvene mreže jednim klikom miša, čime efektivno sklapa ugovor sa kompanijom koja je vlasnik društvene mreže. Osim toga, potrebno je uzeti u obzir da se svi korisnički podaci i sadržaji objavljeni na društvenim mrežama nalaze na serverima kompanija koje posjeduju društvene mreže ili email servise, najčešće u inostranstvu, pa je prikupljanje podataka neophodno za dokazivanje mogućeg krivičnog djela, što često se povezuje s dugotrajnim i složenim procesom pružanja međunarodne pravne pomoći, što donekle usporava stvari i otežava dokazivanje i rasvjetljavanje ovakvih zločina. Phishing je proces kojim prevaranti dobijaju osjetljive informacije, kao što su korisnička imena, lozinke ili informacije o kreditnoj kartici, slanjem lažnih e-poruka ili tekstualnih poruka za koje se čini da ih šalju legitimne organizacije (Nakić, A., 2017).

Čini se da ove poruke često dolaze iz banaka, popularnih društvenih mreža ili web-lokacija za kupovinu i prodaju. Phishing se uglavnom obavlja putem e-pošte ili tekstualnih poruka u stvarnom vremenu (instant messaging), pri čemu se od korisnika često traži da ostave svoje podatke na lažnim web stranicama (gotovo identičnim pravim stranicama). Čak se i lažni iskačući prozori mogu pojaviti na legitimnim stranicama. Nakon što kliknete na takav prozor ili unesete svoje lične ili podatke o identitetu, vaši podaci se prenose na drugu osobu. To znači da od tog trenutka nepozvane osobe mogu pristupiti vašem računu. [14]

Također, neke e-poruke sadrže veze i nadaju se da će vas uvjeriti da posjetite web stranicu na kojoj ćete preuzimati zlonamjerni ili zlonamjerni softver (malware) koji prevaranti mogu koristiti za dobivanje podataka ili novca. Od pribora se može instalirati i pozvati ransomware, ne samo zlonamjerni softver. Takvi programi šifriraju vaše datoteke, uključujući muziku i fotografije, a prevaranti zahtijevaju "otkupninu" da bi ih vratili. Vishing je sličan phishingu, ali se odnosi na lažne pozive u kojima se prevarant predstavlja kao zaposlenik neke institucije (kao što je banka) i traži od vas da prebacite sredstva sa svog računa na nepoznati račun. U tom cilju prevaranti pokušavaju da priču "prodaju" što uvjerljivije. Kao rezultat toga, prevaranti će se pretvarati da su zaposleni u satelitskoj televiziji, telekomunikacijama ili komunalnim preduzećima i ponuditi vam povrat novca.

[14] https://www.hub.hr/hr/sigurnost-na-internetu/vrste-prijevara/phishing (19.3.2022.)

Da bi to učinili, od vas će tražiti da stavite svoju karticu u token i date im kod za autorizaciju transakcije. Ovaj kod će se tada koristiti za izvršenje trgovanja sa vašeg računa. Stoga je veoma važno da svaki poziv koji od vas traži lične podatke, broj računa ili druge identifikacione podatke morate biti oprezni kako ne biste postali žrtva prevare. Svi koji imaju adresu e-pošte primaju neželjenu poštu - neželjene promotivne e-poruke koje se automatski šalju hiljadama ljudi i reklamiraju ili reklamiraju različite proizvode i usluge. Prevaranti takođe šalju milione takvih e-mailova širom interneta navodno da predstavljaju finansijske ili druge institucije. Njihovi mejlovi sadržavali su priloge koji su navodno sadržavali informacije o sumnjivim transakcijama, računima, faksovima ili glasovnim porukama. Zaštita djece i maloljetnika na internetu jednako je važna kao i njihova zaštita u stvarnom svijetu.

Djeca i maloljetnici su ranjiva grupa korisnika interneta koji zapravo nisu svjesni svih opasnosti, od kojih je najopasnija pornografija. Uz kontinuirani razvoj tehnologije i sve veći broj korisnika interneta, važnost zaštite djece u svijetu interneta raste iz dana u dan. Vrijednost interneta kao obrazovnog alata je neupitna, a bogatstvo informacija koje pruža odavno je prepoznato. Također, internet se smatra tehnološkim čudom koje nažalost nudi ogromne mogućnosti za zlostavljanje djece i dugo je bio ogromna industrija i sredstvo ilegalnog zarađivanja ogromnih suma novca, a u mnogim slučajevima i novca zarađenog zlostavljanjem djece. Internet je pojačao uznemirujući fenomen, dječiju pornografiju, o čemu svjedoči sve veća količina pornografije na internetu (Marczi, S., 2014).

Dječija pornografija je nesumnjivo postala jedan od najčešćih oblika seksualnog zlostavljanja djece i maloljetnika. Kontinuiranim unaprijeđenjem i povećanom dostupnošću elektronskih sredstava komunikacije, zloupotreba dječije pornografije dostigla je nezamislive nivoe, što zahtijeva jedinstveni sistem za borbu protiv dječje pornografije i drugih oblika seksualne eksploatacije i zlostavljanja djece, uz međunarodnu i prevenciju širom svijeta. Osnova za suprotstavljanje, sprječavanje i kažnjavanje ovakvog zlostavljanja djece i maloljetnika sadržana je u međunarodnim instrumentima koji garantuju osnovna prava osoba i građana, uključujući djecu i maloljetnike, te predstavljaju najširu zaštitu zajamčenih ljudskih prava (Derečinović, D., 2003.).

1.2. Cyber prijetnje

Kako bismo zaštitili naše računare, podatke koje oni sadrže i sve što radimo koristeći internet, potrebno je poduzeti određene mjere kako bismo spriječili moguće cyber upade u naše računare, pokušaje preuzimanja podataka ili kontrolne opreme, kroz različite vrste profesionalnih i obuka. U slučaju upada u nečije računare, kriminalci koriste neki zlonamjerni program da nenamjerno dobiju pristup tom računaru. O takvim programima i načinima za sprečavanje njihovih štetnih efekatac reći ćemo nešto u nastavku rada.

Ako je vaš računar zaražen virusom/trojanskim, primijetit ćete da se vaš računar ponaša čudno, muzika se automatski uključuje, poruke ili iskačući prozori se pojavljuju na ekranu vašeg računara, datoteke se mijenjaju ili brišu, vaš tvrdi disk je oštećen ili izbrisan, vaš računar je spor ili uopšte ne reaguje.

Postavlja se pitanje, kako možemo izbjeći viruse/trojance!? Neki od načina, tačnije zaštitne mjere za izbjegavanje virusa i trojanaca koje možemo koristiti su: da instaliramo antivirusni/antimalware program na svoj računar, da provjerimo je li naš antimalware program ažuriran, da skeniramo cijeli računar sedmično, da preuzimamo samo sadržaje iz pouzdanih izvora sa interneta. Također bitno je izbjegavati preuzimanje piratskog sadržaja (uključujući filmove, muziku i kompjuterske programe). Iako je besplatan, takav sadržaj može sadržavati zlonamjerni softver, Uvjerite se da su uobičajene aplikacije i dodaci, kao što su Microsoft Office, Adobe Acrobat i Adobe Flash, uvijek ažurni i da imaju sve sigurnosne funkcije. Mnoge aplikacije se mogu automatski ažurirati. [15]

Moramo biti posebno oprezni kada plaćamo online, te je potrebno da uvijek provjerimo da li je stranica na kojoj se nalazimo zaštićena. Da bi bili sigurni da posjećujete pravu stranicu, trebate unijeti adresu u svoj pretraživač umjesto da kliknete na vezu. Ako je vaš računar zaražen, primijetit ćete da se iskačući prozori s adverom pojavljuju na vašem računalu čak i ako vaš računar nije povezan s internetom, početna stranica vašeg preglednika ili postavke pretraživanja se mijenjaju bez upozorenja, a nova, neočekivana i neželjena traka sa alatkama se pojavljuje na vašem pretraživaču , vaš računar usporava, a sistem se sve češće ruši.

[15] https://support.microsoft.com/hr-hr/windows/za%C5%A1tita-pc-ja-od-virusa-b2025ed1-02d5-1e87-ba5f-71999008e026 (21.3.2022.)

1.3. Cyber odbrambene tehnologije

Cyber tehnologije nisu prijetnja, već odgovor na prijetnju.

U nastavku rada, predstaviti ćemo nekoliko primjera kako izbjeći softvere za špijunažu.

Ako slijedite ove savjete, možete sa sigurnošću reći da ćete biti sigurni od špijunskog/advera, ali i od mnogih drugih sigurnosnih prijetnji na internetu. Preuzmite i instalirajte anti-špijunski program sa interneta! Microsoft korisnicima Windowsa pruža Windows Security Essentials, besplatni antišpijunski program. Osim toga, drugi proizvođači softvera nude slične proizvode, a mi ćemo preporučiti najbolje rješenje za vaš sistem, a to je da ažurirate program. Ako koristite Windows, možete preuzeti ažuriranja programa sa Microsoft web lokacije. Na istoj stranici možete automatski ažurirati svoj računar, tako da ne morate da brinete o preuzimanju najnovijih ažuriranja i verzija softvera.[16]

Oprezno surfajte internetom, te još opreznije preuzimajte sadržaj. Preuzmite programe samo sa web lokacija u koje imate povjerenja. Ako imate pitanja o sigurnosti određenog programa, možete unijeti njegovo ime u pretraživač i provjeriti da li je neko prijavio da program također sadrži špijunski softver. Pročitajte sva sigurnosna upozorenja, licencne ugovore i obavijesti o privatnosti prije preuzimanja bilo kojeg programa, te nikada nemojte kliknuti na "OK" ili "slažem se" u iskačućem prozoru osim ako niste sigurni s čime se slažete.

Budite oprezni s besplatnim programima za dijeljenje muzike ili filmova i svakako istražite rješenja u paketu s takvim programima. Veoma je bitno voditi računa da ispravan i legitiman antivirusni i antimalware program uvijek bude instaliran na računaru.

Ono što možemo još reći, to je da je posebno važno nikada ne klikčete na iskačuće prozore koji tvrde da je vaš računar zaražen ili nude skeniranje vašeg računara u potrazi za greškama. Ovo je skoro uvijek jedan vid prevare. Potrebno je koristiti kvalitetne lozinke te tako da zaštitite svoj račun lozinkom koju je teško pogoditi. Ako je vaša lozinka ugrožena, neko bi mogao dobiti neovlašteni pristup vašem računu, lažno se predstavljati ili zloupotrebiti vaše podatke na bilo koji drugi način. Postavke privatnosti i sigurnosti pomoći će vam da odredite ko može pristupiti vašim objavama. Prilagodite postavke privatnosti i sigurnosti koliko god je to moguće kako biste dijelili informacije najbolje što možete. Možete ograničiti informacije

[16] http://www.download.hr/forum/vijesti/2129-prijete-cyber-teroristi.html (19.03.2022.)

koje dijelite s javnošću. Krađa identiteta postala je jedna od najozbiljnijih ilegalnih aktivnosti na internetu. Kriminalci koriste informacije izvučene sa društvenih mreža kako bi preuzeli identitet drugih, a zatim se sakrili iza svog identiteta, koristeći sofisticirane tehnike društvenog inženjeringa za provođenje raznih vrsta prijevara na internetu, ciljajući na pojedince i kompanije. Bitno je obrazovati djecu te ih osvijestiti kroz razne edukacije koliko je bitno dijeliti podatke, na pravi i ispravan način. U interesu je svih roditelja da svoju djecu edukuju o bezbjednom ponašanju na internetu i prate ponašanje svoje dece kada su online. Podučavajući djecu o sigurnosti na internetu, slijedeći njihove navike na mreži i usmjeravajući ih na odgovarajuće web stranice, roditelji svoju djecu mogu učiniti sigurnim i odgovornim korisnicima.

Pažljivim odabirom onoga što ćete objaviti na društvenim mrežama možete zaštititi svoj lični integritet i ugled, jer ono što se jednom objavi, ostaje zauvijek na internetu, nikada se ne može u potpunosti povući i gubite kontrolu nad daljom distribucijom i korištenjem objavljenog sadržaja. Stoga uvijek dobro razmislite prije postavljanja fotografija, videa ili tekstualnog sadržaja. Postoje ljudi koje možemo nazvati predatorima (npr. pedofili) na društvenim mrežama a koriste ih da pronađu potencijalne žrtve. Vrlo je lako stvoriti i održavati lažni identitet na internetu, pa je korisno uvijek biti skeptičan prema svemu što čujete i vidite na društvenim mrežama. Ako želite uživo upoznati ljude koje ste upoznali na društvenim mrežama, nađite se na javnom mjestu, po mogućnosti u društvu poznatih.

Kako prepoznati phishing? Lažni e-mailovi se mogu slati s adresa koje izgledaju slične službenoj adresi institucije s kojom komunicirate, ali ako ih pažljivo pogledate, vidjet ćete razliku od prave adrese. U takvim, lažnim, mailovima često se traže lični podaci kao što su lozinke, podaci o online bankarstvu, kontakti ili brojevi kreditnih kartica. Loš pravopis i formatiranje teksta e-poruke ponekad mogu sadržavati gramatičke i pravopisne greške. Također, lažne web stranice mogu izgledati malo drugačije i sadržavati pogrešno napisane riječi. Može biti napisano na lošem bosanskom, srpskom ili hrvatskom jeziku ili zvučati kao loš automatski prijevod (npr. iz Google Translate). Budite oprezni ako dobijete e-poštu bez teksta i samo u prilogu. Prava institucija i agencija vam nikada neće poslati e-mail bez sadržaja.

Kako bismo se što efikasnije zaštitili od ovakvih online prevara, potrebno je biti oprezan sa svim emailovima koje primamo. Povratne adrese ili adrese pošiljaoca mogu biti krivotvorene. Možete vidjeti punu adresu e-pošte pošiljaoca tako da postavite pokazivač miša iznad imena

pošiljaoca. Zaglavlja e-pošte i linkovi na web stranice također mogu biti lažni. Ako zadržite pokazivač iznad veze, vidjet ćete potpuno drugačiju stranicu. Stoga se ne preporučuje otvaranje linkova iz neočekivanih ili sumnjivih poruka e-pošte. Konkretno, nikada ne biste trebali otvarati priloge neočekivanih poruka e-pošte s ekstenzijama .exe, .pif ili .vbf.

Da biste zaštitili svoj račun i smanjili količinu neželjenih e-poruka, potrebno je poduzeti sljedeće korake:

- Poništite izbor u polju - ako institucija ili pojedinac zatraže vašu adresu e-pošte, pročitajte tekst malim slovima i jasno naznačite da ne želite dijeliti svoje podatke s drugima
- Uključite filter za neželjenu poštu - vaš administrator će vam dati opciju da filtrirate dolaznu e-poštu i preusmjerite neželjenu poštu u vaš spam folder. Ovaj folder će se s vremena na vrijeme prazniti, tako da ubuduće nećete primati toliko neželjenih e-poruka. Neka neželjena pošta će i dalje biti u vašem sandučetu i moraćete da je izbrišete. Označite takve poruke, zanemarite ih i izbrišite. Ako dobijete e-poštu s neočekivanim prilogom ili vezom, nemojte je otvarati.

Kako se mogu zaštititi od krađe identiteta?

Postoji nekoliko jednostavnih koraka koje trebate poduzeti, te tako možete u velikoj mjeri zaštititi svoj identitet od cyber kriminalaca. S tim u vezi, potrebno je pridržavati se sljedećih nekoliko pravila: zaštitite svoje poruke i poštu ispravnim korisničkim imenom i lozinkom;koristite drugačiji PIN i lozinku za svaki nalog i aplikaciju (ako koristite istu lozinku za sve i prevaranti ih se dočepaju, imat će pristup svemu); ne otkrivajte svoju lozinku nikome; budite oprezni kada koristite internet u kafiću ili ste aktivni na društvenim mrežama i forumima, virtuelnim chat sobama, jer su to situacije koje koriste prevaranti za curenje ličnih podataka drugih; nikada ne ostavljajte lične podatke na internetu, kao što su brojevi telefona, datumi rođenja ili podaci o zaposlenju; naučite kako koristiti svoje sigurnosne opcije na mreži i postaviti ih na način koji vam najbolje odgovara; budite svjesni s kim ste "prijatelji" na društvenim mrežama i kome dozvoljavate da se pridruži vašoj mreži. Također bitno je da izbjegavate online opcije automatskog dovršavanja i popunjavanja obrazaca jer prevaranti mogu lako pristupiti takvim programima. Čuvajte se fišing finansijskih institucija koje traže

od vas da potvrdite podatke o računu. Pomozite da se razotkriju prevaranti tako što ćete prijaviti takve e-poruke agenciji iz koje su navodno došli. [17]

Finansijske institucije nikada ne traže od klijenata da potvrde putem e-pošte. Ako smatrate da je neko ukrao vaš identitet, neko je dobio neovlašćen pristup podacima o vašem bankovnom računu ili je neko nezakonito pristupio nekim vašim računima na internetu, odmah prijavite svoju sumnju policiji.

Kako zaštititi dijete? Postojio nekoliko koraka da se zaštiti. Ti koraci su: naučite svoje dijete da ne šalje svoje lične podatke na internet (ime, adresu, broj telefona, lozinku, ime roditelja, naziv kluba kojem pripada, itd.); stavite računar u stan gdje možete lako da kontrolišete njegove aktivnosti – najbolje u dnevnoj, a ne u dječijoj sobi, te redovno provjeravajte historiju pretraživanja da vidite koje stranice dijete posjećuje; redovno pitajte svoje dijete o aktivnostima na mreži i prijateljima; možete instalirati programe za privatnost i neprikladan sadržaj. Također, možete napraviti pravila korištenja interneta, to jeste da se dogovorite sa svojom djecom o korištenju interneta. Provođenje previše vremena na mreži, posebno noću, može ukazivati na probleme. Tada morate pratiti promjene u djetetovom okruženju (prisustvo stranaca, povjerljivost, neprimjereno seksualno znanje, problemi sa spavanjem, itd.). Također, ograničite djecu da kreiraju i koriste internet profile i ostavljaju svoje lične podatke. Na ovaj način ćete uveliko smanjiti rizik od kontakta sa strancima. Vaše dijete mora znati da može prestati koristiti računar ako prekrši dogovorena pravila. [18]

Kako prepoznati izloženost djece neprikladnom sadržaju na internetu?

Vaše dijete postaje tužno, ljuto ili uznemireno nakon korištenja mobilnog telefona ili interneta; izbjegava da priča o tome kako koristi svoj kompjuter ili telefon; izbjegava grupne aktivnosti; pokazuje promjene u raspoloženju, ponašanju ili apetitu; plaši se fizičkog kontakta i ima odbrambeni govor tijela; prikriva se i skriva u pokušaju da bude nevidljiv i slično.[19]

Svi imamo informacije na svojim pametnim telefonima koje hakeri mogu koristiti za krađu identiteta ili novca sa bankovnih računa. Koristeći se mudro i slijedeći neke od savjeta i pravila koja dajemo u nastavku, možete se efikasno zaštititi od takvih napada i zloupotreba.

[17] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (22.3.2022.)
[18] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (22.3.2022.)
[19] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (22.3.2022.)

Ažuriranja softvera se instaliraju čim postanu dostupna - isto važi i za računare i pametne telefone. Iako ažuriranja mogu biti zamorna i dosadna, a ponekad mogu promijeniti izgled web stranica koje biramo i na koje smo navikli, ne bi trebali odustati od ove učinkovite metode sprječavanja hakovanja. Takođe se preporuč.uje izbjegavanje tzv. „rootiranja“ telefona, jer se na taj način omogućava neovlašteni pristup podacima pohranjenim na telefonu. Termin "root" u drugim aspektima odnosi se na proces omogućavanja punog pristupa operativnom sistemu pametnog telefona. Ovo vam omogućava da promijenite gotovo bilo koji dio softverskog koda uređaja.

Dakle, "rooting" je u osnovi hakovanje vlastitog uređaja, a korisnici iPhonea i drugih IOS uređaja ovu proceduru nazivaju "jailbreaking". Budite oprezni kada instalirate nove aplikacije - prilikom instaliranja aplikacija za pametne telefone, često je potrebna dozvola za čitanje datoteka, pristup kameri ili mikrofonu. Sve ove, inače korisne mogućnosti, predstavljaju potencijal za zloupotrebu uređaja, odnosno podataka pohranjenih u njemu. Stoga se mora pažljivo razmotriti prije odobravanja pristupa, a osnovni savjet je da ne instalirate ništa sa nepoznatih i neprovjerenih stranica.

Provjerite šta je instalirano na vašem telefonu - ponekad se čak i bezopasna aplikacija koja je već na vašem telefonu može pretvoriti u zlonamjerni softver s naknadnim ažuriranjima. Može biti korisno pogledati sve aplikacije na svom pametnom telefonu i provjeriti dozvole koje koriste. Postoje i sigurnosne aplikacije koje bi mogle pomoći u ovoj situaciji, kao što su besplatni softverski paketi Avast i McAfee, koji vas upozoravaju kada pokušate instalirati zlonamjerne aplikacije i upozoravaju vas kada su instalirane nepouzdane aplikacije ili stranice, kako bi vas upozorili na pokušaj phishinga. Provjerite je li vaš telefon zaključan kada ga ne koristite. Android i iOS mogu pružiti šestocifreni pristupni kod. Zatim postoje i druge opcije, poput otiska prsta ili prepoznavanja lica, iako čak ni takve metode ponekad ne stoje na putu tvrdoglavim i vještim hakerima koji pronalaze načine da kopiraju otiske prstiju ili prevare kameru pokazujući vašu sliku. Također, vodite računa o otključavanju funkcije "Smart Lock" vašeg pametnog telefona kada ste kod kuće ili u blizini pametnog sata. Telefon neće znati da je ukraden, pa će lopovima omogućiti pristup podacima.

Daljinski nadgledajte i zaključavajte svoj telefon – da biste zaštitili podatke pohranjene na vašem telefonu, čak i u slučaju krađe, jedna od opcija je da podesite telefon da automatski briše podatke nakon višestrukih pokušaja pogrešne lozinke. Također, ne zaboravite da i Apple i Google nude usluge lokacije izgubljenog telefona, kao i mogućnost daljinskog zaključavanja

ili brisanja podataka. Korisnici Apple-a svojim telefonima pristupaju putem iClouda - Postavke > iCloud > Find My iPhone, dok korisnici Androida mogu pristupiti Googleovim uslugama putem google.co.uk/android/devidemanager. Preporučuje se da uključite melodiju zvona ako je telefon izgubljen ili ukraden. Ne ostavljajte internetske usluge otključane – automatska prijava uvelike olakšava korištenje telefona, ali je i posao lopova koji jednostavno otvori pretraživač kako bi pristupio svim online nalozima.

U najboljem slučaju, opcija automatske prijave ne bi se trebala koristiti uopće. Ne biste trebali koristiti istu lozinku za različite aplikacije ili usluge. Hakeri su dužni hakovati internetske usluge kako bi ukrali korisničke podatke, a zatim ih testirali na drugim stranicama. Unošenje lažnih podataka – Kombinovanjem svih navedenih načina i sredstava za osiguranje vašeg pametnog telefona podaci na vašem pametnom telefonu su veoma sigurni, ali neki hakeri podataka ne mogu pristupiti telefonu. Dakle, datum rođenja, mjesto rođenja, majčino djevojačko prezime itd. možete pronaći na Facebooku ili nekoj drugoj društvenoj mreži. Ove informacije su ponekad dovoljne za pronalaženje i postavljanje ispravne lozinke i pristup računu. Takve napade možete spriječiti unosom lažnih podataka iz svog životopisa.

Rizici korištenja otvorene bežične mreže uvijek su prisutni, ali možda ne znate da to znači da gotovo svi u blizini mogu vidjeti šta radite na mreži. Doduše, takav napad zahtijeva poseban softver i posebne vještine, ali kada su u pitanju ove stvari, opreza nikad dosta. Ako sumnjate u sigurnost svoje bežične mreže, preporučuje se VPN alat poput CyberGhost ili TunnelBear, koji je dostupan i za Android i za iOS. Ovi alati usmjeravaju promet kroz privatne šifrirane kanale, pa čak i ako neko prati vaš promet, ne može vidjeti šta radite na mreži. Nemojte dozvoliti obavještenja na zaključanom ekranu - mnoge aplikacije postavljaju poruke i obavještenja na zaključani ekran vašeg telefona. Pitanje je šta takve obavijesti sadrže. Dakle, nije loša ideja da razmislite o onemogućavanju pristupa Siri sa zaključanog ekrana na iOS-u. Najsigurnije je potpuno isključiti postavke: Postavke > Touch ID i šifra > Onemogući Siri na zaključanom ekranu. Zaključajte pojedinačne aplikacije - jaki pristupni kodovi mogu sačuvati podatke na vašem telefonu, ali također mogu pretpostaviti da je vaš telefon ukraden dok ga koristite. U ovom slučaju, "druga linija odbrane" za podatke pohranjene na vašem telefonu bila bi zaključavanje pojedinačnih aplikacija na Androidu, jer bi svako ko ima otključan telefon teško pokušao pristupiti vašoj e-pošti ili aplikacijama za bankarstvo, bez druge aplikacije Ova funkcija nije ugrađena u operativni sistem, ali postoji mnogo besplatnih aplikacija koje to omogućavaju, npr. AVG Antivirus je besplatan. Korisnici iOS-a ne mogu direktno zaključati pojedinačne aplikacije, ali to mogu učiniti pomoću Folder Lock, koji je

dostupan za besplatno preuzimanje sa App Store-a. Ova aplikacija štiti vaše dokumente i mape dodatnom lozinkom, smanjujući mogućnost neovlaštenog pristupa informacijama (Kulović, A., 2019).

Sat će vas upozoriti da vam je telefon ukraden - ako niste sigurni može li pametni sat pružiti dodatnu zaštitu za vaš pametni telefon, onda treba da znate da će vas uređaji poput Apple Watcha ili Android Weara upozoriti ako izgubite Bluetooth vezu sa vašim telefonom. Jer, ako dobijete ovo obavještenje na javnom mjestu, velike su šanse da vam je telefon upravo ukraden. Osim toga, uređaj će zvoniti svaki put kada se nalazite na 50 metara ili manje od svog telefona, tako da vam daje dovoljno vremena da pronađete ukradeni telefon ili ga zaključate prije nego što lopovi pokušaju doći do vaših podataka.

GLAVA II

ULOGA CYBER SIGURNOSTI U KONTEKSTU NOVIH IZAZOVA I PRIJETNJI

Snažan interes za potencijalne cyber katastrofe datira još od sredine 1990-ih, kada su se pojavili izvještaji poput kompjuterskih napada, te predstavlja sve veći rizik.

Danas postoji jedan specifičan domen ljudskog delovanja a to je cyber prostor. Njegove prepoznatljive i jedinstvene karakteristike su kreiranje, pohranjivanje, mijenjanje, razmjena i korištenje informacija korištenjem elektronskog i elektromagnetnog spektra za stvaranje, pohranjivanje, mijenjanje, razmjenu i korištenje međusobno povezanih sistema zasnovanih na informaciono-komunikacionim tehnologijama (IKT) i pripadajućoj infrastrukturi.” (Kuehl, 2009).

Gornja definicija cyber prostora nije isključiva definicija, ali se citira kao opsežna definicija u stručnoj literaturi (Kramer, 2009). Zbog sve višeg razvijanja cyber kriminala, dovedeno je u pitanje neophodno funkcionisanje mnogih društvenih klasa. Zbog toga, u pogledu sigurnosti, potrebno je demonstrirati odgovarajuće kompetencije i mjere zaštite kao, prevladati i eliminisati situacije koje narušavaju društvenu stabilnost, razvoj države i društva (Masleša, 2001). Psihološka istraživanja pokazuju da su osjećajne potrebe dio ljudske prirode te da je neophodno kazniti ljude koji krše društvene norme.

2.1. Cyber terorizam

Iako je jasno da teroristi postaju sve veći korisnici IT opreme i interneta, važno je istaći da nije svaka nelegalna upotreba IT opreme sama po sebi "mreža" terorizam. „Cyber“ terorizam je prilično nov termin koji opisuje infiltraciju i virtuelni kompjuterski svijet. U širem smislu, "cyber terorizam" se odnosi na napade i prijetnje kompjuterima, kompjuterske mreže i IT uređaji za skladištenje koji se koriste u svrhe zastrašivanja, te utjecati na strukture upravljanja i javnost u političkom i društvenom životu. S tim u vezi, cyber terorizam je klasifikovan kao napad, i trebalo bi da izazove nasilje nad ljudima i objektima, ili barem nanese dovoljno štete da izazove strah.

Situacije kao što su neovlašteni daljinski upad u kompjutersku mrežu kontrole zračnog ili cestovnog saobraćaja, uzrokujući štetu kao što je ljudski život, teška materijalna šteta i panika, definitivno se definirana kao IT Terorizam, uz ulazak u manje važnu kompjutersku mrežu i onemogućavanje iste. Upotreba od strane drugih korisnika ne može se smatrati terorističkim napadom, već kompjuterskim napadom.

Nažalost, danas nije do kraja razjašnjeno šta je informacioni terorizam, te se često pojavljuje nesporazum u tumačenju. Termin "cyber" terorizam se često pogrešno shvata. Slučajevi zloupotrebe računara ili interneta kao što su hakiranje, prijenos virusa i niz kompjuterskih online događaja koji uzrokuju samo manju štetu ili poteškoće je klasificirano samo kao pokušaji cyber kriminalaca da testiraju svoje sposobnosti. Oni na taj način sebi i svojoj okolini demonstriraju kako mogu uticati ili nanijeti štetu nekome ili nečemu.

U prošlosti su zabilježeni IT incidenti koji su uključivali teroriste, ali nisu prouzročili značajniju štetu osim finansijske.

Da bi se IT napad klasifikovao kao cyber terorizam mora ispunjavati određene kriterije. Ti kriteriji su da se sazna identitet napadača kao i teroristička organizacija koja stoji iza njega; ugao i ishod napada, prouzrokovana šteta te teroristički cilj.

Cyber terorizmom takođe treba manipulisati takozvanim „informacionim ratovanjem“, gdje se računari i računarske mreže koriste u kontekstu ratnih sukoba među narodima. Informacioni rat se vodi kroz ofanzivne i odbrambene aktivnosti državne strukture. Međunarodni sukobi, terorističke taktike zastrašivanja koje se koriste u terorizmu zasnovani su na ideologiji. Ova dva oblika djelovanja mogu se preklapati kada se koriste određene tehnike kao što je ometanje računarskih mreža i slično.

Teroristi također mogu koristiti tehnike hakovanja kako bi skrenuli pažnju na sebe. Postoje tehnike koje se koriste za neovlašteno prikupljanje podataka, ali nijedna od ovih aktivnosti ne predstavlja potpuni teroristički akt ili napad, tako da ne potpada pod pojam "cyber" terorizam. Tehnologija, kao i svaka druga napredna tehnologija, može se koristiti ilegalno. Cyber terorizam nije slučajno zaobilaženje zakonskih pravila za korištenje kompjuterske opreme. Internet terorista ne znači druge oblike kriminala već je riječ definirana kao unaprijed zamišljena, gdje su ideološki motivisani napadi na računarske sisteme, programe, baze podataka i mreže implementirani uz pomoć informacionih tehnologija i dovode do straha,

nasilja i nanošenje značajne materijalne štete neborbenim ciljevima i radi uticaja na javnost i politiku proces.

Jednostavno rečeno, cyber terorizam je korištenje visokotehnoloških sredstava za borbu koje se dešava zbog određenih kriminalnih ciljeva. Upoređujući prijetnju stvarnog "cyber" terorizma sa općom svakodnevnom realnošću, korištenje napredne informatičke tehnologije od strane terorista treba imati na umu dvije različite stvari, a to je da oba aspekta zaslužuju pažnju i analizu. Donijeti odluku o tome da li su potrebne konkretne mjere za borbu protiv terorizma ne zavisi samo od stvarne prijetnje cyber terorizma, već i od postojanja potencijalne IT podrške.

Društvo je teroristima veoma privlačno iz više razloga. Prije svega, njihov potencijal, kompjuteri, omogućavaju teroristima da izvode napade na velikom dometu što im garantuje anonimnost i niske finansijske troškove. Neke mete privlačne teroristima nemoguće je probiti jer nisu izvodljive na daljinu ili bez vlastitih (terorističkih) žrtava. Neki ciljevi, kao što su transportni, energetski ili komunikacioni sistemi, ne mogu biti podložni klasičnom terorističkom napadu bi izazvao toliko štete i podstakao strah javnosti, te se tada trude što je više moguće, napad izvršiti pomoću informacionih tehnologija, a reakcija javnosti se neće na osjetiti na baš velikom nivou. Većina hakerskih napada se drži u tajnosti od javnosti kako bi se izbjegla panika i rast. Također, nepovjerenje u kompromitovane sisteme, ozbiljne i uspješne kompjuterske terorističke napade često bude skriveno od javnosti (Stanković, N. 2014).

Informaciona tehnologija može pomoći teroristima jer se koristiti i kao multiplikator moći, jer im omogućava pristup ciljevima koje nikada ne bi mogli postići. To im ipak neće omogućiti pristupiti drugim aspektima, kao što su nacionalna sigurnost i sistem odbrane. Istraživanja koja je provela Agencija za nacionalnu sigurnost (NSA) 1997. godine dokazala su da su američki vojni kompjuterski sistemi u nekim slučajevima podložni hakiranju. Američki vojni kompjuterski sistemi registrovali su čak 250.000 hakiranja svake godine, ali do sada nije zabilježena šteta ili barem javnost nije upoznata sa istom. Međutim, barem u teoriji, postoje određena ograničenja u korištenju informacijske tehnologije od strane terorista. Uprkos tome što su ranjivi, računarski sistemi su i dalje veoma složene strukture, što nam daje zaključak da praćenje implementacije samog napada i postizanje željenog nivoa može biti veoma složeno.

Teroristi neće biti motivisani da koriste nove metode i alate u svojim napadima osim ako staro (tradicionalno) se ne smatra neprikladnim. Iako je mnogo prednosti koje napadi na „daljinsko

upravljanje“ nude, ono istovremeno čine da se teroristi osjećaju nesigurno i teško kontroliraju postignute rezultate. Općenito, ako teroristi nisu sigurni, nerado eksperimentiraju. To će imati željeni efekat.

Osvrnuti ćemo se na drugi oblik koji se odnosi na nivo koji trenutno koriste teroristi. Informacijska tehnologija je koristan alat za podršku koji se može postaviti kod kuće. Vidjelo se da su terorističke grupe zapravo imale koristi u velikoj mjeri od informaciona tehnologije, ali ta korist nije veća od bilo koje druge moderne tehnologije. Naivno je misliti da teroristi, kao i svaka druga kriminalna grupa, neće imati koristi od razvijanja IT-a.

U opštoj upotrebi informacionih tehnologija, poznata je i nedvosmislena činjenica da današnji teroristi koriste kompjutere za komunikaciju i skladištenje regrutacija podataka i članstva, širenje publiciteta, prikupljanje podataka i finansije. Teško je precizno procijeniti stepen informatizacije terorističkih organizacija.

Do danas nije zabilježen nijedan veći teroristički napad korištenjem informatičke tehnologije. Prijavljeno je samo nekoliko hakiranja koji su povezani sa terorističkim organizacijama ili koje ih izvode. Tako su 1998. Tamilski tigrovi preplavili ambasadu Šri Lanke bombama za e-poštu. Taj napad nije izazvao gubitke. Od tada je zabilježen niz IT napada vezanih za rat na Kosovu, palestinsko-izraelski sukob, kinesko-tajvanski sukob, Indija-Pakistan itd., koji su više oblik mrežnog napada.

Istraživanja pokazuju da su 90% cyber incidenata krivi amateri, 9,9% su odgovorni "profesionalni" hakeri i industrijski špijuni, a samo 0,1% odgovorni su profesionalci za cyber kriminal svjetske klase. Još jedna studija koja se bavi promjenom raspona prijetnji koje se odnose na međunarodni terorizam, koji pokazuje da se, iako je tehnologija napredovala, promijenila "Referentna knjiga horora", ali njihovi ciljevi i strategije ostaju isti. Zaključili su da su teroristi prihvatili informacionu tehnologiju kao nezavisno oruđe komandovanja i kontrole, ali ipak nisu uvijek spremni za napad na važne informacione strukture. Jasno je da su teroristi iskoristili sve prednosti moderne informacione tehnologije. Nadalje, teško je procijeniti kako će potencijalno napadnuti IT sistem reagirati. Bez obzira na poduzete mjere zaštite ipak postoji opasnost od napada, a trenutni strah od napada može nadmašiti stvarnu prijetnju. Teroristi su uvijek korak ispred antiterorizma jer uvijek traže najslabiju kariku.

Zauzvrat, strah mora biti uravnotežen između stvarnih nivoa prijetnji i nivoa koji značajno ne ograničavaju legitimnu upotrebu informatika i mora se fokusirati na preventivne mjere i brzu

procjenu i sanaciju mogućih oštećenja. Danas teroristi koriste informacijsku tehnologiju za šifriranje i to znači da ne treba ukinuti mogućnost legitimne šifrirane komunikacije. Drugim riječima, razvoj bezbjednosnih mjera treba više da se fokusira na efektivne mjere i kvalitetnu ručnu kontrolu važnih informacionih sistema, kao i efikasnu zaštitu od enkripcije.

Ne postoji precizna definicija "hakovanja". Neki kažu da je to namjerni programerski (u većini slučajeva) kolaps informacionih sistema zbog neke lične frustracije, dok drugi kažu da su sakupljači povjerljivih podataka za preprodaju, a opet, treći kažu kažu da su hakeri ljudi pokušavaju da privuku pažnju svojim virusnim programima iz čiste dosade.

Velike kompanije ih zapošljavaju. Prvi slučaj "hakovanja" zabilježen je 1972. godine, kada je John T. Draper slučajno otkrio da je uz pomoć obične zviždaljke moguće napraviti tonove koji se mogu napraviti da biste mogli besplatno telefonirati. Taj slučaj snimljen je pod imenom BLUE BOX.

Današnji hakeri su uglavnom navikli koristiti posebne pisane kompjuterske programe koji se nalaze u računaru (mi ga zovemo virus) te imaju određeni cilj. Cilj može biti brisanje podataka, kopiranje podataka ili preimenovanje podataka. Upadi u kompjuterske sisteme najčešći su u Sjedinjenim Državama, te je američki Kongres morao da donese zakon o zloupotrebi kompjutera. Zakon nalaže odluku o pet godina zatvora i/ili velika novčana kazna. Kevin Mitnick je najpoznatiji haker svih vremena. On je uz pomoć kompjutera uspio doći do oko 20000 brojeva kreditnih kartica, hiljade brojeva mobilnih telefona te je mogao da ih ilegalno koristi i dijeli svakodnevno na različitim kompjuterskim mrežama u SAD. Nikada nije priznao na koji način je to uspio uraditi ali se pretpostavlja da je upao u sistem NORAD13.

2.2.Cyber sigurnost i upravljanje internetom

Cyber prostor postoji samo unutar parametara izgradnje i regulacije od ljudi. Do danas, ove parametre nije direktno postavila vlada, već postoji takozvani proces odozdo prema gore, koji se često naziva internet samoregulacijom. Ovaj proces se često naziva interni volumen (upravljanje internetom) i definira se kao razvoj i implementacija vlasti, privatnog sektora i civilnog društva u svojim specifičnim ulogama, izvedenih iz zajedničkih principa, normi, pravila, procedura donošenja odluka i procesi koji oblikuju razvoj i upotrebu interneta" (wGiG, 2005.) Internet je relativno novo okruženje za ljudske aktivnosti, stvoreno sa drugima.

Prije 20 godina, ne samo da se kritična infrastruktura djelomično oslanjala na internet, već se sam internet (barem djelomično) nije činio izvodljivim, a danas se smatra veoma bitnim za svakodnevne društvene potrebe, te se može reći da je upravljanje internetom samo složeno i dinamično. Razvoj interneta i tehnologije omogićava hakerima velike prijetnje, te je to jedan od najvećih izazova današnjice, jer mogu izazvati značajnu štetu po ekonomsku, nacionalnu i međunarodnu sigurnost (Generalna skupština Ujedinjenih nacija, 2010).

Joseph Nye (2011), ugledni profesor sa Harvarda definira četiri glavne kategorije cyber pretnji koje su opasne po nacionalnu bezbjednost, a to su špijunaža, cyber kriminal, cyber rat i cyber terorizam. Uzroci špijunaže pomoću interneta mogu se svrstati u tri skupine: (1) nedostaci u dizajnu interneta, (2) nedostaci u hardveru i softveru i (3) trend postavljanja sve više kritičnih sistema online (Clark i Knack, 2010).

Prijetnje po sigurnosti informacija dolaze iz različitih izvora, te se ogledaju u takvim aktivnostima usmjerenim na pojedince, poduzeća, nacionalnu infrastrukturu i vlade. Njihove akcije su značajni rizici po opštu bezbjednost, nacionalnu bezbjednost i stabilnost međusobno povezane međunarodne zajednice (Generalna skupština Ujedinjenih nacija, 2010).

Danas su informacione i komunikacione tehnologije sveprisutne i široko dostupne. One nisu ni civilne ni vojne prirode, već su u mnogim slučajevima u vlasništvu i pod upravom privatnog sektora, ili lični. Zbog složene veze između telekomunikacija i interneta, svaki uređaj može biti izvor ili meta sve sofisticiranijih zloupotreba.

Grupa vladinih eksperata Ujedinjenih nacija za razvoj IKT Međunarodne bezbjednosne službe pripremaju izvještaj u kojem se pozivaju na zemlje članice UN-a o jačanju informacione sigurnosti i međunarodne saradnje (Generalna skupština Ujedinjenih nacija, 2010). Izvještaj daje dalje preporuke dijaloga između država članica UN-a za smanjenje rizika i zaštitu ugrožene nacionalne i međunarodne infrastrukture. Izvještaj UN-a kaže da je globalna IKT mreža postala pozornica za destruktivne aktivnosti. Motivacije za ove ometajuće aktivnosti su različitem a mogu se javiti kao jednostavna demonstracija tehničkih vještina za krađu novca ili informacija, ili kao nastavak sukoba među nacijama. Izvori prijetnji su nedržavni akteri poput kriminalaca i eventualno terorista, kao i sama država.

IKT se može koristiti za uništavanje informacionih resursa i infrastrukture, te kao prijetnja međunarodnom miru i nacionalnoj sigurnosti. Za sada postoji nekoliko naznaka da teroristi pokušavaju da naškode ili unište IKT infrastrukturu ili izvode terorističke operacije pomoću

IKT, iako bi se to moglo intenzivirati u budućnosti. Trenutno se teroristi prvenstveno oslanjaju na ove tehnologije da komuniciraju, prikupljaju informacije, regrutuju, organiziraju, promoviraju svoje ideje i aktivnosti i prikupljaju sredstva, ali vremenom mogu koristiti IKT za napad, te povećati izvještavanje o nacionalnim planovima razvoja IKT ratnih i obavještajnih aktivnosti, te u političke svrhe.

Zabrinutost je također porasla za pojedince, grupe ili organizacije, uključujući kriminalne organizacije uključene u medijaciju. Agenti, odnosno posrednici, su zaduženi za provođenje ometajućih mrežnih aktivnosti u ime drugih, a sve zbog finansijske dobiti ili nekih drugih ličnih ciljeva, državnim i nedržavnim akterima mogu pružiti niz zlonamjernih usluga. Sve veća upotreba IKT-a u kritičnoj infrastrukturi donosi nove mogućnosti za ranjivosti i kršenja, kao i sve veću upotrebu mobilnih komunikacionih uređaja i usluga zasnovanih na webu. Zemlje su takođe zabrinute da bi lanci snabdevanja IKT mogli biti pogođeni, a to može da utiče da utiče na normalnu, sigurnu i pouzdanu upotrebu IKT. Zlonamjerna upotreba IKT uništava povjerenje u proizvode i usluge, uništava povjerenje trgovine i utiču na nacionalnu bezbednost. Različiti nivoi IKT sposobnosti i sigurnosti u različitim zemljama povećavaju ranjivost globalnih mreža.

Razlike u nacionalnim zakonima i praksa može otežati postizanje sigurnog i otpornog digitalnog okruženja. Dok su mnoge zemlje poput Sjedinjenih Država i Ujedinjenog Kraljevstva zabrinute za sigurnost mreže trošeći milione na ovo i brzo usvajanje zakona, drugi nemaju ni osnovnu IT infrastrukturu, a kamoli strategiju da se s tim nose cyber pretnje koje utiču i/ili potiču sa njegove teritorije. S obzirom na visoku cijenu cyber sigurnosti (procjenjuje se na 3-10% budžeta), nejasno je koliko brzo će manje razvijene zemlje moći prikupiti potrebna sredstva za izgradnju tehničkih kapaciteta za cyber bezbjednost (Buckland, Schreier & Winkler, 2010).

2.3.Izazovi demokratskog nadzora nad cyber sigurnosti

Izgradnja modernog, transparentnog društva zahtijeva uspostavljanje prave ravnoteže između potrebe za zaštitom političkog i ustavnog poretka i princip vladavine prava koji poštuje osnovna prava i slobode građana (Masleša, 2001). Zato što je cyber sigurnost relativno nova, u mnogim zemljama postavlja se pitanje bezbjednosnih aktera, demokratskog nadzora, u vidu

ombudsmana, skupštinskih odbora i drugih specijalizovanih agencija. Mnogo je faktora koji pogoršavaju demokratski izazov, nadzor, u vezi sa mjerama kibernetičke sigurnosti.

Ženevski centar za demokratiju kontrola oružanih snaga (dcaF) identificirala je nekoliko izazova (Buckland, Schreier i Winkler, 2010.), a o njima ćemo reći nešto u nastavku.

Prvo, složenost mreže pogoršava probleme praćenja te u cyber bezbjednost uključuje veliki broj različitih državnih, privatnih, međunarodnih i drugih nedržavnih aktera. Opet, veoma raznolik skup aktera uključenih u ono što se može učiniti u širem smislu naziva cyber napadom. Sama složenost mreže za regulatore, kao što su parlamentarni odbori (obično sa ograničenim ovlaštenjima), otežavaju im praćenje relevantnih aktera i njihovo razumijevanje aktivnosti, ili čak zakonsko ovlaštenje da to učini.

Drugo, tehnička složenost pogoršava probleme kontrole jer visoko tehnička priroda izazova kibernetičke sigurnosti i kako se nositi s njima, a supervizori često nemaju potrebnu stručnost da ih razumiju. Javno-privatno partnerstvo se dalje pogoršava a problem je taj što se stvara rascjep između visoke plate i sofisticiranosti stručnjaka koji su uključeni u izvršenje instrukcija, odnosno oni su slabo plaćeni i slabo informisani.

Treće, pravna složenost pogoršava regulatorna pitanja. Cyber bezbjednost nas izlaže složenim pravnim pitanjima koja se odnose na privatnost i slobodu izražavanja, između ostalog. Ova složenost se dodatno povećava kroz javno-privatna partnerstva i povezana pravna pitanja u vezi sa odgovornošću i kontrolom. Drugi razlog za zabrinutost je da postoje napetost između zaštite privatnosti i poboljšane identifikacije i provjere identiteta korisnika. Istina je da zemlje i kompanije često bez adekvatnog demokratskog nadzora, prikupljaju i obrađuju velike količine radi vaše sigurnosti (i sigurnost kupaca).

Četvrto, heterogenost aktera pogoršava probleme kontrole. U većini slučajeva, regulatori su organizovani kao agencije ili organizacije sa sličnim funkcijama. Na primjer, parlamentarni odbor bi mogao da nadzire obavještajne službe i aktivnosti, oružane snage i pravosuđe.

Peto, pitanja nadzora pogoršavaju percepciju osnaživanja. Općenito govoreći, Državna agencija odgovorna je za svoj rad. Ovo ostavlja privatne partnere ovih agencija van kontrole.

Šesto, poremećaj odnosa principal-agent pogoršava regulatorne probleme (Buckland, B., & sur., 2010).

Postupci svakog državnog agenta povezani su lancem odgovornosti Principal agentu. Dakle, postoji niz odgovornosti i nadzora između demokratskih institucija (kao što su parlamenti) i pojedinaca ili institucija. Ovo je implementirano državnom direktivom. Iako se čini da su javne IT kompanije samo agenti države (Principal), ovaj odnos je često složeniji i dvosmisleniji jer velika količina asimetričnih informacija koje smanjuju transparentnost i ometaju efikasan rad mehanizma za praćenje. Moderno društvo postalo je nepovratno ovisno o informacijskim i komunikacijskim tehnologijama. Nažalost, pored brojnih prednosti novog proizvoda tehnologije, a njihovo sve veće usvajanje je praćeno nizom cyber prijetnji koje se razvijaju na brže, sofisticiranije i zlokobnije načine. Cyber prijetnje su danas jedan od najvećih problema u svijetu. U ovom članku predstavljamo pojam, lokaciju i ulogu kibernetičke sigurnosti u razvoju modernog društva.

GLAVA III

IZAZOVI MODERNOG DIGITALNOG SVIJETA

Danas je koncept privatnosti prisutan na internetu i u svakodnevnom životu, svuda. Također, danas je internet jedan od najvažnijih, ako ne i najvažniji, dio svakodnevnog života. Međutim, mnogi od nas još uvijek nisu svjesni potencijalnih opasnosti korištenja interneta, od lažnih izjava do ličnih podataka drugih ljudi, lažnih obećanja ili čak traženih finansijskih i drugih vrsta pomoći za uporne oblike zlostavljanja, psihološki uticaj na korisnike i slično. Digitalni svijet, ranije poznat kao virtuelni svijet, postao je dio stvarnosti koji se naziva stvarni svijet. Naše ponašanje u digitalnom svijetu je vrlo realno uticaj na stvarni svijet. Razne komunikacije, finansijske transakcije, informacije i učenje, zabava svih vrsta dio su naših svakodnevnih aktivnosti. Konzumiramo "u pokretu" koristeći lične ili laptop računare, pametne mobilne telefone, igraće konzole, smart TV i drugo, poznati kao pametni uređaji koji omogućavaju pristup internetu. A mi, korisnici raznih informacionih i komunikacionih sistema često se ponašamo naivno iako smo mnogo puta do sada upozoreni na moguće opasnosti.

Kako se pojavljuju nove opasnosti interneta, tako se pojavljuju i novi izazovi za njihovu prevenciju. Inženjeri informacionih tehnologija unapređuju postojeće i razvijaju ih. Novi oblici tehničke zaštite, ali bez potpune ili apsolutne zaštite, često je korisnik, odnosno ljudski element, ključni i najslabiji dio sigurnosti. Uvjerenje o tehničkoj zaštiti je nedovoljno, te osim edukacije korisnika, potrebno je i zakonski regulirati sankcije za prekršioce.

S razvojem digitalnog doba, uključujući i pojavu društvenih mreža i mobilnih uređaja aplikacije (pametni telefoni, društvene mreže, mobilne aplikacije itd.), protok informacija nesumnjivo donosi ogromne mogućnosti i prednosti današnjem životu, ali istovremeno, nove digitalne tehnologije otvaraju niz društvenih i etičkih pitanja. Informaciona i komunikacijska tehnologija (IKT) omogućava sve vrste informacija, koje predstavljaju najprodorniju tehnologiju opšte namjene koja je danas dostupna. Nova pitanja vezana za sigurnost na mreži, uključuju slučajeve zloupotreba IKT-a u obliku neželjenih podataka, krađe podataka, obavještajnih podataka, itd.

Zbog sve većeg zloupotrebe djece na internetu, Evropski parlament i Vijeće EU je dogovorila nova pravila EU o zaštiti podataka: Uredbu o zaštiti Obrada ličnih podataka i slobodan protok

takvih podataka Podaci (Opća uredba o zaštiti podataka) stupila je na snagu 24. maja 2016. godine, a Direktno primjenjiv na sve države članice EU od 25. maja 2018. U navedenim okolnostima djeca će moći koristiti određene internet usluge i Usluge koje daju lične podatke samo uz pristanak roditelja (Granica starosti je od 13 do 16 godina). Sveprisutnost interneta u svakodnevnom životu ljudi dovela je do pojave da virtuelni svijetovi sve više postaju dio stvarnog svijeta, odnosno postaju jasnije granice između virtualnog svijeta i stvarnog svijeta.

Internet sve više obuhvata postojeći stvarni svijet, a time i sve oblasti ljudskog života. Bez svakodnevne upotrebe interneta život postaje nezamisliv i nemoguć. moderno društvo u kojem se aktivnosti kreću iz stvarnog svijeta u virtualni svijet dozvoljava i ubrzani razvoj socijalnog inženjeringa, odnosno razvoj online prevara (Haley, 2011; Mitnick, Simon i Woz-Niack, 2002; Selma i Thibaut, 2018).

U početku se čini beznačajnim, a trud je mali, ali količina ličnih podataka, kao što je prilikom instaliranja manjih aplikacija, korištenjem društvenih aplikacija mreže, kupovina karata za kino na internetu, itd., može na kraju dovesti do materijalnog gubitka, ali i djelimičnog gubitka privatnosti.

Bezobzirno i rizično ponašanje korisnika informacionog sistema će ozbiljno uticati na cijeli sistem bezbjednosti informacija. Važnost znanja, ponašanje i svijest o sigurnosnim pitanjima između informacija i privatnih podataka, korisnici interneta prvo prepoznaju mrežni administratori i stručnjaci za sigurnost. Tek nakon toga su naučnici počeli da se bave ovim problemom. Koliko god se trudili, još uvijek postoji relativno malo završenih naučnih istraživanja u ovoj oblasti (Crossler et al., 2013; Kwang i Choo, 2011), od kojih se većina uglavnom bavi pitanjima kvaliteta i snage lozinke za korisnike računarskog sistema (Dell'Amico, Michiardi i Roudier, 2010; Kelley et al, 2012; Voyiatzis, Fidas, Serpanos i Avouris, 2011; Wanli, Campbell, Tran i Kleiman, 2010). Da, na primjer, nedavno istraživanje pokazalo je da većina korisnika procjene njegove jačine i kvaliteta lozinke su osrednje, sa samo 13,8% korisnika kao loše (Šolić, Očevćić i Blažević, 2015), ali je pitanje kako su stručnjaci procijenili svoje lozinke. Što se tiče studija u zemljama EU, glavni fokus je na identifikaciji rizičnih oblika ponašanja na mreži kod djece i adolescenata. Tokom rada sa njima rijetko se javlja u odrasloj dobi (nakon 21 godine) da izgleda zainteresovano. Odrasli kao korisnici interneta javljaju se prvenstveno u kontekstu zaštite djece.

Razumijevanje opasnih situacija je izuzetno važan aspekt online sigurnosti jer sigurnost se nikada ne može u potpunosti postići, ali je također moguća identifikacija rizika ako se otkriju

na vrijeme, njihov utjecaj se može smanjiti. Stoga je tako Prikupljanje podataka od samih korisnika je prvi korak u razvoju algoritama sigurnost na internetu, što je i glavna svrha tih istraživanja u cilju zaštite od cyber krimiala.

3.1. Informacijska sigurnost

Državne izvršne agencije drže visoko povjerljive informacije političke, vojne, ekonomske i druge prirode koje mogu biti od interesa za neke strane obavještajne agencije, strane privredne subjekte, te organizirani kriminal i terorističke organizacije. Informaciona sigurnost uključuje pet aspekata, a to su sigurnosna provjera, fizičku sigurnost, sigurnost podataka, sigurnost informacionog sistema i sigurnost poslovne saradnje. Odgovornost Ureda vijeća za nacionalnu sigurnost (UVNS) je uspostavljanje i implementaciju mjera i standarda informacione sigurnosti. S razvojem nauke i tehnologije, sve više podataka kritičnih za nacionalnu sigurnost pohranjuje se u informacione sisteme organa državne uprave ili se razmjenjuje putem informacionih i komunikacionih kanala.

Za otkrivanje i spriječavanje neovlašćenog pristupa zaštićenim informaciono-komunikacionim sistemima državnih organa i odavanje poverljivih informacija zadužena je Sigurnosno-obavještajna agencija (SOA). Elektronski napadi i prijetnje informacijskoj sigurnosti postaju sve složeniji, a da bi im se suprotstavili potrebno je kontinuirano učenje, praćenje trendova i inovativna rješenja.

Zbog visoke razine informatičkog znanja i iskustva potencijalnih cyber napadača te relativno širokog kruga istomišljenika sposobnih za takve napade, ne može se zanemariti mogućnost da sve države budu suočene sa cyber prijetnjama. Informacijska sigurnost također je vrlo važna za sve subjekte, a posebno za one koji koriste moderne visoke tehnologije. Tehničke tajne mogu biti predmet interesovanja raznih pojedinaca, organizacija i pojedinačnih zemalja.

Odluka Vijeća o sigurnosti povjerljivih podataka o zaštiti povjerljivih podataka (EUCI) propisuje da će komunikacijski i informacioni sistemi rukovati povjerljivim podacima EU u skladu sa konceptom informacione sigurnosti.

Informacionu sigurnost u oblasti komunikacija i informacionih sistema možemo definisati kao povjerenje da će takvi sistemi zaštititi podatke koje obrađuju i obavljati svoju ulogu kada je to potrebno i pod kontrolom legitimnih korisnika. Efikasna sigurnost informacija mora

osigurati odgovarajuće nivoe povjerljivosti, integriteta, pristupačnosti, neospornosti i autentičnosti. Sigurnost informacija, poznata i kao sigurnost podataka, štiti poslovne knjige, lične podatke ili intelektualnu svojinu.

Informacije se mogu pohraniti na više mjesta i pristupiti im na više načina. Informacije se pohranjuju u dokumentima, prenosivim diskovima, laptopima, serverima, ličnim uređajima i drugim upravljanim uređajima. Ove informacije su vrijedne za pojedinačne korisnike i cijelu poslovnu organizaciju. Stoga ih treba pravilno čuvati. Proces zaštite informacija naziva se informacijska sigurnost. Informaciona sigurnost je krovni izraz za način na koji organizacije i pojedinci štite svoju vrijednu imovinu, bilo da su poslovni podaci, intelektualna svojina ili na neki drugi način. Podaci se mogu pohraniti na mnogo načina – na primjer, to mogu biti fizički dokumenti na serverima i tvrdim diskovima, u oblaku ili na privatnim uređajima.

Drugim riječima, sigurnost informacija se može opisati kao sprječavanje neovlaštenog pristupa ili izmjene podataka tokom procesa organiziranja ili migracije s jednog uređaja na drugi. Informacije mogu biti: biometrija, profili na društvenim mrežama, podaci mobilnog telefona, itd. Iz očiglednih razloga, postoje razlike u načinu na koji se informacije čuvaju; papirni dokumenti ne mogu biti zaštićeni na isti način kao digitalni dokumenti. Zaštitit ćete ih tako što ćete ih pohraniti u zatvorene ladice kojima samo ovlašteni zaposleni mogu pristupiti, a digitalne datoteke zahtijevaju potpuno drugačiji tip zaštite (kao što je kontrola pristupa kako bi se osiguralo da im samo ovlašteni korisnici mogu pristupiti).

Opšti princip ostaje isti – kontrola ko može vidjeti informacije je implementirana, ali pristup je drugačiji. Informaciona sigurnost se općenito odnosi na praksu zaštite ličnih podataka i pristup toj sigurnosnoj praksi. Podaci, uključujući lične informacije ili informacije visoke vrijednosti, moraju biti povjerljivi i svaki mogući neovlašteni pristup mora biti zabranjen. Što se tiče integriteta, pohranjene informacije treba čuvati u izvornom obliku i zaštititi od bilo kakve izmjene od strane neovlaštenih korisnika.

Konačno, važno je da pohranjenim podacima u svakom trenutku može pristupiti samo ovlašteno osoblje. DOS napadi, odnosno napadi koji uključuju uskraćivanje usluge, upravo su o tome u pitanju. Da bi osigurale efektivno poslovanje i sigurnost informacija, organizacije uvode širok spektar politika kao što su: politike kontrole pristupa, politike lozinki i podrška podataka i operativni planovi. Mjere također mogu uključivati otkrivanje cyber krađe i sistemski i regulatorni nadzor.

Bilo da se radi o specifičnoj mrežnoj sigurnosti ili sigurnosti informacija općenito, postoje tri glavne osnove mrežne sigurnosti koje morate razumjeti, a to su

- Ljudi: Zaposleni su ljudi koji svakodnevno dolaze u kontakt s osjetljivim informacijama i za organizacije je od ključne važnosti da ih educiraju o rizicima da ostanu sigurni.
- Proces: Organizacije treba da dokumentuju korake koji zaposleni preduzimaju da bi osigurali bezbjednost. Ovo uključuje definisanje uloga i odgovornosti za aktivnosti zaštite podataka.
- Tehnologija: Postoje mnogi elementi odbrambene tehnologije koje organizacije mogu implementirati kao odgovor na prijetnje, kao što su antivirusni softver, prava pristupa i enkripcija podataka.

Kako cyber prijetnje postaju sve sofisticiranije, organizacije i pojedinci bi trebali koristiti vještine kako bi koristili najbolje informacije i resurse koji ih mogu zaštititi. Neki stručni savjeti su uvijek instalirajte antivirusni softver na sve uređaje, koristite sigurni zaštitni zid za dodatnu zaštitu između vaše lokalne mreže i interneta, osigurajte da je IT osoblje uvijek u toku sa najnovijim ažuriranjima softvera i zakrpama, omogućite obuku zaposlenima da prepoznaju sumnjive mejlove, linkove ili prijetnje, često pravite sigurnosne kopije kako biste osigurali brzu reakciju na gubitak podataka u slučaju ransomware napada.

3.2.Ponašanje djece i mladih na internetu

Nedavno je tehnologija postala sastavni dio našeg svakodnevnog života, te je intenzivan razvoj moderne tehnologije imao je veliki uticaj na gotovo sva polja u našem životu. Bez interneta i druge elektronike svakodnevni život je gotovo nezamisliv. Činjenica je da virtuelni svijet sve više postaje dio stvarnog svijeta, te jasna granica između "online" i "offline" stvarnosti nestaje (Velky i Romstein, 2018).

Internet je izuzetno atraktivan zbog brojnih mogućnosti koje nudi djeci i mladima, jer im olakšava komunikaciju i održavaju odnose i prijateljstva sa svojim vršnjacima, omogućava im pristup obrazovnim sadržajima, resursima za učenje i prostor za kreativnost, građanski aktivizam i dr. (Cassidy, Faucher i Jackson 2013; Pregrad, Tomić-Latinac, Mikulić i Šeparović, 2010).

U tipičnom radnom danu mladi provode dva do tri sata na mreži (navedeno sa 32,2%) i vikendomm, dok je 46,3% učenika je izjavilo da provode više od 4 sata na internetu. Djevojke provode visše vremena na internetu, čak do 32,4% na uobičajen radni dan, gdje to traje 4 sata, a u nekim slučajevima čak i više.

S obzirom na sve veći značaj i prisutnost elektronskih medija u životima ljudi, nije iznenađujuće što imaju veliki uticaj na roditeljstvo, rast i socijalizaciju. Međutim, unatoč brojnim prednostima, postoje i razni "novi" online rizici. Razvoj digitalnog doba donio je mnoge mogućnosti i prednosti, a utjecao je i na nastanak serijala socijalna i etička pitanja. Vejmelka, Strabić i Jazvo (2017) ističu tu izloženost te navode da online rizici mogu imati dugoročne i snažne negativne efekte na sve ljude, posebno djecu i adolescenate, te naglašavaju važnost razumijevanja interakcija sa mladima u virtuelnom okruženju koji je osmišljen da dizajnira odgovarajuće i pravovremene strategije prevencije i otkrivanje i rješavanje rizičnog ponašanja na mreži. Rizično ponašanje se definira kao opasnost ili negativan ishod u području „zdravlje djece“. Psihosocijalno i kognitivno funkcioniranje u odrasloj dobi, odnosno za djecu koja pokazuju rizično ponašanje, za iste postoji rizik od manje odgovornosti zbog punoljetnosti. Prema ovoj definiciji, rizik za djecau i tinejdžere koji se nalaze u virtuelnom okruženju mogu se definirati kao štetne aktivnosti, opasnosti ili negativni ishodi djece i mladih u virtuelnom okruženju, ili uz pomoć savremene tehnologije. Mnoga istraživanja su se fokusirala na rizična ponašanja djece i adolescenata, ali postoje i mnoga neslaganja među istraživačima. Razlog tome je konceptualizacija i mjerenje različitih fenomena rizičnog ponašanja djece i adolescenata u virtuelnim okruženjima (npr. ovisnost o internetu, elektronsko nasilje i slično).

Danas su prisutna opasna ponašanja i aktivnosti na mreži za mlade koji provode vrijeme na internetu. Stvarno okruženje se vezuje za teoriju svakodnevnih aktivnosti adaptacije u kontekstu virtuelnog okruženja. Uz svakodnevnu upotrebu interneta, tinejdžeri su češće izloženi nasilju zbog ponašanja u virtuelnom području. Kada se akumuliraju, dolazi do društveno neprihvatljivog ponašanja. Što se više vremena provodi u određenim online aktivnostima, to je veća učestalost učešća u elektronskom nasilju, a nedostatak jasno definisanih pravila ponašanja pri korišćenju interneta može dovesti do dezinhibicije motivisanih „nasilnika“ koji mogu da ohrabre te se osoba se upušta u elektronsko nasilje, pri čemu virtuelni prostor postaje novo okruženje za ispoljavanje neadekvatnih i opasnih obrazaca ponašanja (Vejmelka et al., 2017).

Kada su u pitanju djeca i tinejdžeri koji pokazuju rizično ponašanje u virtuelnim okruženjima, posljednjih godina u literaturi se mnogo raspravljalo o elektronskom okruženju. Nasilje, tema i oslanjanje na internet je vruća tema posljednjih 20 godina (Mihajlov i Vejmelka, 2017.). Elektronsko nasilje Willard (2004) definira kao slanje ili objavljivanje štetnog ili uvrijedljivog sadržaja putem interneta ili drugog digitalnog sadržaja tehnologije.

Kronično nasilje dovodi do kriterija klasičnog vršnjačkog nasilja, kao što su ponovljeno i namjerno nanošenje štete drugima putem digitalne tehnologije i elektronike. Tokunaga (2010) koristi širu definiciju elektronskog nasilja, tvrdeći da je elektronsko nasilje svako ometanje moderne tehnologije u kojoj komunikacija između pojedinaca ili grupa uključuje informacije uvredljive ili neprijateljske prirode, s namjerom da izazove neugodnost ili štetu drugima. Ovisnost o internetu opisuje se kao stanje u kojem pojedinac gubi kontrolu koristi internet, pa ga i dalje prekomjerno koristi do te mjere da to doživi i dođe do problematičnih ishoda koji su negativno uticali na njegov život (Weinstein, Curtis Feder, Rosenberg i Dannon, 2014).

Problematično korištenje interneta ili ovisnost o internetu definira se kao pretjerana ili loše kontrolirana preokupacija, impulsivnost ili ponašanja koja dovode do stresa i smanjenog učinka. Riječ "ovisnost" prihvatili su istraživači i drugi stručnjaci u ovoj oblasti. Inače, ovisnost o internetu još uvijek nije uključena u dijagnozu i statistiku. Postojala je živa debata o uključivanju ovisnosti o internetu u službene klasifikacije bolesti, te su potrebna daljnja istraživanja u ovoj oblasti (Petry et al., 2014). U literaturi se ovisnost o internetu najčešće svrstava u tri tipa, uključujući ovisnost o video igricama, ovisnost o seksu i ovisnost o internet povezanosti.

Govoreći o ovisnosti o online igrama, ispostavilo se da je prvobitna motivacija za igranje video igrica bila zabava, bijeg od problema i virtuelna prijateljstva i kao prva očigledna štetna posljedica ekscesa utvrđene su promjene raspoloženja, gubitak kontrole, apstinencijalni sindrom i tendencije sukoba (King, Delfabbro, Griffiths & Gradisar, 2012). Neki od ostalih rizika s kojima se djeca i tinejdžeri suočavaju u virtuelnim svjetovima su regrutovanje djece i omladine radi razotkrivanja ili eksploatacije, komunikacija koja izaziva podjele, dopisivanje i zabavljanje sa strancima, izlaganje raznog neprimjerenog sadržaja (seks, nasilje, diskriminacija i mržnja), podsticanje na upotrebu psihoaktivnih supstanci, kockanje i slično. S obzirom na navedeno, djeca i adolescenti se smatraju posebno ranjivom grupom te je za njih korištenje interneta i virtualne komunikacije sastavni dio svakodnevnog života života, a često nisu svjesni rizika s kojima se suočavaju kada se približavaju internet interakciji i ponašanja

mladih ljudi u virtuelnim okruženjima su u fokusu mnogih istraživači. Što se tiče nasilnih iskustava, prikupljeni podaci odražavaju prethodna iskustva. Djeca i adolescenti koji su doživjeli nasilje, tako da je 32,3% doživjelo nasilje ponašanje, 43,5% iskusilo nasilničko ponašanje, 9,7% ovo je nasilje. Od sada je jasan odnos, obično je to iskustvo vršnjačkog nasilja (43,5%), to jeste otprilike 1 od 10 djece doživljava roditeljsko nasilje, 6,5% djece je bilo nasilno prema roditeljima, a 3,2% prema braći i sestrama. Što se tiče iskustava vršnjačkog nasilja, svako četvrto djece doživjelo je cyberbullying (25,8%), a slični rezultati su dobijeni i za iskustvo fizičkog nasilja (27,4%) i emocionalnog nasilja (21,0%).

Kada pišemo o današnjim generacijama djece, nije lako zastati i utvrditi kako su generacije koje su danas odrasle, generacije sa ekranima osjetljivim na dodir i kako se način na koji su djeca odrastala tokom decenija promijenio od doba bez ekrana do djece.

Prave posljedice ovih promjena nisu u potpunosti istražene, a sve veći broj istraživanja ispituje uticaj ekrana i virtuelnih života na predškolce. U evropskim zemljama posljednjih godina se povećao broj djece mlađe od 9 godina koja koriste internet, a djeca u mlađoj dobi koriste različite sadržaje. Djeca mlađa od 9 godina, uz podršku roditelja, koriste internet za niz aktivnosti, kao što su gledanje videa, igranje igrica, traženje informacija, učenje ili druženje. Na primjer, jedno istraživanje pokazalo je da gotovo polovina austrijske djece uzrasta od 3 do 6 godina redovno koristi internet. Internet je nesumnjivo donio mnoge mogućnosti, pružajući platformu za učenje, razvijanje interesovanja, izvore informacija o raznim temama, razvijanje identiteta, povezivanje s vršnjacima i olakšavanje komunikacije s drugima. Istovremeno, važno je shvatiti da internet nosi i određene rizike. Najistaknutiji od njih je, naravno, elektronsko vršnjačko nasilje ili cyber maltretiranje. Elektronsko vršnjačko nasilje uključuje različita ponašanja koja se dešavaju preko interneta, mobilnih telefona i drugih elektronskih uređaja putem kojih pojedinac ili grupa pokušava da naudi nekome. Elektronsko vršnjačko nasilje može uključivati širenje neugodnih informacija (bilo istinitih ili lažnih) o pojedincima, članovima njihovih porodica i/ili prijateljima, širenje povjerljivih informacija samo za video.

Prevalencija ovih ponašanja koja je otkrila da je svaki peti tinejdžer bio izložen uvredljivim informacijama ili komentarima putem Facebooka, a svaki šesti je čak dobio prijetnje. Značajan broj djece i mladih doživio je provalu u njihov imidž (16%), širenje laži (11%), blokiranje ili izbacivanje grupa (11%) ili ohrabrivanje drugih da govore loše o njima (7%).

Svaki šesti je primio neželjene seksualno eksplicitne poruke. Ova ponašanja imaju mnoge posljedice koje su često teže od posljedica vršnjačkog nasilja koje se događa licem u lice.

3.3.Novi internet rizici

Seksting je slanje ili primanje ili prosljeđivanje seksualno sugestivnog ili eksplicitnog sadržaja, uključujući pisane poruke, fotografije i video zapise pojedinaca ili drugih, putem mobilnog telefona ili interneta. Studija poliklinike iz 2019. godine pokazala je da je čak 60% mladih dobilo seksualno sugestivne ili eksplicitne poruke, a više od polovice takve fotografije ili video zapise. Čak 46% mladih dobilo je takav sadržaj bez pitanja. Također je važno napomenuti da najmanje 40% mladih ponekad reaguje na ovu vrstu sadržaja. Samo 6% mladih priznalo je da je slalo takav sadržaj, dok je 17% reklo da je ponovo objavilo takve fotografije i video zapise bez pristanka poznanika. Seksualna iznuda je oblik iznude koju počinitelji provode na internetu i uključuje neki oblik prijetnje, obično postavljanje ili prosljeđivanje seksualno eksplicitnih slika žrtve ako se žrtva ni na koji način ne upušta u daljnju seksualnu aktivnost. Istraživanje iz 2019. pokazalo je da je 13% mladih slalo takve fotografije pod nagovorom, 4% iz prisile, više od 5% na zahtjev znatno starijih odraslih osoba (koji su mislili da je to potpuno dobrovoljno), a 14% mladih seksista je pod uticajem droga. Ove brojke pokazuju da su se rizici na internetu mijenjali tokom godina i važno je biti svjestan ovih rizika kako bismo znali kako pravovremeno odgovoriti.

Dok je 2013. godine 34 % djece i tinejdžera reklo da bi prihvatilo zahtjeve za prijateljstvo od stranaca barem ponekad, istraživanje iz 2019. pokazalo je da 68 posto tinejdžera komunicira sa strancima dvostruko više. Osim toga, 2013. godine, 21% djece i mladih je reklo da bi vjerovatno ili definitivno upoznalo strance koje su upoznali putem Facebooka, od kojih je 8% reklo da bi, a istraživanje iz 2019. pokazalo je da čak 35% mladih ljudi ljudi upoznaje ljude na društvenim mrežama.

Ove brojke upućuju na to da je sve više mladih ljudi spremnih na rizične aktivnosti bez znanja odraslih. Strano istraživanje pokazuje da 97% roditelja barem jednom dnevno provjerava društvene mreže, 25% je na njima cijeli dan, a naše istraživanje iz 2017. pokazuje da svaki roditelj provede više od dva sata dnevno za svojim mobilnim telefonom, četiri po jedan u svakom roditelju. vikendom provede dodatna dva sata dnevno za kompjuterom. Sve veći broj smetnji odvlači nam pažnju od djece i tinejdžera, a istraživanja pokazuju da trend modernih

roditelja koji prekomjerno koriste mobilne uređaje ili obraćaju više pažnje na tehnologiju od djece utječe na stilove privrženosti i rast djece.

Dakle, prije nego pokušamo promijeniti svoju djecu, važno je da se zapitamo jesmo li im uzor, kako i koliko vremena provodimo pred ekranima, gledamo li svaku poruku ili e-mail koji dobijemo, da li svaki put kada zazvoni telefon, prekinuti razgovor sa svojim djetetom obavještenjem ili pozivnicom. Strana istraživanja također pokazuju da roditelji godišnje objave u prosjeku 195 slika svoje djece. Poliklinička anketa iz 2017. pokazala je da je 65 posto odraslih objavilo fotografiju predškolca na društvenim mrežama. Dokle god objavljujemo slike naše djece na društvenim mrežama, teško je uvjeriti našu djecu jer ih upućujemo da to ne rade, bilo da objavljuju svoje ili nečije slike. Roditelji i druge odrasle osobe koje su važne za živote njihove djece neizostavni su saveznici u suočavanju s izazovima odrastanja u virtuelnom svijetu.

Međutim, rad sa roditeljima čini da se osjećaju da često nerado učestvuju u online životima svoje djece, govoreći da njihova djeca razumiju modernu tehnologiju bolje od njih i da ne znaju kako doprinijeti njihovoj sigurnosti. Kao rezultat toga, istraživanje iz 2013. pokazalo je da je čak 78% djece i tinejdžera reklo da ne postoje pravila za njihovo korištenje društvenih mreža, a 2017. godine četvrtina roditelja predškolaca izjavila je da nikada ne postavljaju pravila. Ove vrtoglavo brze promjene se dešavaju na takav način da većina roditelja s vremenom više ne može pratiti njih, čak i ako su voljni ostati uključeni u virtuelne živote svoje djece. Zapravo, djeca danas znaju više o korištenju tehnologije, ali znati kako koristiti internet ne znači nužno znati kako ga koristiti na način koji je siguran i odgovoran za nas i druge.

Današnje generacije djece prve su koje odrastaju koristeći informacione i komunikacione tehnologije od malih nogu. Zbog toga je njihov odnos prema tehnologiji vrlo intuitivan i spontan, oni su sposobni da brže prevladaju promjene i od njih možemo mnogo naučiti. Istovremeno, budući da nemaju iskustvo odrastanja bez moderne tehnologije, nedostaje im potrebna kritika i potrebna im je vodstvo i podrška. Stoga ohrabrujemo roditelje da pokažu interesovanje za online živote svoje djece na nenametljiv, ali podržavajući način. S obzirom da 95% hrvatske djece i tinejdžera danas pristupa kompjuteru putem mobilnog telefona, jasno je da se ponašanje djece na internetu ne može u potpunosti kontrolirati. U skladu s tim je i rezultat brojnih studija koje pokazuju da je zapravo važnije usmjeravati, odnosno usmjeravati online ponašanje djece kroz dijalog i postavljanje pravila. U svim pitanjima, uključujući i

sigurnost djece na internetu, roditeljstvo se zasniva na povjerljivom i toplom odnosu između roditelja i djeteta.

Ovaj odnos stvara sigurno okruženje i povećava vjerovatnoću da će djeca tražiti savjet ili pomoć od svojih roditelja. Također je važno da roditelji budu svjesni znakova koji mogu ukazivati na to da njihovo dijete doživljava ili čini nasilje, te da su spremni da traže pomoć i podršku kada su u pitanju. Uvjerljivo, prema istraživanju iz 2019. godine, dok četvrtina tinejdžera većinu svog slobodnog vremena provodi na društvenim mrežama, manje od 5% bira društvene mreže kao svoju omiljenu aktivnost u slobodno vrijeme, što se nije promijenilo od istraživanja prije šest godina. danas, uprkos tome što njihovo ponašanje sugerira drugačije, i dalje radije biraju povezivanje s prijateljima u realnom vremenu, a ne u virtuelnom svijetu. Nadzor ovih dana nije u potpunosti izvodljiv, a studije pokazuju da ni on ne funkcionira.

Sva istraživanja i svakodnevna klinička praksa vraćaju nas na važnost odnosa i odnosa s djecom. U mladosti to znači, između ostalog, prepoznati da dijete nešto želi, čak i ako ne možemo zadovoljiti njegove želje, a u adolescenciji ćemo mladima pokazivati njihova interesovanja i dostupnost umjesto da postavljamo puno pitanja. Razgovaranje o nasilju otvoreno, te njegovanje brige, postavljanje granica, poštivanje i osnaživanje djece i mladih bez obzira na godine gledamo kao temeljne vrijednosti u roditeljstvu i odnosima s djecom za koju mi kao odrasli moramo čuti, viđanje i poštovanje neće biti njihovo.

Mitovi u koje mnogi mladi vjeruju

Mnogi mladi ljudi su uvjereni da u to ne sumnjaju, a neki od njih su dio razloga zašto ne reagiraju kada primjete cyberbullying, bilo da se to dešava njima ili njihovim vršnjacima. Evo nekih uobičajenih mitova koje čujemo od mladih ljudi u našem svakodnevnom radu o kojima vrijedi razgovarati:

Mit 1. Oni koji najviše pate od cyber maltretiranja to zaslužuju. Niko ne zaslužuje nasilje od bilo koga.

Mit 2: Nasilje na internetu se ne kažnjava, a počinioci se ionako ne mogu otkriti. Ako ono što govorimo ili radimo izvan naših virtuelnih života nije legalno, nezakonito je i na internetu. Osim toga, policija također ima svoje metode za pronalaženje sajber kriminalaca.

Mit 3. Nema smisla obraćati se odraslima jer se to dešava na mreži. Kao što odrasli mogu pomoći djeci i mladima u stvarnom životu, oni također mogu pomoći u elektronskom nasilju.

Mit 4. Na internetu se svi često vrijeđaju, što je normalno. U redu je šaliti se, ali ne ako nekoga uvrijedi i postane nasilan. Samo zato što se nešto čini uobičajenim ne znači da je normalno.

Mit 5. Ako primijetim da se cyber maltretiranje dešava drugim ljudima, ne mogu ništa učiniti. Uvijek se možemo odazvati – reći odraslima, nazvati nazvati stručne službe i pružiti podršku onima koji se susreću s tim. Problem je u tome što neke studije procjenjuju da čak 90% djece dozvoljava ili podržava nasilje na mreži ignorirajući neprikladno ponašanje vršnjaka na mreži.

Mit 6: Nasilje na internetu nije tako ozbiljno kao nasilje licem u lice. Nasilje na internetu ponekad može imati veće posljedice od nasilja licem u lice. Vršnjačko elektronsko nasilje koje stvara ovo karakterizira anonimnost počinitelja (mladi ljudi često ne znaju ko je to učinio i mogu biti sumnjičavi prema većini ljudi koje poznaju, signalizirajući odnos nepovjerenja i straha), svakodnevno 24 sata stalne izloženosti, 7 dana u sedmici. O tome svjedoči nedostatak nadzora odraslih, što može dovesti do nesigurnosti i anksioznosti kod žrtve, kao i smanjenog iskustva odgovornosti kod počinitelja.

Rečenice poput "isključi internet", "ignoriraj ih", "vrati ih", "nemoj se opterećivati time", "ako ne pošalješ ovakve slike bit ćeš dobro", osim što ne ispunjavaju njihove utješna namjera, povrijediti djecu i tinejdžere jer pokazuju nerazumijevanje i krivicu, više da pokušaju da se utješe usred bespomoćnosti ili ljutnje, ili samo da riješe problem, pomaže tinejdžerima da se obrate roditeljima i odraslima samo kada imaju problem Sve je manje ljudi.

GLAVA IV

SISTEM BORBI PROTIV CYBER PRIJETNJI

Kako se pojedinci i zajednice širom svijeta povezuju, druže i organiziraju putem cyber prostora, to je postalo definišuća karakteristika modernog života. Od 2000. do 2010. broj korisnika interneta i najšire mreže cyber prostora povećao se sa 360 miliona na 2 milijarde. Svo domaće i međunarodno poslovanje se već zasniva na trgovini robom i uslugama, što se danas može obaviti za nekoliko sekundi jer je cyber prostor postao inkubator za nove poslovne forme, naučna i tehnološka dostignuća, širenje informacija i nove društvene mreže.Stoga je cyber prostor danas ključan za svjetsku ekonomiju i poslovanje.

4.1. Internet kriminal

Prema Enciklopediji Britannica, cyber rat predstavlja rat koji vode kompjuteri i mreže koje ih povezuju. Sprovode ga zemlje ili drugi subjekti u kojima učestvuju protiv drugih zemalja. Cyber ratovanje se najčešće vodi protiv vladinih i vojnih mreža kako bi se spriječilo, ometalo ili spriječilo njihovo korištenje. Cyber ratovanje ne treba poistovijetiti sa terorističkom eksploatacijom cyber prostora, cyber špijunažom i cyber kriminalom. Iako se slične taktike koriste u sva četiri oblika operacija, bilo bi pogrešno sve ih definirati kao radnje cyber ratovanja. Neke zemlje koje su vodile cyber rat se takođe mogu baviti destruktivnim aktivnostima kao što je cyber špijunaža, ali te aktivnosti same po sebi ne predstavljaju cyber rat. Cyber ratovanje se često poistovjećuje sa informacionim ratovanjem. Informacijski rat se odnosi na radnje koje se poduzimaju kako bi se stekla informacijska prednost utjecanjem na informacije i procese protivnika. Sistemi zasnovani na informacijama i računarskim mrežama, istovremeno štite i sopstvene informacije, procese zasnovane na tim informacijama, informacione sisteme i računarske mreže. Stoga se može reći da je cyber rat dio informacionog ratovanja (drugi dio je kao što je propagandni rat, psihološki rat, itd.). Informacioni rat znači da je to rat koji vodi informaciona tehnologija, a skoro svaki savremeni rat vodi informaciona tehnologija, o informacionom ratu nema smisla govoriti. Primjer cyber ratovanja je takozvani prvi cyber rat (Web War 1), u kojem je DDoS napao estonsku vladu, ministarstva, medije, banke i kompanije, što je dovelo do isključenja ovih subjekata sa interneta na neko vrijeme, kao i ruskih servera koje koriste brojne gruzijske vladine agencije,

mediji i komercijalni subjekti koji rade istovremeno s ruskim vojnim operacijama protiv Gruzije.

4.2. Internetski rat

Pored prva dva pojma, postoji i pojam cyber kriminal, koji se definiše kao zločini počinjeni korišćenjem računarske tehnologije i u cyber prostoru. U vezi sa pojmom „internet crime“, uključujući prevare u online bankarstvu i prevare s kreditnim karticama, možemo reći se da je to rastući globalni sektor organiziranog kriminala s godišnjom stopom rasta od oko 40% i trenutnim prihodom od oko 100 milijardi dolara. Treba naglasiti da pojam cyber kriminal treba da uključuje samo krivična djela koja se odnose na upotrebu računara ili računarskih mreža kada su povezani sa prirodom zločina, a ne sa svim zločinima u kojima se računar i njegovi povezani periferni uređaji na neki način pojavljuju kao sredstvo izvršenja. Na primjer, krivotvorenje valute nije cyber kriminal, bez obzira na to da li počinitelj koristi kompjutersku tehnologiju da krivotvori valutu.

4.3. Kako se boriti protiv cyber kriminala

Da bismo se osigurali od cyber napada (špijunaža, terorizam, rat, kriminal), potrebno je da poduzeti određene korake kako bi zaštitili podatke koji se nalaze u našim računarima i sve ono što radimo koristeći internet, te napraviti zaštitu od mogućih cyber-upada u naš računar, pokušaja preuzimanja podataka ili kontrole nad uređajem, od strane raznih vrsta specijaliziranih i dobro obučenih cyber- kriminalaca. Tom prilikom kriminalci koriste određene štetne programe kako bi neopaženo pristupili našim računarima.

Uvođenjem takzvane cyber-etike u život ljudi bit će preventiva protiv cyber kriminala, jer će doprinijeti njihovoj kulturi korištenja cyber-prostora kroz obrazovne i popularno-znanstvene projekte (takav program je pozitivno djelovao u Nigeriji). S naglim širenjem cyber kriminala, preventivne mjere usmjerene prema pojedincima kao što su anti-kriminalizacija, propaganda protiv zlostavljanja i anti-phishing, praksa oblikovanja negativnog stava prema zločinima i otkrivanje odgovornosti za počinjenje cyber kriminala dobivaju na važnosti. Poboljšanje društva kao protupotez za izostavljanje kriminalnih aktera koji izazivaju pozitivan ili neutralan stav prema cyber kriminalitetu treba biti usmjereno prema boljem životu, jer što je viši standard, to je niža razina cyber kriminala. Poduzimanje individualiziranih mjera za

sprječavanje ljudi koji su skloni počiniti cyber kriminal spriječit će takve napade čak i prije nego što se dogode (s prijetnjama cyber iznuđivanja i ransomwarea, takve akcije dobivaju na važnosti). Za borbu protiv cyber kriminala, posebni programi su smanjivanje viktimizacije u području cyber sigurnosti poticanjem zaštitnog stava osoba koje mogu postati žrtve. Put izrade takvih programa dovest će do pada aktivnosti cyber kriminala. U preventivnom procesu trebaju sudjelovati posebna javna tijela i nevladine organizacije. Sveobuhvatne preventivne mjere protiv cyber kriminala koje se približavaju pojedincu na međunarodnoj razini omogućit će osmišljavanje specifičnih pilot-programa za individualiziranu prevenciju.[20]

Kako bi se zaštitili od cyber napada, potrebno je koristiti određene taktičke, organizacijske, tehnološko-softverske i tehničke mjere. Neke od najvažnijih mjera ćemo navesti u nastavku:

- potrebno je da se svi informišemo o mjerema sigurnosti na internetu,
- primjena sigurnosnih savjeta na sve oblike internet komunikacije (računari, mobiteli i dr.),
- postavljanje osnovnih zaštitita na računarima i drugim uređajima protiv zlonamjernih softvera (kao što su virusi i računarski špijuni (spyware),
- lične podatke, kao i podatke klijenata, te i internet transkacije potrebno je veoma dobro zaštiti kako bi bile sigurne,
- napraviti politiku i načine upotrebe računara i drugih uređaja unutar organizacije, te o tome obavijestiti sve članove i istu uvrstiti u lične ugovore o radu,
- pratiti upotrebu intertneta od strane članova organizacije.

Stalno jačanje specijaliziranih jedinica, odnosno timova, za borbu protiv cyber kriminala trebalo bi biti strateški prioritet. Da bi se to sprovelo na dobar način, relevantni organi trebaju da razmotre sljedeće akcije:

- Uspostaviti – tamo gdje to još uvijek nije učinjeno – specijalizirane jedinice za cyber kriminal u okviru kriminalističke policije,
- tačno ustrojstvo i funkcije trebaju biti rezultat pomne analize potreba i zasnovani na zakonu.

- Preispitati funkcije i osiguravanje resursa specijaliziranih jedinica, na redovnoj osnovi,

[20] Veresha, R. (2018). PREVENTIVNE MJERE PROTIV RAČUNALNOG KRIMINALA: PRIBLIŽAVANJE POJEDINCU. Informatologia, 51 (3-4), 189-199. https://doi.org/10.32914/i.51.3-4.7 (4.3.2023.)

- to bi trebalo omogućiti prilagodbe i time odgovoriti na nove izazove i veće zahtjeve.
- Olakšati saradnju i razmjenu dobrih praksi između specijaliziranih jedinica,
- na regionalnoj i međunarodnoj razini.
- Unaprijediti procedure za istrage kibernetičkog kriminala i postupanje s elektronskim dokazima. Ispitati i razmotriti provedbu državnih i međunarodnih standarda i dobrih praksi u ovom smislu,
- razmotriti korištenje Vodiča o elektronskim dokazima koji je razvijen u okviru CyberCrime@IPA projekta.[21]

4.4. Kako se zaštiti protiv cyber kriminala (štetnih programa)

Prilikom cyber napada kriminalci koriste određene štetne programe kako bi neopaženo pristupili našim računarima. O takvim programima i načinima zaštite od njihovog štetnog djelovanja reći ćemo nešto u nastavku rada.

4.4.1. Malware

Malware je zajednički naziv za štetne ili maliciozne programe koje cyber-kriminalci koriste kako bi pristupili tuđim računarima. Takvi programi su obično skriveni u prilozima ili besplatnom sadržaju. Koriste se za niz nezakonitih radnji, kao što su krađa ličnih podataka, brisanje ili oštećivanje podataka, stvaranje **botnet** mreža (mreža zaraženih računara) i zaobilaženje sigurnosnih programa. Postoji cijeli niz različitih štetnih programa, a ovom prilikom ćemo se pozabaviti virusima, trojancima, špijunskim programima (spyware), reklamnim programima (adware) i programima za zastrašivanje (scareware).[22]

4.4.1.1. Virusi/Trojanci

Virus je program koji se može reproducirati i koji često sa sobom donosi štetne programe, koji mogu naštetiti datotekama i programima na vašim računarima. Nadalje, virusi se koriste za praćenje svega što radite na računarima, te omogućavaju nedozvoljen i potencijalno štetan pristup vašim personalnim računarima. Većina korisnika interneta svjesna je opasnosti koju donose virusi, a zaštita je moguća zahvaljujući različitim antivirusnim programima i firewall-om (vatrozidom). Međutim, osobe koje stvaraju viruse, neprekidno pronalaze nove načine širenja virusa na vaše računare. Stoga je neophodno biti veoma oprezan tokom rada na internetu, preuzimanja različitih sadržaja i sl.

[21] https://rm.coe.int/16802f6a44 (4.2.2023.)
[22] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (5.2.2023.)

Na internetu vas često zatrpavaju zahtjevima za preuzimanjem različitih sadržaja, uključujući pozadine za radnu površinu (wallpapers), screensavere i widgete. Odlučite li se na preuzimanje takvih sadržaja, morate znati da, u tom slučaju, možda preuzimate trojanca. Kao što i sam naziv govori, trojanac je štetni program koji imitira da je nešto što nije i u sebi sadrži skriveni program, čija je svrha činjenje štete. Svojim djelovanjem trojanac na računaru može napraviti različite vrste štete: izbrisati ili presnimiti podatke na računaru, snimiti udarce po tastaturi kako bi pristupili vašim ličnim podacima, deaktivirati vatrozid (firewall) i antivirusni program i instalirati druge viruse.

Kako prepoznati virus/trojanca?

Ako je računar zaražen virusom/trojancem, primijetit ćete da se računar ponaša neuobičajeno, muzika se sama uključuje, na zaslonu računara se pojavljuju poruke ili skočni prozori, datoteke su promijenjene ili izbrisane, tvrdi disk je oštećen ili izbrisan, računar je spor ili uopće ne reaguje.

Kako izbjeći viruse/trojance?

Neophodne mjere zaštite kako bi se izbjegli virusi i trojanci su:

- na računar instalirati antivirusni program/program protiv malwarea,
- provjeriti jesu li antivirusni programi protiv malwarea ažurirani,
- svake sedmice pregledati cijeli računar,
- sa interneta preuzimati samo onaj sadržaj koji dolazi iz vjerodostojnih izvora
- ne preuzimajte piratske sadržaje (uključujući filmove, muziku i računarske programe). Iako su besplatni, takvi sadržaji mogu sadržavati štetne programe,
- paziti da su uobičajene aplikacije i programski dodaci (plug-ins), kao što su Microsoft Office, Adobe Acrobat i Adobe Flash, uvijek ažurirani i imaju sve sigurnosne elemente. Brojne aplikacije se mogu automatski ažurirati.
- neophodno je biti posebno oprezan prilikom plaćanja putem interneta, uvijek provjeriti da li je stranica na kojoj se nalazite zaštićena. Kako bi se uvjerili da se ide na vjerodostojnu stranicu, potrebno je upisati adresu u preglednik, umjesto klika na link (poveznicu).[23]

[23] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (5.2.2023.)

4.4.1.2. Spyware/Adware

Spyware je program koji „špijunira“ vaše aktivnosti na internetu, dok je **adware** program koji na računare instalira skočne prozore i oglase. Mnogi od poznatih virusa rade i jedno i drugo. Spayware u najboljem slučaju može biti prilično bezopasan – može prikupiti informacije o vašim navikama surfanja i prikazivati oglase koji odgovaraju onome što vas zanima (adware). Pa čak i tada je riječ o svojevrsnom napadu na privatnost i može značajno usporiti rad računara. U najgorem slučaju spyware može biti maliciozan i skenirati vaš tvrdi disk u potrazi za ličnim podacima, poput bankovnih podataka i lozinki, te ih otkriti kriminalcima. Osim toga, može pokušati srušiti instalirane antivirusne programe i anti-spyware programe.

Kako prepoznati da je računar zaražen spywareom/adwareom?

Ukoliko je računar zaražen primijetit ćete da se na računaru pojavljuju skočni prozori sa oglasima (adware) čak i kada računar nije spojen na internet, početna stranica preglednika ili postavke pretraživanja se mijenjaju bez prethodnog upozorenja, na pregledniku se pojavila nova, neočekivana i neželjena alatna traka, računar je sporiji, a sistem se sve češće ruši.

Kako izbjeći spyware/adware?

Ukoliko se pridržavate sljedećeih savjeta, sa priličnom sigurnošću se može reći da ćete biti sigurni od spywarea/adwarea, ali i brojnih drugih sigurnosnih prijetnji na internetu.

- **Sa interneta preuzeti i instalirati anti-spyware program**

Korisnicima OS-a Windows Microsoft nudi besplatni anti-spyware program Windows Security Essentials. Također, drugi proizvođači programskih rješenja nude slične proizvode, te će vam biti preporučeno najprikladnije rješenje za vaš system.

- **Ažurirajte programe**

Koristite li Windows, dopune za svoje programe možete preuzeti sa Microsoftove stranice. Na istoj stranici možete omogućiti svom računaru da se automatski ažurira, zbog čega nećete morati sami brinuti o preuzimanju najnovijih programskih dopuna i verzija.[24]

[24] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (5.2.2023.)

- **Oprezno surfajte internetom i preuzimajte sadržaj**

Programe preuzimajte samo sa stranica kojima vjerujete. Ako sumnjate u sigurnost pojedinog programa, možete upisati njegov naziv u preglednik i provjeriti da li je neko prijavio da pomenuti program sadrži i spyware.

- Čitajte sve sigurnosna upozorenja, ugovore o licenci i izjave o zaštiti privatnosti, prije nego preuzmete bilo koji program,
- Nikada nemojte kliknuti na „OK“ ili „I agree“ u skočnom prozoru, osim ako niste sigurni da znate na šta pristajete,
- Budite oprezni s programima za razmjenu besplatne muzike ili filmova i svakako proučite rješenja koja dolaze u paketu sa takvim programima.

4.4.1.3. Scareware

Scareware ili program za zastrašivanje je vrsta malicioznoga programa koji generira skočne prozore slične porukama operativnog sistema Windows i koji zatim imitira antivirusni ili anti-spyware program, firewall (vatrozidnu) aplikaciju ili čistač baze podataka. Cilj takvih poruka je uvjeriti korisnika da se na njegovom računaru nalazi niz zaraženih datoteka. Korisniku se onda savjetuje kupovina određenog softverskog rješenja koje će riješiti njegov problem. A problem, zapravo uopće ne postoji, dok je preporučeni program vjerovatno pravi **malware**. Ukoliko korisnik povjeruje porukama, ne samo da će izgubiti novac potrošen na beskorisni program, već će se njegovi lični, povjerljivi podaci vrlo vjerovatno naći u rukama pravih kriminalaca.

Kako izbjeći scareware?

Neophodno je voditi računa da su na računaru uvijek instalirani valjani i legitimni antivirusni te anti-malware programi. Ono što je posebno važno – nikada nemojte kliknuti na skočne prozore koji tvrde da je računar zaražen ili nude skeniranje računara u potrazi za greškama. Gotovo je uvijek riječ o prevarama.[25]

[25] https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala (5.2.2022.)

ZAKLJUČAK

Današnji, popularni online svijet, ne možemo posmatrati kao sigurno mjesto u kojem se možemo nonšalantno ponašati. Razlog tome je što internet kriminalci nikad ne spavaju i veoma su kreativni. Također, svaka nova tehnologija koja se ustali, uđe u svakodnevni život pojedinaca i postane alat, automatski postaje meta napada, samo drukčijim sredstvima. U slučaju cyber napada i prijetnji, štete su velike, ali rješenja postoje, posebno ako na njih mislimo na vrijeme, odnosno prije nego što postanemo žrtva, bilo kao kompanija ili pojedinac.

Realno gledano, danas je stanje informacijske sigurnosi na relativno niskom nivou. Razlog tome jeste što u institucijama nedostaje pravila i sistematičnosti, koje se odnose na regulaciju informacione sigurnosti, a to predstavlja ključni korak za zaštitu od cyber napada i prijetnji. Jedan od najvećih problema današnjice kada govorimo u cyber prijetanjama jeste nedostatak adekvatnih sredstava, izostanak svijesti i nedovoljna obučenost i nesvjesnost osoblja o važnosti i riziku o cyber prijetnjama.

Stoga je upitno, u smislu kratkoročnih mjera pokrenuti programe edukacije osoblja o pitanjima cyber prijetnji i sigurnosti. Važno je skrenuti im pažnju na ranjivost i podložnost sistema na cyber prijetnje, te načine na koje oni mogu djelimično djelovati kako bi se to spriječilo.

Dugoročno gledano, trebao bi se poboljšati sustav upravljanja incidentima narušavanja informacijske sigurnosti te bi trebao postojati plan oporavka i funkcioniranje u kriznim situacijama. Uz to, dobra ideja je napraviti i procjenu rizika, kako bi se ustanovilo koje su slabosti i potencijalni nedostaci sustava.

Najznačajnije specifičnosti cyber prijetnji je tzv. cyber prostor te tehnologija koja olakšava provedbu ovih djela. Cyber napadi su jedna od najvećih prijetnji koji uz pomoć tehnologije sve više rastu, a dijele se na cyber kriminal, cyber špijunažu, cyber terorizam, kibernetski rat te hibridni rat. Cyber kriminal su krivična djela poput prijevara na području internet bankarstva, odnosno sva djela kod kojih je upotreba računala ključna za napad. Cyber špijunaža je odavanje tajni ili povjerljivih podataka pomoću špijunskih programa. Nadalje, za cyber terorizam se može reći da su to planirani napadi na računalne sisteme od strane

nacionalnih skupina, dok je kibernetski rat, rat koji se poduzima od strane država, a vodi se protiv drugih država sa ciljem uništavanja njihove upotrebe.

Borba protiv navedenih cyber prijetnji sprovodi se u obliku međunarodne suradnje specijaliziranih organizacija. Kao odgovor na konstantna ugrožavanja sigurnosti, Konvencija o cyber kriminalu koju je donijelo Vijeće Europe, je dobar temelj za uspostavu učinkovite borbe cyber kriminala, ali i općenito cyber prijetnji.

Za efikasnu borbu protiv cyber kriminala potrebno je da se uspostavi saradnja između javnog (državnog) i privatnog sektora. Oni bi trebali imati povjerenje u cyber-sigurnost, jer ako se dovede na dobar nivo pomoći će im da uspije u svom poslu. Ulaganje je poslovna potreba, a ne nepotreban trošak. Osvrčući se na javni sektor, potrebno je da se uloži novac u poboljšanje sigurnosti jer doprinosi sigurnosti društva u cjelini, te je za ovo potrebno napraviti nacrt da se dio novca izdvaja iz budžeta. Za obezbjeđivanje adekvatnih resursa za postizanje ciljeva potrebna su ulaganja, ali za sigurnost mreže obično nije problem materijalne prirode, već su problem ljudski resursi. Razvijanje adekvatnog ljudskog kadra je veoma dugotrajan proces i ne može se postići u kratkom vremenskom periodu, tako da ovaj proces treba započeti što prije. Svakako i razvoj ljudskih resursa i nabavka zahtijevaju adekvatna finansijska sredstva i opremu.

U današnjem, putem interneta, povezanom svijetu, svi imamo koristi od naprednih programa cyber obrane. Na individualnom nivou, napad cyber sigurnosti može rezultirati svime, od krađe identiteta, pokušaja iznude i sve do gubitka važnih podataka. Danas postoji mnogo različitih vrsta zaštite i alata, od kojih svaki ima različite funkcije i metode, a svima je zajedničko da doprinose sigurnosti informacija. Sigurnost informacija je mnoštvo različitih cyber strategija za sprječavanje neovlaštenog pristupa organizacijskim resursima kao što su računala, mreže i podaci. Sigurnost informacija održava integritet i povjerljivost podataka i sprječava napadače i cyber prijetnje da im pristupe.

Motivi cyber prijetnji mogu biti različite prirode i zato sve službe u međusobnoj koordinaciji imaju zadatak implementirati nove programe cyber sigurnosti. Isto tako treba svakodnevno raditi na sortiranju izvora cyber prijetnji da bi se tačno znalo koja protumjera će se upotrijebiti protiv određenog izvora cyber napada. Da bi programi cyber zaštite bili što kvalitetniji potrebno je dobro pznavati razine cyber prijetnji prema nivou sigurnosti, a to znači da svi oni koji sudjeluju u sistemu zaštite trebaju biti stručno osposobljeni.

Provođenje preventivnih mjera i metoda zaštite od cyber prijetnji treba biti brzo i efikasno budući da je vrijeme krucijalno pri javljanju cyber prijetnji. Potrebno je jasno razraditi područja u kojima će se primjeniti preventivne mjere i metode zaštite. Razvoj programa cyber zaštite je kompleksan ali uz adekvatnu obuku izvediv zadatak. Potrebno je oformiti stručne timove koji će svaki sa svog područja složiti kvalitetan program. Baza pri razvoju programa cyber zaštite mora bit načelo isplanirati-štititi-identificirati-reagirati. Svaki od ovih koraka mora efikasno i precizno izvršiti svoju zadaću da bi kompletan program zaštite uspio.

Rad na svakodnevnim analizama rizika i mogućih posljedica od strane cyber napada moraju biti što efikasniji i precizniji. Da bi se postigla što veća sigurnost, neophodno je da konačna rješenja budu tačna jer mjesta pogreškama kad je u pitanju cyber napad, zapravo i nema. Svi trebaju znati da borba protiv cyber napada nije izbor nego uslov o kojem ovisi mnogo toga. Potrebno je svakodnevno tragati za boljim i efikasnijim rješenjima. Provođenje istraživanja će dati rezultate pomoću kojih će se donijeti precizni standardi za borbu protiv cyber kriminala. Isto tako poboljšanje standarda može se izvršiti ukoliko se poštuju i preporuke koje su date radi bolje obrane od cyber napada.

Sigurnosna rješenja se mogu podijeliti u nekoliko grupa, a razlikuju se u dvije glavne karakteristike: proaktivna i reaktivna rješenja. Proaktivna rješenja štite sustave od prijetnji, baziraju se na brzoj identifikaciji i eliminaciji prijetnji, a reaktivna rješenja se javljaju u trenutku kada se već dogodio iskorak i kada je potrebno primijeniti sigurnosne politike definirane u slučaju incidenta.

Ovisno o određenom cilju, cyber motivi mogu biti različite i široke prirode. Motivi cyber prijetnji se karakteriziraju prema izvorima i prema nivou sigurnosti što itekako određuje metode kojima se službe za cyber sigurnost služe u borbi protiv cyber napada. Da bi se određena cyber prijetnja uklonila što brže i što bolje, sami motivi cyber prijetnji predstavljaju možda i najvažniji korak.

Cyber napadi ne ostavljaju iste posljedice na sve organizacije ili pojedince a razlog tome je što svi djeluju drugačije u borbi protiv istih.

U radu je potvrđena generalna hipoteza jer su kroz istraživanje date najznačajnije odlike cyber prijetnji, te načini pomoću kojih se moguće boriti sa cyber prijetnjama i rizicima.

Lista skraćenica

BiH- Bosna i Hercegovina

CERT/CSIRT- Computer emergency response team – Tim za hitne kompjuterske intervencije

DDoS – Distributed Denial of Service Attack – Distibuirani napad usraćivanjem resursa

EU- Evropska unija

EUCI- Vijeća o sigurnosti povjerljivih podataka o zaštiti povjerljivih podataka

ID- identifikacija

IKT- informaciono-komunikacionim tehnologijama

IoT – Internet of Things – Internet stvari

IT- Informacione tehnologije

NAS- Network Attached Storage – Mrežna pohrana

NIS – Norton Internet Security – Norton internet sigurnost

NORAD (13) - North American Aerospace Defense Command - Zapovjedništvo protuzračne obrane Sjeverne Amerike

NSA- National Security Agency - Agencija za nacionalnu sigurnost

OEBS – Organization for Security and Co-operation in Europe - Organizacija za evropsku bezbjednost i saradnju

OSCE - Organization for Security and Co-operation in Europe - Organizacija za sigurnost i saradnju u Evropi

SAD – Sjedinjene Američke Države

SQL – Structured Query Languague – Jezik strukturisanih upita

UN- United Nations – Ujedinjene nacije

UNESCO- United Nations Education Science and Culture - Organizacija Ujedinjenih naroda za obrazovanje, nauku i kulturu

USA- United States of America – Ujedinjene Američke Države

UVNS- Ured Vijeća za nacionalnu sigurnost

WWW- World Wide Web

Popis literature

Knjige:

1. Azinović, V., (2012)., Uvod u studije terorizma“, Sarajevo,
2. Babić, V., (2009)., Kompjuterski kriminal“, Sarajevo,
3. Babić, V.„(2015) „Cyber terorizam- Suvremena sigurnosna prijetnja“, Novi Travnik,. godina;
4. Baraković, S., Baraković H, J., (2015)„We have problems for solutions: the State of cybersecurity in B&H“,
5. Buckland, Benjamin, S. Schreier, Fred and winkler Theodor H. 2010. “Democratic Governance: Challenges of Cyber Security”, dcaF, Geneva, Switzerland.
6. Clarke, R., Knake, R.,. 2010. “Cyber War: The next Threat to National Computer Communication Review, 39(5), 22-31.
7. Derenčinović, D., (2003), DJEČJA PORNOGRAFIJA NA INTERNETU - O KAŽNJIVOSTI POSJEDOVANJA I VIRTUALNOJ DJEČJOJ PORNOGRAFIJI, Naučni rad, Pravni fakultet, Zagreb
8. Finnemore, M., Sikkink,K., 1998. “International norm dynamics and political change, international organization”, Gao (Government accountability office). 1996. Gao report aiMd. 96-84.
9. Hamid, A., Rashid, M. i Hong, C. S., (2006). Routing Security in Sensor Network: HELLO Flood Attack and Defense. ICNEWS.
10. Heijden, R., Dietzel, S., Leinmuller, T. i Kargl, F. (2019). Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. IEEE Communications Surveys & Tutorials 21(1), 779-811.
11. Helmbrecht, U., Purser, S., Klæstrup, R., “Cyber Security: Future, challenges and opportunities”. European network and information Security agency (eniSa), 2011.
12. Hu, Y. C., Perrig, A., Johnson, D. B., (2003). Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. IEEE INFOCOM.
13. Izet Beridan, „Leksikon sigurnosti“, Sarajevo, „DES“ 2001. godina;
14. Kavitha, T. i Sridharan, D. (2010). Security Vulnerabilities In Wireless Sensor Networks: A Survey. Journal of Information Assurance and Security 5, 31-44.
15. Krauss, C., Schneider, M. i Eckert, C. (2008). On handling insider attacks in wireless sensor networks. Information Security Technical Report, 13, 165-172.

16. Kulović, A., (2019.), BEŽIČNE MREŽE, UMREŽAVANJE I BEŽIČNI PRIJENOS, Diplomski rad, FIT, Travnik
17. Lukasik, S. (2011). Why the Arpanet Was Built. IEEE Annals of the History of Computing, 33(3), 4-21.
18. M. Bhardwaj, G.P. Singh., (2011), Types of Hacking Attack and their Counter Measure.
19. Marczi , S., (2014.), ODNOSI MEĐU MLADIMA U VIRTUALNOM SVIJETU, Diplomski rad, Sveučilište J.J. Strossmayera, Osijek
20. Masleša, R., (2001), Teorije i sistemi sigurnosti, Magistrat, Sarajevo.
21. Navarro, J. N. i Jasinski, J. L. (2012). Going cyber: Using Routine Activities Theory to predict cyberbullying experiences. Sociological Spectrum, 32(1), 81 – 94.
22. Newsome, J., Shi, E., Song, D. i Perrig, A. (2004). The Sybil Attack in Sensor Networks: Analysis and Defenses. IPSN (Information Processing in Sensor Networks).
23. Ngai, E., Liu, J. i Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications, 30, 2353-2364.
24. P.W. Singer, Allan Friedman, „Cybersecurity and cyberwar- what everyone needs to know“, SAD, 2014. godina;
25. Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A. i Patsakis, C. (2018). Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. IEEE Access, 6, 9390-9403.
26. Roberts, L. G. i Wolff, S. (2009). A Brief History of the Internet. ACM SIGCOMM
27. Stanković, N. (2014.), Terorizam i finansiranje terorizma, Markos – Banja Luka; Evropski Univerzitet Brčko
28. Termiz, Dž., „Metodologija društvenih nauka“, Sarajevo, 2003. godina;
29. Termiz, Dž., „Specifičnosti metodologije istraživanja u bezbjednosnoj djelatnosti“, Sarajevo, 2014. godina;
30. Termiz, Dž., Metodologija društvenih nauka- Drugo dopunjeno i prošireno izdanje, Lukavac, 2009. godina;
31. Termiz, Dž., Milosavljević, S., „Praktikum iz metodologije politikologije“ ,Sarajevo 2000. godina;
32. Veresha, R. (2018). PREVENTIVNE MJERE PROTIV RAČUNALNOG KRIMINALA: PRIBLIŽAVANJE POJEDINCU. Informatologia, 51 (3-4)

Dokumenti:

1. Ministarstvo unutarnjih poslova (2019). Online prijava zlostavljanja djeteta - RED BUTTON. Preuzeto s https://mup.gov.hr/online-prijave/online-prijava-zlostavljanja-djeteta-red-button/zlostavljanje-putem-interneta/rizici-online-komunikacije-s-nepoznatim-osobama/281701
2. Ministarstvo socijalne politike i mladih. (2015). Pravilnik o vođenju evidencije i dokumentacije pružatelja socijalnih usluga, te načinu i rokovima za dostavu izvješća. Narodne novine 100/2015.
3. Security and what to do about it". ecco; First edition. council of europe. 2001. "convention on cybercrime". Budapest, 23. 11. 2001. directorate-General for external policies of the union. 2011. "cybersecurity and cyber-power: concepts, conditions and capabilities for cooperation for action within the eu".
4. Study requested by the european parliament's. ecoSoc. 2007. "ecoSoc resolution 2007/20 – international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related crime".

Internet izvori:

1. http://sipa.gov.ba/hr
2. http://www.download.hr/forum/vijesti/2129-prijete-cyber-teroristi.html
3. http://www.fup.gov.ba/
4. http://www.msb.gov.ba/Default.aspx?langTag=hr-HR&pageIndex=1
5. http://www.nacional.hr/clanak/121487/cyber-terorizam-i-kolaps-civilizacije
6. http://www.phy.pmf.unizg.hr/~dandroic/nastava/rm/racunalni_virusi.pdf
7. http://www.znanost.com/clanak/skolovanje-mladih-strucnjaka-za-poslove-drzavne-cyber-
8. www.msb.gov.ba/docs/Strategija_za_CERT.doc
9. https://www.acunetix.com/websitesecurity/web-application-attack