RAČUNALNI KRIMINALITET U KONTEKSTU SIGURNOSTI I ZAŠTITE

Matešić, Mario

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite
Specijalistički diplomski stručni studij sigurnosti i zaštite

Mario Matešić

RAČUNALNI KRIMINALITET U KONTEKSTU SIGURNOSTI I ZAŠTITE

ZAVRŠNI RAD

Karlovac, 2019.

Karlovac University of Applied Sciences
Safety and Protection Department
Professional graduate Study of Safety and Protection

Mario Matešić

COMPUTER CRIME IN THE CONTEXT OF SECURITY AND PROTECTION

FINAL PAPER

Karlovac, 2019

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite
Specijalistički diplomski stručni studij sigurnosti i zaštite

Mario Matešić

RAČUNALNI KRIMINALITET U KONTEKSTU SIGURNOSTI I ZAŠTITE

DIPLOMSKI RAD

Mentor:
dr.sc. Damir Kralj, prof.v.š.

Karlovac, 2019

VELEUČILIŠTE U KARLOVCU

KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički diplomski stručni studij sigurnosti i zaštite
(označiti)

Usmjerenje: Zaštita na radu Karlovac: 22.08.2019.

ZADATAK ZAVRŠNOG RADA

Student: Mario Matešić Matični broj: 0248038969

Naslov: RAČUNALNI KRIMINALITET U KONTEKSTU SIGURNOSTI I ZAŠTITE

Opis zadatka:

- na osnovi dostupnih izvora te vlastitih iskustava i saznanja, analizirati dostupne pojavne oblike računalnog kriminaliteta kao i njihov oslonac na tradicionalne oblike sveukupnog socijalnog inženjeringa kao potencijalne opasnosti koja posredno može ugroziti život, zdravlje i materijalne vrijednosti u raznim područjima ljudske djelatnosti;
- polazeći od pretpostavke da se praksa i svijest pojedinca u području poznavanja opasnosti primjene zaštitnih mjera protiv računalnog kriminaliteta projicira na ukupnu svijest zajednice, sukladno mogućnostima načiniti kratki anketni upitnik i primijeniti ga na prigodnu dostupnu populaciju sastavljenu od stručnjaka i studenata u području sigurnosti i zaštite, te izvršiti osnovnu statističku analizu prikupljenih rezultata;
- na osnovi prethodne teorijske analize i dobivenih anketnih rezultata, dati procjenu postojećeg stanja i predložiti mogućnosti poboljšanja svijesti djelatnika i metoda zaštite od računalnog kriminaliteta u području sigurnosti i zaštite.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
22.08.2019.	12.12.2019.	19.12.2019.

Mentor: Predsjednik Ispitnog povjerenstva:

dr.sc. Damir Kralj, prof.v.š. Ivan Štedul,prof., v.pred.

PREDGOVOR

Ovom prilikom se zahvaljujem mentoru dr. sc. Damiru Kralju, prof. v. š. na ukazanoj pomoći, stručnim savjetima i posvećenom vremenu tijekom izrade diplomskog rada.

Također se zahvaljujem i ostalim profesorima i asistentima Veleučilišta u Karlovcu, Studija sigurnosti i zaštite na suradnji i pruženom znanju.

A najveće hvala mojim roditeljima, sestri i djevojci na strpljenju, razumijevanju i podršci tijekom studija.

„Učenje je kao veslanje uzvodno; čim se prestane, odmah se kreće nazad.“

Lao Ce

SAŽETAK

Računalni kriminalitet postaje sinonim za različite upade u računalni sustav pojedinca ili pravnih osoba. Razlog za to ne moraju nužno biti financije nego i poruka prijetnje, upozorenje građanima, opstrukcija operativnog sustava jednog poduzeća. No, bez obzira na razloge, sve je veći broj različitih računalnih napada kao na primjer od hakiranja do računalne sabotaže i softverskog piratstva. Zbog takvih pojava, svaka zemlja članica Europske Unije poseže za različitim mjerama u svrhu zaštite od računalnog kriminaliteta što je zahtjevno s obzirom na virtualnost računalnog svijeta. Posljedice računalnog kriminaliteta su dalekosežne jer štete trgovini, kompetitivnosti, inovacijama i globalnom ekonomskom rastu. To upućuje razna poduzeća na izdvajanja ogromnih financijskih troškova s ciljem prevencije računalnog kriminaliteta te edukaciju zaposlenika, jer većina grešaka rezultat su ljudskih slabosti. Učinjeno je online istraživanje o sigurnosti i zaštiti na računalu za radno sposobne ljude, a ono je ukazalo na određenu ležernost u pristupu prema zaštiti od računalnog kriminala. Cilj rada je prepoznavanje štetnih pojava u cilju zaštite života i zdravlja ljudi - radnika te zaštite materijalnih dobara.

Ključne riječi: računalni kriminalitet, sigurnost, zaštita, prevencija, online istraživanje

SUMMARY

The computer crime becomes equivalent word for different invasions in different computer systems of indviduals and legal persons. The reason for invasion must not be only money but also threat message, a warning to citizens, an obstruction of company's operational system. Whatever the reasons are, the number of different computer attacks such as hacking, computer sabotage and software piracy is on the rise. Because of these advents, every EU member country takes measures for protection against the computer criminal, what is very demanding regarding the virtuality of computer world. The consequences of computer criminal are large as they make damage to trade, competitiveness, innovation and global economic growth. It gives a reason to different companies to allocate money for computer criminal prevention and education of the employees because a lot of mistakes are the result of human weakness. An online survey on computer security and protection among the working population has been done, and it has indicated a certain degree of ease in accessing computer crime protection. The aim of this thesis is to identify harmful phenomena in order to protect the life and health of people-workers and protection of material goods.

Keywords: computer criminal, security, protection, prevention, online research

SADRŽAJ

ZADATAK ZAVRŠNOG RADA I

PREDGOVOR II

SAŽETAK III

SUMMARY III

SADRŽAJ IV

1. UVOD 1

1.1. Predmet i cilj rada 1

1.2. Glavna hipoteza rada 1

1.3. Izvori podataka i metode prikupljanja 1

2. RAČUNALNI KRIMINALITET 2

2.1. Determinante računalnog kriminaliteta 3

2.1.1. Pojmovno određenje i osnovna obilježja 3

2.1.2. Nastanak i razvoj 3

2.2. Metode računalnih napada kroz studiju primjera 4

2.2.1. Hakiranje (engl.hacking) 5

2.2.2. Računalna špijunaža 5

2.2.3. Računalna sabotaža 6

2.2.4. Računalna prijevara 7

2.2.5. Računalno krivotvorenje 9

2.2.6. Softversko piratstvo 10

2.2.7. Nezakoniti sadržaji 12

2.3. Kibernetički napad i samoobrana 13

3. PRAVNA REGULACIJA 16

3.1. Tallinnski priručnik 16

3.2. Internacionalni režimi koji reguliraju računalni kriminalitet 18

3.3. Kibernetički kriminalitet u Republici Hrvatskoj 19

4. POSLJEDICE I PREVENCIJA RAČUNALNOG KRIMINALITETA.....22
4.1. Posljedice računalnog kriminaliteta na štićena dobra i vrijednosti.....23
4.2. Pogreške u zaštiti 24
4.3. Metode i sredstva prevencije 25
5. ISTRAŽIVANJE O RAČUNALNOM KRIMINALU 27
5.1. Metodologija istraživanja.....27
5.1. Rezultati istraživanja.....28
6. ZAKLJUČAK 38
7. LITERATURA 40
8. PRILOZI 43
8.1. Upitnik 43
8.2. Popis tablica 46
8.3. Popis slika 46
8.4. Popis grafikona 46

1. UVOD

Rad se sastoji od teorijskog dijela istraživanja koji se zasniva na analizi dobivenih podataka iz stručne i znanstvene literature, prikupljanja dostupnih pisanih i internetskih sadržaja, raznih članaka, časopisa te ostalih sekundarnih izvora iz područja računalne kriminalistike. U prvom dijelu rada, opisani su determinantni računalnog kriminaliteta i metode računalnih napada što spada pod kaznena djela. Postojeći načini sankcioniranja računalnih kaznenih djela opisani su u trećem poglavlju i to na regionalnoj i međunarodnoj razini. Posebno posvećena je pažnja priručniku Tallinnski. Ključno je opisivanje metoda i sredstava prevencije računalnog kriminaliteta što je veoma zahtjevan zadatak s obzirom da obilježja računalnog kriminaliteta uključuju virtualnost svijeta. Uglavnom, opisuju se izdvojene i sistematizirane štetne posljedice računalnog kriminaliteta za određena štićena dobra i vrijednosti te su istražena dostupna iskustva problema i havarija u poslovnom svijetu i industriji koji su bili izravna ili posredna posljedica napada iz domene računalnog kriminaliteta. Proveo sam istraživanje o metodama zaštite i sigurnosti od računalnog kriminaliteta. U radu su navedene preporuke za prevenciju i zaštitu u kontekstu SiZ.

1.1. Predmet i cilj rada

Cilj i zadatak ovog diplomskog rada je opisati značaj računalnog kriminaliteta do danas, te opisati prepoznavanje ovih štetnih pojava u cilju zaštite života i zdravlja ljudi - radnika te zaštite materijalnih dobara.

1.2. Glavna hipoteza rada

Glavna hipoteza je da ispitivanjem navika i stupnja svjesnosti potencijalnih prijetnji od digitaliziranih metoda socijalnog inženjeringa, dobivamo sliku o stanju pojedinca koja se izravno projicira na kolektivnu svijest zajednice. Kroz rezultate tada vidimo kako preventivno djelovati kroz razne oblike edukacije.

1.3. Izvori podataka i metode prikupljanja

Metodologija rada sačinjava anketa o računalnom kriminalitetu te provođenje ispitivanja među radno sposobnim ljudima koji su svakodnevno u doticaju sa računalnom tehnologijom. U prikupljanju literature korištena je dostupna literatura koja se tiče teme rada. Kao baze podataka poslužili su Eurostat, službene stranice Ministarstva unutarnjih poslova, Eurosta, online knjižnica te baze podataka poput Emerald, Researchgate, Hrčak, Science Direct, Link Springer i Narodne novine - rad je bilo potrebno potkrijepiti određenim zakonskim propisima i odredbama , a zato je poslužila stranica Narodne novine.

2. RAČUNALNI KRIMINALITET

Računalna automatizacija i aplikacije temeljito su počele djelovati na radna mjesta što je dovelo do eliminiranja starih radnih mjesta te stvorilo nova radna mjesta s tim da su novi poslovi promijenjeni poradi prilagodbe uporabe računala [1]. Sve te raznolike aplikacije koje su nazočne u svijetu računala, od zbrajanja pa sve do pripremanja kalkulacija za brzu razmjenu podataka, imaju jedinstven cilj - povećavanje produktivnosti [1]. Nadasve, utjecaj računala (*engl.computer*) [2] izmijenio je način na koji se izvršavaju poslovi i mjesto gdje se izvršavaju. Prema riječima autorice Ribić, računala su donijela svoj vlastiti kriminal [1]. Prijestupi su stvarni problemi rastućeg značenja prema postojećem pregledu koje je izdalo Udruženje američkih odvjetnika. Prema posljednim podacima tog pregleda:

"*...vidljivo je da 70 tvrtki godišnje pokazuje rezultate nastalih šteta računalnog kriminaliteta, a gubici se kreću između 145 do 730 milijuna američkih dolara.* " [1].

Kada se govori o računalnom kriminalitetu, prvo se pomisli na metode manipuliranja računalima poput neovlaštenog pristupa računalnom sustavu, na zaraze sustava virusima, manipuliranje podacima, trojanskim konjima i sl. [2]. Ali, navodi se jedan zanimljiv pojavni oblik računalnog kriminaliteta a to je *HOAX* (hrv. obmana). To je blaži oblik računalnog kriminaliteta. Riječ je o e-mailovima neistinitog sadržaja, koji se šalju s ciljem zastrašivanja ili dezinformiranja primatelja [2].

Postoje neke vrste računalnog kriminaliteta koje su toliko ozbiljne da mogu čak ugroziti nacionalnu sigurnost. Primjerice, NASA je otkrila par puta ilegalan ulaz u njihovo računalo, a više puta su uništeni važni podaci. Postoje određeni računalni hakeri koji otkrivaju lozinke te na taj način lako ulaze u računalni sustav tvrtke. Zlouporabu računala olakšava loš sustav sigurnosti što nije začuđujuće kod pojedinaca, ali je uočeno da velike tvrtke, institucije, banke i drugi imaju začuđujuće niske stupnjeve sigurnosti. Čak se dogodi da otpušteni djelatnik ode od poslodavca, a da se nakon njegova odlaska ne izmijeni lozinka kojom se on služio, odnosno ne deaktivira se njegov korisnički račun [1].

Autorica Babić dodaje da je tijekom pisanja svoje knjige “Kompjuterski kriminal metodologija kriminalističkih istraživanja i razjašnjavanje i suzbijanje kompjuterskog kriminala” uočila da zaposlenici između sebe znaju ili lako otkriju lozinke kojima se drugi zaposlenici služe te da obično za lozinku uzimaju nešto što lako pamte, kao na primjer ime djevojke, supruge, broj telefona, datum rođenja, ime djeteta, kućnog ljubimca i sl.

Već davne 1997. godine Vijeće Europe osnovalo je Ekspertnu komisiju za kriminalitet u kibernetičkom prostoru čiji zadatak je izrada međunarodnog instrumenta za suzbijanje kriminaliteta u kibernetičkom prostoru. Vijeće Europe objašnjava da pojava razvoja informacijsko-komunikacijskih tehnologija, prije svega interneta, a time i kaznenih djela na internetu, čime je kazneno pravo usmjereno na kompjutorski kriminalitet, postalo preusko pa se kaznenopravna zaštita proširila na cijeli kibernetički prostor [3] te time dovela do potrebe stvaranje navedene ekspertne komisije.

2.1. Determinante računalnog kriminaliteta

2.1.1. Pojmovno određenje i osnovna obilježja

Računalni kriminal nije uvijek bio kršenje formalnog prava. Tek od 1979. godine, Ministarstvo pravosuđa SAD-a je definiralo računalni kriminal kao bilo koji nelegalni akt za čije počinjenje je upotrebljeno računalo ili računalna tehnologija. Potrebu za ovim nametnula je činjenica, da je samo krajem 70-ih godina već bilo više stotina (preko 500) kaznenih djela učinjenih upotrebom računala [1].

Prema napisima autora I. Vuletića, u sklopu njegova objavljena rada o računalnoj prijevari u hrvatskom kaznenom pravu, temeljno obilježje računalnog kriminaliteta je nematerijalna priroda računalnih podataka kao objekta ovih kaznenih djela [4] što znači nešto što nije opipljivo. U ovom slučaju, primjenjuju se opća načela kaznenog prava. Ipak, spomenuta nematerijalna (virtualna) priroda, uz druge probleme kao što su složenost računalnog sustava, anonimnost korisnika, globalna računalna povezanost i dr.: "*ukazuje na očiglednu potrebu za redefinicijom tradicionalnih kaznenopravnih koncepata."* [4] [cit. 680].

2.1.2. Nastanak i razvoj

Povijest i preteča suvremenih digitalnih računala seže čak u 3 mileniju prije Krista, kada se u Kini, Japanu i Indiji počinje koristiti prva ručna računala koja su se nazivala abak ili abakus. Nadalje, u sedamnaestom stoljeću su se razvila prva mehanička računala, u devetnaestom stoljeću električna računala, a tek sredinom dvadesetog stoljeća prva elektronička digitalna računala. Ovo ukazuje na to da je iznimno teško utvrditi kada je došlo

do prvih oblika računalnog kriminaliteta [5]. Postoje samo pretpostavke da se u najranijoj dobi njihova korištenja, u vrijem prije Krista, netko sjetio kako ih zloupotrijebiti. Navodno se pojava i primjena računalnog kriminaliteta vezuje uz primjenu prvih računala te uz izum Josepha Marie Jacquarda, koji je 1808. godine usavršio prvi tkalački stroj, tako da je automatski utiskivao uzorke na tkaninu uz pomoć bušene kartice [5]. To je kasnije 1883. godine iskoristio Charles Babbage. On je postavio teorijske osnove za rad suvremenih računala. U vrijeme dok Charles Babbage razvija svoja računala, radnici su poduzimali niz aktivnosti u cilju zaustavljanja uvođenja novih tehnologija u industriju kako ne bi ostali bez posla. U biti, riječ je bila o sabotažama. Te počinjene sabotaže predstavljala su prva kaznena djela iz gospodarskog kriminala - računalni kriminalitet [5]. I treće, začetke računalnog kriminaliteta još nalazimo u pojavi tzv. poslovnog kriminaliteta, poznatijeg pod nazivom kriminalitet "bijelih ovratnika", početkom 20. stoljeća.

Nadalje, šezdestih i sedamdesetih godina izmišljeno je niz hakerskih metoda i alata za provaljivanje u tuđe računalne sustave i zlouporaba sredstava komunikacije. Počinju se razvijati maliciozni računalni programi kao virusi, crvi i trojanski konji [5].

Korjene nastanka računalnog kriminaliteta treba tražiti i u telekomunikacijskom kriminalitetu iz šezdesetih godina XX. stoljeća kada se pojavljuju tzv. *phreakeri*. Phreakeri su osobe koje rabe različite metode kako bi besplatno koristile telefonske usluge [4] prema [6] [cit. 23]. Uočeno je da otkrivši načine zlouporabe tadašnje telekomunikacijske tehnologije, vrlo brzi su tako stečeno znanje primijenili na područje informacijske tehnologije [6]. Na taj način, mnogi freakeri (*engl. phreakeri*) postaju hakeri (*engl. hackeri*) što dovodi i do brisanja granice između telekomunikacijskog i računalnog kriminaliteta [6].

Glede razvoja računalnog kriminaliteta, prva računala su korištena u znanstvene i vojne svrhe te za poslovanje gospodarskih subjekata. Poticaj za razvoj računalnog kriminaliteta je bio primjena modema, koja omogućava vezu između međusobno udaljenih sustava. Na to se nadovezuje razvoj osobnih računala s čime počinje snažniji val računalnog kriminaliteta.

2.2. Metode računalnih napada kroz studiju primjera

Glede prvog slučaja računalnog kriminaliteta u nas, prvi put zabilježen je 1983. godine. Ostao je zapamćen slučaj službenika Istarske banke (1983. godina). Djelatnici navedene banke B. B. i S. U. te djelatnik podružnice Zagrebačke banke u Puli P. R., radili su u tim bankama kao operateri na sustavu. Prva dvojica uz pomoć djelatnika iz Zagrebačke banke izveli su financijsku malverzaciju na računalu s kojim su namjeravali oštetiti banku u iznosu preko 10 milijuna tadašnjih dinara. U istrazi su priznali da su namjeravali podijeliti iznos na jednake

dijelove. Iako nisu podigli novac, računalna prijevara je otkrivena i prijavljeni su nadležnim tijrlima.

2.2.1. Hakiranje (engl.hacking)

Hakiranje (engl. hacking) je neovlašteni pristup podacima i programima, a njegovu pojavu uvjetovao je brzi napredak u tehnologiji elektroničkih računala, koji je donio činjenicu da se danas najrazličitije banke podatka, počevši od privatnih, preko poslovnih, pa do državnih, temelje na automatskoj obradi podataka podržavanoj elektroničkim računalima [1]. U literaturi se spominju slavni slučajevi hakera u nekim razvijenim zemljama, kao na primjer slučaj Golda i Shifreena u Velikoj Britaniji. Autorica Babić opisuje hakere kao osobe muškog spola, u dobi od 15 i 35 godina, najčešće između 14 i 16 godina, inteligentniji su od ostalih ljudi. Ne ističu se vanjštinom od ostalih ali obavezno imaju neuredne radne ili spavaće sobe.

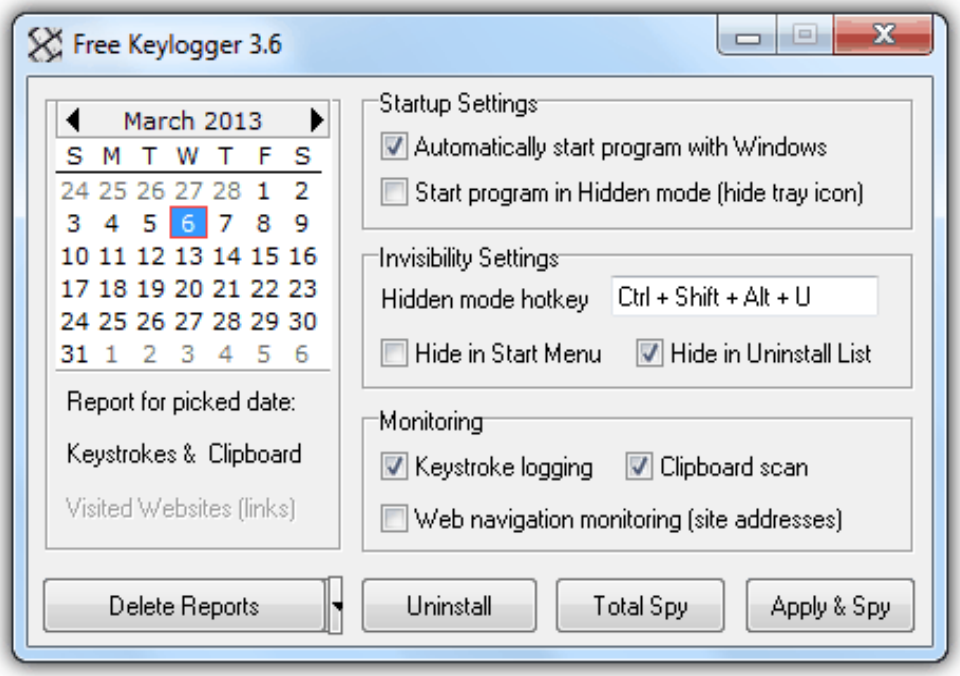
2.2.2. Računalna špijunaža

Računalnu špijunažu čine manipulacije neovlaštenog pribavljanja tajnih podataka i informacija pohranjenih u sustavima ili prijenosu putem telekomunikacijskih kanala [6]. Danas je vrlo teško reći koliko se slučajeva špijunaže događa svaki dan. Razne novine i televizijske kuće izvješćuju o velikim špijunskim aferama, ali razlog što znamo za njih je to što je netko uhvaćen. Isto tako, veoma je teško procijeniti koliko se špijunaže događa zbog toga što u mnogim slučajevima razna poduzeća i vladine agencije ne publiciraju uspjele ili neuspjele pokušaje prisluškivanja i špijunaže zbog negativnog publiciteta. Postoje određeni čimbenici koji mogu pomoći u shvaćanju opsega računalne špijunaže. To su:

- Dostupna i povoljna cijena računala koja su sve jednostavnija za korištenje
- Računala se koriste za pohranu osjetljivih i povjerljivih podataka
- Podaci u digitalnom obliku se lako prebacuju i prenose
- Današnji operacijski sustavi i aplikacije sadrže mnoge elemente sigurnosne ranjivosti
- Primjena interneta ubrzala je razvoj računalne špijunaže

Veliki dio računalne špijunaže otpada na industrijsku špijunažu. Savezni istražni ured (engl. *Federal Bureau of Investigation*, FBI) procjenjuje da industrijska špijunaža uzrokuje gubitke od 100 milijuna kuna godišnje za američka poduzeća [7]. U stvari, koliki se novac okreće ne može se uopće odrediti.

Oblici špijuniranja pomoću *Keyloggera* (Slika 1) su učestala pojava. Riječ je o softveru ili hardveru koji bilježi tipke koje su pritisnute na tipkovnici računala



Slika 1 – Keylogger [8]

Nadalje, kombinacija pritisaka tipki može sadržavati lozinku, dokaz, nezakonitu radnju ili druge tajne informacije koje bi ljudi zadržali za sebe. Špijuniranje tipki nije novo, već potječe od prve pojave pisaćih strojeva koji su koristili trake na kojima su ostala otisnuta sva slova. U današnje vrijeme, koristi se specijaliziran softver i hardver. Tijekom zadnjih par godina na internetu se pojavljuje veliki broj specijaliziranih softverskih *keyloggera*, što besplatnih, što komercijalnih. *Keylogeri* su vrlo raširen alat za računalnu špijunažu kojeg koriste šefovi za špijuniranje zaposlenika, nadalje, djeca ih koriste za špijunažu roditelja, roditelj za nadgledanje aktivnosti djece tijekom korištenja računala, vladine obavještajne agencije i policija koriste ih za hvatanje kriminalaca. Ako špijun ima fizički pristup računalu kojeg želi špijunirati, *keyloggeri* su vrlo čest izbor kao alat špijuniranja [6].

2.2.3. Računalna sabotaža

Računalne sabotaže sastoje se od uništenja ili oštećenja računala i drugih uređaja za obradu podataka u okviru računalnih sustava te brisanju ili mijenjanje podataka. Cilj im je sprječavanje korištenja potrebnih informacija koji se nalaze u datotekama računala. Najčešći oblici računalne sabotaže su oni koji djeluju destruktivno na operacijsko-informacijski mehanizam i korisničke programe, prije svega one, koji imaju funkciju čuvanja podataka [5].

"*Inače, tradicionalna zakonodavstva imala su odgovor na djela računalne sabotaže samo kada je do uništenja ili oštećenja došlo na tehničkoj osnovici, a ne kada su u pitanju bili računalni podaci.* " [cit. 5].

Isti autor objašnjava razlog zašto nije bilo moguće zaštiti integritet podataka postojećim propisima, jer je riječ o nematerijalnim dobrima, a zaštita se odnosila samo na materijalna dobra [5].

Iz tog razloga, došlo je do nadopune postojećeg zakonodavstva (Kazneni zakon). Promjene u zakonodavstvu po pitanju računalne sabotaže izvršile su sljedeće zemlje: Austrija, Njemačka, Finska, Francuska, Japan i Nizozemska. Ali, svaka zemlja je izvršila promjene na različit način. Primjerice, Japan, u svojem zakonu, pokriva sve dokumente, a ne samo računalne podatke Neke zemlje uključuju posebne kvalifikacijske okvire za računalne sabotaže koje mogu dovesti do opstrukcije poslovanja ili značajnih šteta na računalnim sustavima [5]. Pojedine američke države kao što su Kalifornija, Maine, Minessota, Nebraska i Texas, donijele su posebne propise o virusima. U Švicarskoj se kažnjava svaka osoba koja proizvede, uveze ili trguje računalnim programima koji se mogu iskoristiti za brisanje ili uništavanje podataka [5].

Prema navodima Ranabahta i suradnika u članku "*Optimal sabotage attack on composite material parts*" [9] uvedene su posebne odredbe za tzv. *Industry 4.0* oblik poslovanja koji predviđa potpuno automatizirano proizvodno okruženje u kojem računalna proizvodna oprema tzv. Kibernetičko-fizikalni sustavi (engl. *Cyber-Physical Systems,* CPS), izvršavaju sve zadatke. Ovi su strojevi otvoreni za razne kibernetičke i kibernetičko-fizičke napade, uključujući sabotaže. Dodaje se da u kontekstu proizvodnje, napadi sabotaže imaju za cilj oštećenje opreme ili propadanje mehaničkih svojstava proizvedenog dijela, a oni su posebno u svojem radu fokus stavili na kompozitne materijale [9]. Kompozitni materijalni dijelovi pretežno se koriste u sigurnosno kritičnim sustavima, npr. nosivi dijelovi zrakoplova. Upozoravaju na postojanje različitih metoda kompromitiranja različitih proizvodnih uređaja i zlonamjerne manipulacije koje će sabotirati dio [9]. Generalni zaključak je da će sve više razvijati računalna sabotaža i da će s vremenom razvijati i usavršavati različite visoke tehnologije za računalnu sabotažu. Izvoditelji računalnih sabotaža postat će sve smjeliji i hrabriji a njihovi ciljevi sve viši. Moguće da će računalne sabotaže biti usmjerene na banke podataka, računalne resurse, vladine komunikacijske sustave, elektrocentrale, zračne luke i sl.

2.2.4. Računalna prijevara

Računalna prijevara je najčešći oblik računalnog kriminaliteta Zbog globalne rasprostranjenosti interneta broj računalnih prijevara u stalnom je porastu i sa sve većim

materijalnim posljedicama. Štoviše, računalni kriminal postaje predmetom reguliranja međunarodnih dokumenata u svrhu zaštite i prevencije. Ipak, u Republici Hrvatskoj, ovaj kaznenopravni fenomen je do sada uglavnom bio zapostavljen, uz tek poneki fragmentarni osvrt [1]. Prema Središnjem državnom portalu, računalne prijevare definiraju se kao prijevare u kojima napadači pomoću zlonamjernih poruka elektroničke pošte i zlonamjernih sadržaja pokušavaju doći do osobnih podataka žrtve ili nanijeti joj materijalnu štetu [10]. Kada korisnik računala dobije poruke, može biti i e-poruka u kojoj ga obavještava da ga čeka lutrijski dobitak ili poslovna ponuda za posao, na primjer, u inozemstvo, vrlo vjerojatno je riječ o računalnoj prijevari. Preporučuje se brisanje takvih poruka bez otvaranja. Još se događa da dobitnik treba platiti naknadu, pa su prevaranti dobili dodatan dobitak. I tako prestaje daljnja komunikacija.

Prema Državnom središnjem portalu, drugi oblik računalne prijevare je krađa identiteta [10]. U tim slučajevima kada osoba pošalje svoje podatke, gotovo sigurno postoji opasnost od zlouporabe podataka odnosno krađe identiteta. [10].

Treći oblik računalne prijevare su tzv. "Nigerijska pisma". Tu se radi o odličnoj "poslovnoj ponudi" koju šalju, primjerice, razni sadašnji ili bivši dužnosnici afričkih zemalja tražeći pomoć pri transferu novčanih sredstava, obavezno značajnijih iznosa, koja su ostala na njihovim računima kada su ih otjerali s vlasti ili iz zemlje, a naravno uz primamljivu naknadu od 20 do 35 posto iznosa s njihovog računa u trenutku kada novac "sjedne" na pomagačev račun. Tzv. afrički dužnosnici do imena potencijalnih žrtava dolaze iz raznih izvora, odnosno medija, poslovnih časopisa, internet stranica i slično [10].

Sve ove situacije upućuju na značajan oprez građana po pitanju računalnih prijevara. Zakonske odredbe za računalne prijevare postaju jasne i konkretne te su kazne sasvim primjerene što se vidi iz sljedećega:

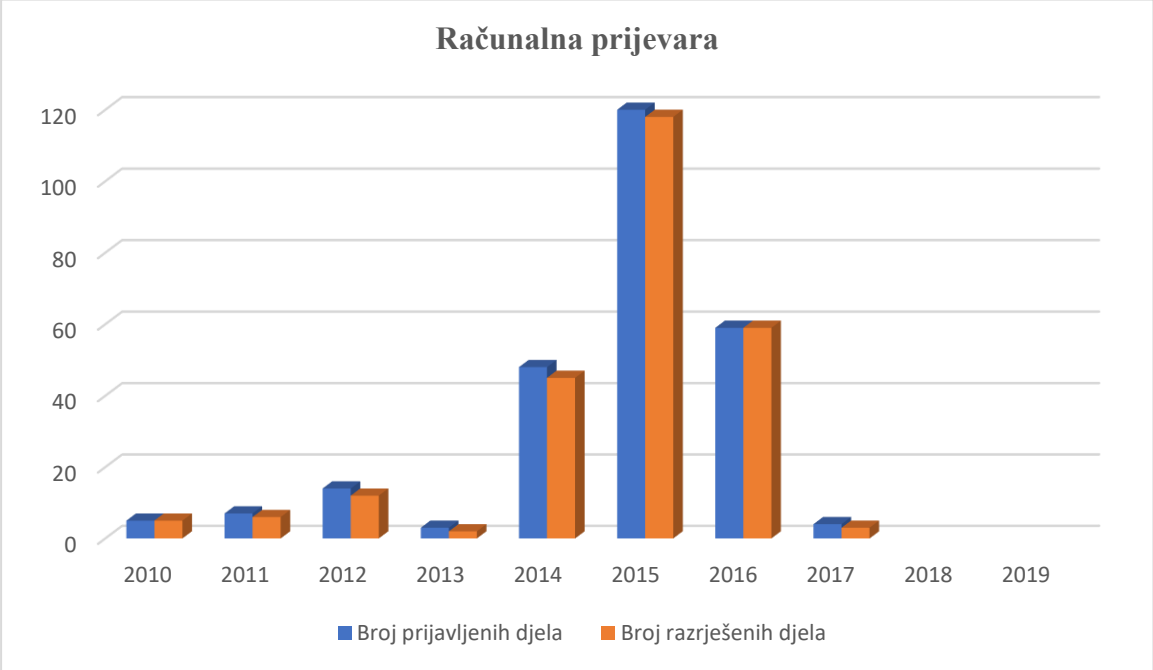
Prema Kaznenom zakonu Republike Hrvatske (RH), Članak 271. računalna prijevara je [11]:

(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2) Ako je kaznenim djelom iz stavka 1. ovoga članka pribavljena znatna imovinska korist ili prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od jedne do osam godina.

(3) Podaci koji su nastali počinjenjem kaznenog djela iz stavka 1. i 2. ovoga članka će se uništiti.

Postoji više vrsta kriminaliteta: gospodarski, opći, organizirani kriminalitet, kriminalitet zlouporabe droge. U gospodarski kriminalitet spadaju računalne prijevare i računalno krivotvorenje. Također, u gospodarski kriminalitet spadaju pronevjera, nedozvoljene igre na sreću, povreda tuđih prava, zlouporaba povjerenja u gospodarskom poslovanju, prijevara u gospodarskom poslovanju i drugo. No, za ovaj rad, ključna je računalna prijevara i krivotvorenje. U nastavku slijedi analiza računalne prijevare na području Karlovačke županije (Grafikon 1).

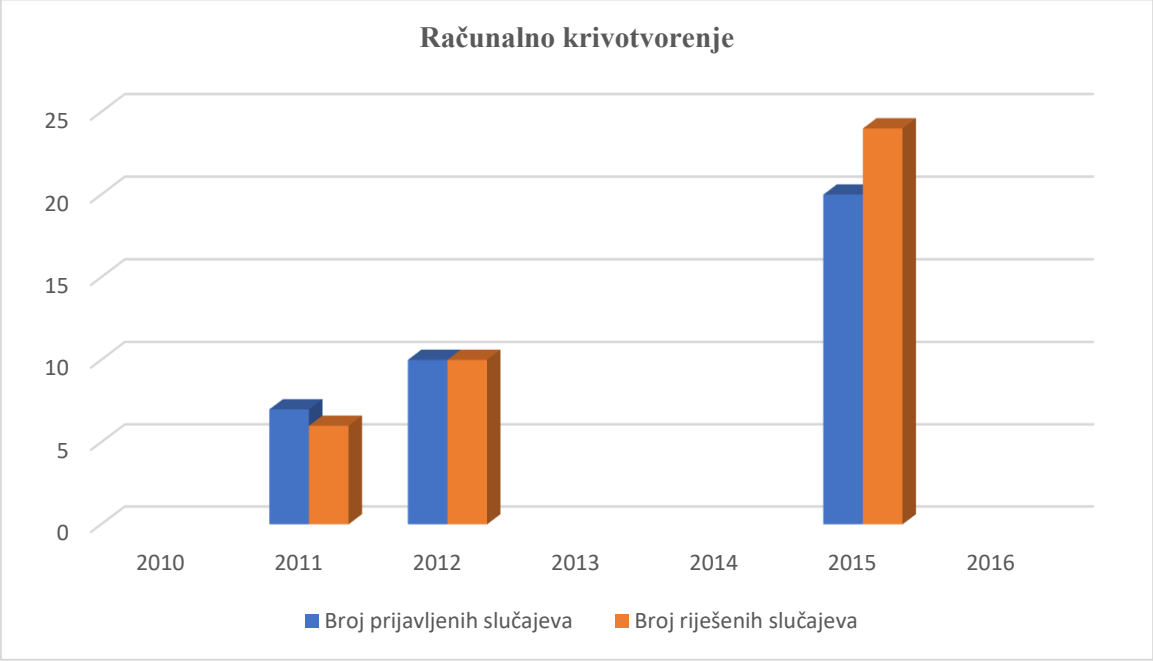


Grafikon 1. Statistički pokazatelji o računalnim prijevarama na području Karlovačke županije

Na temelju statističkih podataka koji su dostupni na službenim stranicama Policijske uprave karlovačke, uviđa se da dolazi do značajnog porasta računalne prijevare na području Karlovačke županije, s tim da nema podataka za 2018 i 2019. godinu. Uočen je najveći porast kaznenih djela računalne prijevare u 2015. godini (120 slučajeva), a od toga nisu riješena samo dva slučaja.

2.2.5. Računalno krivotvorenje

Na službenim stranicama Policijske uprave karlovačke, dostupni su statistički podaci o računalnom krivotvorenju. U nastavku slijedi analiza računalnog krivotvorenja (Grafikon 2).



Grafikon 2. Statistički pokazatelji računalnog krivotvorenja na području Karlovačke županije

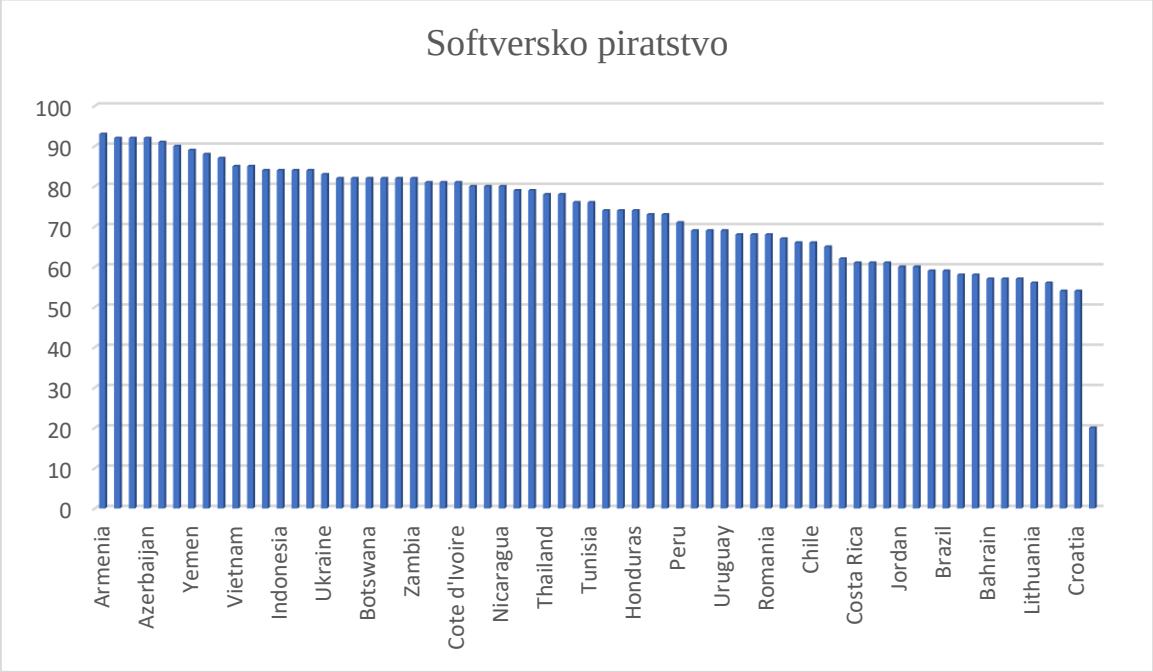
Dobiveni podaci upućuju na slab broj prijavljenih i razriješenih slučajeva računalnog krivotvorenja na području Karlovačke županije. U 2015. godini uočen je značajan porast računalnog krivotvorenja (20 prijavljenih slučajeva) na području Karlovačke županije. Kada se usporede prethodni podaci o računalnoj prijevari i ovi podaci o računalnom krivotvorenju, uočava se jedan zajednički segment a to je da najveći broj prijavljenih i riješenih slučajeva je u 2015. godini. Za 2010., 2013., 2014. i 2016. godinu, nema zabilježenih podataka o računalnom krivotvorenju na području Karlovačke županije.

2.2.6. Softversko piratstvo

Opća definicija softver (eng. software, SW) definira kao ukupnost ljudskog znanja ugrađenog u elektroničko računalo [14]. Softver predstavlja ukupnost nematerijalnih komponenata poslovnih upravljačkih informacijskih sustava [14]. Drugim riječima to je svekoliko ljudsko znanje ugrađeno u računalni hardver, a time i u poslovni upravljački sustav [14].

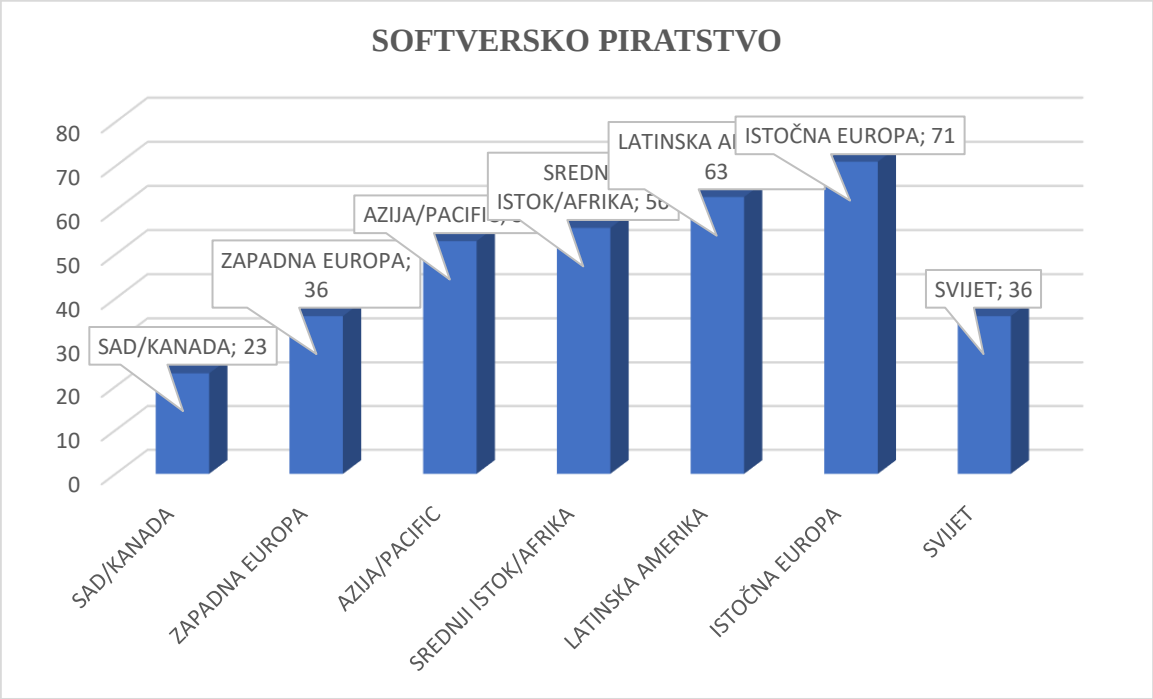
Softversko piratstvo uključuje krivotvorenje, neovlašteno umnožavanje, instaliranje, korištenje, stavljanje u promet (prodaja, distribucija, uvoz-izvoz, posudba, darovanje) računalnih programa [15]. Poslovno softversko udruženje (eng. *Business Sofware Alliance,*

BSA) je međunarodno udruženje proizvođača komercijalnog poslovnog softvera i vodeća organizacija koja je svoj rad posvetila promoviranju sigurnog i legalnog *online* okruženja. Programi BSA podupiru tehnološke inovacije kroz inicijative usmjerene na edukacije i zagovaranje politike promicanja zaštite autorskog prava te kibernetičke sigurnosti trgovine i e-poslovanje [15]. Postoje podaci o [16] softverskom piratstvu u zemljama svijeta te u nastavku slijedi grafikon 3 koji prikazuje postotak softverskog piratstva u zemljama svijeta.



Grafikon 3. Softversko piratstvo po zemljama u svijetu

Prema Grafikonu 3, najveći postotak slučajeva softverskog piratstva ima država Armenija (98%). a najmanje imaju Sjedinjenje Američke države (20%). Hrvatska zauzima 66. mjesto po softverskom piratstvu. Usporedo s tim, analiziraju se podaci o postocima softverskog piratstva prema regijama (SAD-Kanada, zapadna Europa, Azija -Pacific, srednji Istok, Afrika, Latinska Amerika, istočna Europa i cjelokupno-svijet (Grafikon 4).



Grafikon 4. Softversko piratstvo prema regijama

Na temelju Grafikona 4. najveći postotak softverskog piratstva zabilježen je u Istočnoj Europi (71%). Drugi najveći postotak zabilježen je kod Latinske Amerike (63%). Treći najveći postotak zabilježen je kod regije Istočna Afrika (56%). Najmanji postotak slučajeva softverskog piratstva zabilježen je u SAD-u i Kanadi. Ovaj zadnji podatak nužno je usporediti s prethodnim podatkom da je SAD zemlja (od svih zemalja u svijetu) koja ima najniži postotak softverskog piratstva. Iz toga se zaključuje da SAD i Kanada ulažu značajne ljudske i financijske resurse u suzbijanje računalnog kriminaliteta poradi očuvanja gospodarske stabilnosti SAD-a i Kanade.

2.2.7. Nezakoniti sadržaji

Prema Preporukama Europske komisije za učinkovito suzbijanje nezakonitog sadržaja na internetu smatra se da je sadržaj nezakonit unutar i izvan interneta [19]. Nadalje, prema njihovim preporukama, nezakonit sadržaj obuhvaća sve informacije koja nisu u skladu s pravom Europske Unije ili pravom država članica, primjerice teroristički sadržaj, materijali koji se odnose na seksualno zlostavljanje djece (Direktiva o suzbijanju seksualnog zlostavljanja djece), nezakoniti govor mržnje (Okvirna odluka o suzbijanju određenih oblika i načina

izražavanja rasizma i ksenofobije kazneno-pravnim sredstvima), poslovne prijevare i zlouporabe (Direktiva o nepoštenoj poslovnoj praksi ili Direktiva o pravima potrošača) ili povrede prava intelektualnog vlasništva (Direktiva o usklađivanju određenih aspekata autorskog prava i srodnih prava u informacijskom društvu) [19]. Uočeno je da postoji razlika terorističkog sadržaja od ostalih nezakonitih sadržaja. Razlog te razlike je zbog uvećanih rizika za građane i društvo. Širenjem terorističkog sadržaja provodi se radikalizacija, regrutiranje i financiranje terorističkih djelovanja te priprema, obuka i poticanje na napade diljem svijeta. Iz tog razloga, ova Preporuka odgovara na potrebu za proaktivnim mjerama i nužnom brzinom ocjenjivanja i djelovanja protiv terorističkog sadržaja, koji je osobito štetan u prvim satima od objave na internetu [19]. Na temelju toga, jasno je da je suzbijanje nezakonitog sadržaja na internetu na razini Europske unije prepoznato kao jedan od ključnih sigurnosnih izazova, osobito nakon terorističkih napada na teritoriju država članica Europske Unije. Istrage su utvrdile da je bilo zlouporaba interneta i društvenih mreža za pripremanje napada [20].

No, po drugoj strani Europska komisija ne donosi propise za sankciju govora mržnje na internetu. Razlog koji je naveden je da bi time ugrozili slobodu izražavanja i medijski pluralizam. Inače, Velika Britanija, Njemačka i Francuska su veoma rigorozne po tom pitanju za razliku od drugih zemalja članica Europske Unije. Komisija se odlučila za jednostavnije rješenje – doradu postojećeg dobrovoljnog kodeksa kojeg su do sada prihvatili Facebook, Twitter i YouTube i koji za sada ostvaruje dobre rezultate [21].

2.3. Kibernetički napad i samoobrana

Pojava interneta značajno je doprinijela organiziranju, širenju i razvoju terorističkih organizacija, jer te organizacije koriste internet kao servis za vrbovanje novih članova, propagiranje svojih ideja i prikupljanje novaca za svoje potrebe i akcije, i to preko svojih stranica [1]. Sve je više prisutan naziv -kiber napad. Kiber napad mora biti koncipiran na način da uključuje poruku prijetnje, ranjivost i ponudu rizika [1].

U cilju što detaljnijeg upoznavanja kiber napada, treba krenuti od Sjedinjenih Američkih Država koje imaju najviše problema sa kibernetičkim terorizmom. Kod njih su uočene tri skupine:

1. prijetnje od terorista koji su sponzorirani od različitih država među kojima su Irak, Iran, Libija, Kuba i dr.
2. Terorističke skupine: libanonski Hezbollah, palestinski Hamas, egipatski AL-Gamat, Al-Islamia

3. Teroristi pojedinci

Autorica Vladica Babić u svojoj knjizi "Računalni kriminalitet" [1] navodi da se sve više koristi visoka tehnologija za realizaciju kibernetičkih napada od strane terorista.

Ide se od postavke da postoje jasno definirani ciljevi napada. Među prvima, navodi se korisnička lozinka. Pomoću lozinke, može se neometano pristupiti računalnom sustavu kroz različita sredstva i načine. Izvor saznanja mogu biti nelojalni službenici bez obzira na motiv kojima su se koristili pri otkrivanju takvih tajnih podataka.

Drugi cilj odnosi se na podatke i informacije koji se nalaze sačuvani u memoriji računala ili se razmjenjuju putem komunikacijskih kanala.

Treći cilj odnosi se na datoteke. Riječ je o datotekama s brojevima kreditinih kartica i kartica za identifikaciju radi pristupa sustavu. Na ovaj način, počinitelji kibernetičkog napada na kartice zloupotrebljavaju za razne financijske transakcije na štetu vlasnika.

Četvrti cilj odnosi se na računalne programe - kibernetički napad može biti u obliku neovlaštenog brisanja ili mijenjanja, kao i u slučaju neovlaštenog kopiranja. Pri skidanju određenog programa, uobičajeno stoji upozorenje da nije dopušteno neovlašteno skidanje odnosno neovlašteno distribuiranje. Može se tu raditi i o distribuiranju glazbe određenog glazbenog umjetnika ili primjerice različitih statističkih paketa kao npr. SPSS 20.0.

Web stranice i *News* grupe su peti cilj kibernetičkih napada. Vrlo česta pojava je da se napad izvodi tako da se neovlašteno promijeni sadržaj. Sve više je službenih napisa o napadima na *web* stranice. Čini se u prvi mah, da je ovo nešto bezazleno. Nipošto, ovi kibernetički napadi predstavljaju veliku opasnost, jer pokazuju da se unatoč svim mjerama i sredstvima zaštite, može pristupiti i promijeniti sadržaj pa čak i preuzeti kontrola nad radom sustava [5]. U prilog tome ide istraživanje pružatelja usluga za internetsku sigurnost (eng. *Internet security assurance services*, ICSA), koji su utvrdili da je 70 posto velikih i srednjih američkih poduzeća i državnih agencija imalo problem, odnosno ozbiljne sigurnosne propuste.

Onemogućavanje korištenja računalnog sustava je situacija kada se ovlaštenom korisniku nastoji onemogućiti korištenje računalnog sustava, ali bez da to učini ugrožavanjem integriteta podatkovne, programske ili tehničke osnovice [5].

I zadnje su napadi na materijalne resurse informacijskog sustava. Sama riječ upućuje na to da je riječ o fizičkim pristupima računalima te krađi istih. Napad dolazi u različitim situacijama i to: tijekom neovlaštenog pristupa tuđem računalnom sustavu, zatim neovlaštenog brisanje podataka, programa, presnimavanje malicioznog programa i korištenje tuđeg računala na mreži za pristup drugom sustavu [5].

Pošto je sve izraženija militarizacija virtualnog prostora, nužno je poduzeti rigorozne korake u samoobrani od kibernetičkog napada. Prema riječima autora Prpića u članku "Osvrt na Tallinnski priručnik o međunarodnom pravu primjenjivom na kibernetičko ratovanje" [22], NATO-ov Centar izvrsnosti za suradnju svjestan je ozbiljnih problema u svezi kibernetičkih napada i potrebe da se poduzmu koraci u obrani od istih. Iz tog razloga, NATO-ov centar izvrsnosti okupio je niz pravnih praktičara i tehničkih stručnjaka u radno tijelo pod nazivom Međunarodna skupina stručnjaka. Cilj okupljanja je izrada priručnika o međunarodnom pravu za primjenu u svijetu kibernetičkog ratovanja [22]. Zadatak radne skupine je ispitivanje načina na koji se postojeće norme međunarodnog prava primjenjuju na kibernetičko ratovanje kao novu formu ratovanja i istodobno razjašnjavanje nekih od složenih pravnih pitanja koja se odnose na kibernetičke operacije. U obranu od *cyber* napada nije uključen samo NATO-ov centar izvrsnosti, postoje druge organizacije koje se bave kibernetičkim prijetnjama, primjerice Međunarodno multilateralno partnertstvo u borbi protiv kibernetičke prijetnje (engl. *International Multilateral Partnership Against Cyber Threats*, IMPACT).

Jasno je da nema zajedničkog pristupa u borbi protiv kibernetičkih terorista i korištenja interneta od strane terorističkih skupina. Iz tog razloga nudi se nekoliko rješenja. Naime, otkako je kibernetički terorizam dobio obilježje transnacionalnog, jedino dolazi u obzir širi međunarodni konsenzus i globalni zajednički napori u borbi protiv kriminalizacije terorističkih akcija u svim oblicima, a to se implementira kroz univerzalnu jurisdikciju međunarodnih sudova koji trebaju privesti pravdi kibernetičke teroriste. Štoviše, potrebno je uspostaviti funkcionalni pravni okvir koji obuhvaća sva odnosna pitanja koja treba rješavati. Od vitalne je važnosti da zemlje koje imaju zajedničku pravnu definiciju "kiber terorizam" kako bi mogli odgovoriti na takvu vrstu transnacionalnog kriminaliteta. Pravno definirani "kiber terorizam" na temelju svojih jedinstvenih obilježja, ne samo da potpomaže istražni proces, već omogućuju suradnju među zemljama. Kada funkcioniraju na taj način, zajedno iznalaze mogućnosti rješavanja slučajeva. Ono što predstavlja problem je veći broj sporazuma koji postoje, a niti jedan od njih ne osigurava obvezujuću regulatornu jurisdikciju. Većina njih djeluju u ograničenim uvjetima i primjenjuju se na regionalnoj razini. Ujedinjeni Narodi i Interpol promoviraju sigurnost i pokušavaju zaštiti i otkloniti kibernetičke napade na međunarodnoj razini. Najznačajniji sporazum u ovom slučaju je "Konvencija o *cyber* kriminalitetu". Premda se Konvencija o *cyber* kriminalitetu kategorizira kao regionalni napor u borbi protiv kibernetičkih napada, ima značajnu ulogu i za brojne zemlje koje su izvan regije, a ratificirale su sporazum te postale članice Konvencije. Ipak, najprominentniji sporazum u području *cyber* kriminaliteta ne obuhvaća *cyber* terorizam.

3. PRAVNA REGULACIJA

U pravilu, jako je teško dokazati računalna kaznena djela [23]. Postoji više razloga za to. Jedan od najjačih razloga je virtualan svijet računala. Kao drugo navode se specifičnosti tehnoloških sustava, zatim kratki rok za moguće dokazivanje (mnogi računalni zapisi se s vremenom brišu) te međunarodne komponente i sl. [23].

"Čak i njihovo razumijevanje traži odgovarajuća stručna znanja - bez odgovarajućeg poznavanja tehnologije je teško uopće shvatiti bit nekih od opisanih računalnih kaznenih djela. Tu naravno može pomoći vještak, ali će biti potrebna i odgovarajuća stručnost svih: policije, Državnog odvjetništva i sudstva." [cit. 23, p.136] .

Jedan od najznačajnijih oblika pravne regulacije računalnog kriminaliteta je *Tallinnski priručnik* koji je kreiran u gradu Tallinnu.

3.1. Tallinnski priručnik

NATO-ov Centar izvrsnosti za suradnju u obrani od kibernetičkih napada pozvao je neovisnu skupinu stručnjaka da kreiraju zakonski priručnik o kibernetičkom kriminalitetu 2009. godine. Kibernetičke operacije počele su sve više privlačiti pozornost međunarodne pravne zajednice krajem 1990. godine. Još značajnije, 1999. godine u Sjedinjenim Američkim državama Pomorsko ratni koledž poduzeo je prvu glavnu pravnu konferenciju o kibernetičkom kriminalitetu. Nakon 11. rujna 2001. godine, transnacionalni terorizam i nastavljeni oružani sukobi odvratili su pozornost s teme sve do pojave jakih kibernetičkih operacija od strane hakera protiv Estonije (2007. godine) i protiv Gruzije tijekom rata s Ruskom Federacijom (2008. godine) kao i kibernetički incidenti poput ciljanje iranskih nuklearnih postrojenja te slučaj Stuxnet (2010. godina) [24]. Upravo zbog tih događaja, Sjedinjenje Američke Države počele su posvećivati posebnu pažnju kibernetičkom kriminalitetu potičući i druge države na to. Na primjer, Nacionalna sigurnosna strategija Ujedinjenog Kraljevstva iz 2010. godine uvela je kategoriju kibernetički na, a to je bio slučaj i u još nekim državama. Istaknuti su još organizirani kriminalitet i terorizam kao jedna od četiri razine prijetnje za britansku nacionalnu sigurnost. Također, Američka nacionalna sigurnosna strategija (2010. godine) navela je kibernetički kriminalitet kao jednu od najozbiljnijih nacionalnih prijetnji javne sigurnosti i gospodarskih izazova. Prema tome, Američko ministarstvo obrane izdalo je svoju Strategiju za djelovanje u "kiberprostoru" što je postavilo "kiberprostor" kao operativnu domenu. Za odgovor na ove prijetnje, SAD je postavio Ured za praćenje kibernetičkih napada.

I na kraju, sve te aktivnosti dovele su do okupljanja niza stručnjaka i formiranja "Tallinnski priručnika". "Talinnski priručnik" prati međunarodne zakone koji se odnose na kibernetičko ratovanje. Glavni dio čine *jus* ad *bellum,* međunarodni zakon koji uređuje način djelovanja država kao instrument njihove nacionalne politike i jus in bello, međunarodni zakon koji regulira pitanje oružanog sukoba. Kibernetičke aktivnosti koje se pojavljuju na razini *korištenja sile* (ovaj izraz je u biti *jus* i *bellum*), kao cyber kriminalitet nisu detaljno opisani. Ne postoje nikakve zabrane o specifičnim kibernetičkim aktivnostima, izuzev onog što se odnosi na "naoružani sukob" za koji se *jus* i *bellum* primjenjuje. Na primjer, Priručnik bez presedana primjenjuje druge međunarodne zakone kao što je međunarodni zakon o ljudskim pravima ili zakon o telekomunikacijama. Ukratko, Tallinnski nije priručnik o kiber-sigurnosti što je učestali izraz. Kibernetička špijunaža, krađa intelektualnog vlasništva i širok spektar kriminalnih aktivnosti u kiberprostoru postaju stvarna i ozbiljna prijetnja za sve države kao i korporacije i pojedince [24]. Iz tog razloga, primjeren odgovor za njih zahtijeva nacionalne i međunarodne mjere. Ipak, Priručnik se ne bavi s tim pitanjima, jer primjena međunarodnog zakona o korištenju snaga i naoružanih sukoba igraju gotovo nikakvu ulogu u tome. Takav zakon više nije primjenjiv za te prijetnje u *cyber* području već u fizičkom svijetu [24]. "Tallinski Priručnik" se temelji na "kiber do kiber" operacijama. Primjeri uključuju poticanje kibernetičkih operacija protiv državne ključne infrastrukture ili *cyber* napada u kojem su cilj neprijateljski zapovjedni i kontrolni sustavi. Priručnik nije usmjeren na razmatranje zakonskih pitanja koji se tiču kinetičkih *cyber* operacija kao što je zračni napad na *cyber* kontrolni centar. Vrlo vjerojatno je da se to ne odnosi na tradicionalne elektroničke napade [24].

Slijedi isječak iz Tallinnski priručnika (Pravilo 1).

"Svrha Prvog poglavlja (Države i kiberprostor) je postaviti pravila za opće međunarodno pravno oblikovanje odnosa zemljama, kiberinfrastrukture i kiber operacija. Prvi dio odnosi se na pitanja suvereniteta država, jurisdikiciju i kontrolu nad kiber infrastrukturu. Dio 2 bavi primjenom klasično javno međunarodnim zakonskim propisima o odgovornosti zemalja prema cyber operacijama.". [cit. 24 p. 44]

U glavnom sadržaju "Tallinski priručnika" piše:

"Glavnom sadržaju Priručnika prethodi popis svih članova Međunarodne skupine i ostalih sudionika, zatim detaljan popis korištenih pravnih izvora te uvodni dio koji se sastoji od nekoliko kratkih poglavlja. " [22, p. 44]

te da je uvodni dio nezaobilazno štivo i preporučuje se svakome tko planira proučavati "Tallinnski priručnik. Uvod opisuje i predstavlja Priručnik te naglašava područje njegove primjene [22, p. 44]. Pripić [22] opisuje kako nakon uvoda slijedi glavni sadržaj Priručnika,

koji se dijeli na dva dijela, i to dio I., koji razmatra pitanja međunarodnog prava kibernetičke sigurnosti, i dio II., koji razmatra pitanja prava kibernetičkog oružanog sukoba. Ti su dijelovi podijeljeni na poglavlja i odjeljke, svaki odjeljak sadrži pravila, čiji ukupan broj iznosi devedeset i pet. Najveći broj pravila (njih 45) nalazi se u četvrtom poglavlju, koje se bavi pitanjima postupanja u neprijateljstvima [22] [cit.45]. I na kraju, glavni urednik Tallinski priručnika objasnio je:

"*Htjelo se stvoriti doktrinarni rad koji bi bio od koristi državama u formiranju vlastitih stajališta i njihovu djelovanju u kibernetičkom prostoru. Nisu se davale preporuke niti definirala najbolja praksa, nije se ulazilo u političke sfere."* [22] [cit.46].

Na temelju tih riječi zaključuje se da Priručnik želi pružiti analizu pozitivnog međunarodnog prava radi pružanja smjernica državama u provođenju njihovih tuzemnih i međunarodnih politika u kibernetičkom prostoru [22][cit.46]. U zaključnim razmatranjima, navodi da daje pozitivnu ocjenu Priručniku unatoč cijelom nizu ograničenja na koja je navedeni autor upozorio [22]. Njegova jedinstvenost proizlazi iz primjene *lex lata* (lat. relativno) na:

"*novo tehnološko okružje jer je kibernetička tehnologija (kakvu danas poznajemo) novina u odnosu na tradicionalna pravila međunarodnoga prava."* [22] [cit.57].

3.2. Internacionalni režimi koji reguliraju računalni kriminalitet

Kada je riječ o internacionalnim režimima koji reguliraju računalni kriminalitet, nameće se pitanje objašnjenja što je računalni režim. Naime, režimi definiraju raspon dozvoljenih akcija ocrtavajući eksplicitne injukcije za izvoditelje. Najrašireniji definicija internacionalnih režima je definicija S. Krasnera koji imenuje internacionalne režime kao "implicitne ili eksplicitne principe, norme, pravila i procedure za donošenje odluka" [25] prema [26]. Ipak, ova definicija smatra se da je preširoka, a J. Mearsheimer nadodaje da takva formulacija koncepta pokriva većinom svaki regularizirani uzorak aktivnosti među zemljama. Daleko restriktivnija definicija navodi da ograničena definicija režime tretira kao multilateralne sporazume među državama, kojima je cilj regulirati nacionalne akcije unutar područnog pitanja [25] prema [27]. Ipak, smatra se da obje definicije zaslužuju pažnju pod jednakim uvjetima. Trenutna kontroverza i neizvjesnost međunarodnog režima za kibernetički prostor nalazi se unutar posebne vrste režima - normi, pravila i postupaka, koji usmjeravaju ponašanje izvoditelja ili pak više ograničeni multilateralni ugovor s fiksnim kaznama za neposluh [25].

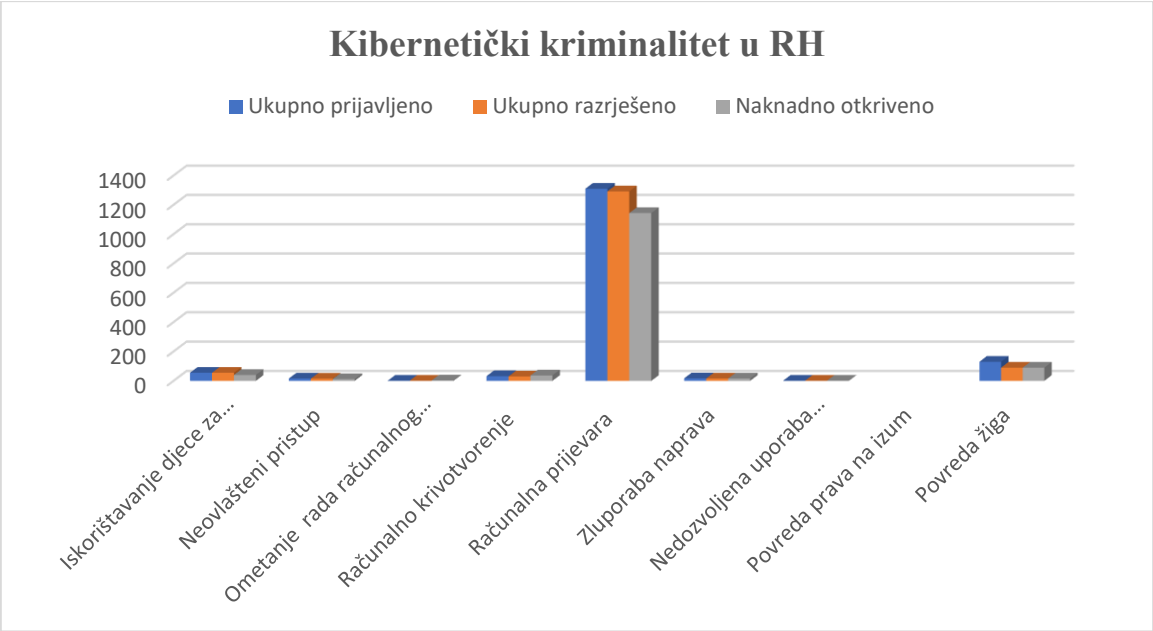
Osim toga, konstruktivistički pristup može biti ključan po ovom pitanju. Konstruktivisti su puno učinili u pokušaju da to objasne. Uz to, konstruktivistički pristup također može osvijetliti proces normalizacije. Konstruktivisti su učinili mnogo posla pokušavajući objasniti

pojavu novih međunarodnih normi. Teorija strateške društvene konstrukcije koju su predložili M. Finnemore i K. Sikkink može pomoći u odgovoru na pitanje kako se može postići režim kibernetičke sigurnosti. Njihov predloženi „životni ciklus“ normi sastoji se od nastanka normi, kaskade normi i internalizacije. Prvo, norma proizilazi iz potrebe za poželjnim ponašanjem dionika, ali nikad ne „ulazi u normativni vakuum“ i mora se natjecati s drugim interesima. Ono što je važno, međunarodne organizacije služe kao platforma putem koje se promiču norme, zahvaljujući njihovoj stručnosti. Razvit ćemo primjer promocije takvih normi za cyber-prostor kasnije u ovom odlomku. Nadalje, institucionalizacija posebnih pravila i načela putem takvih organizacija pomaže razjasniti što je norma i njezino kršenje. Daljnji koraci uključuju uzastopno usvajanje novostvorene norme od strane država, drugim riječima, „kaskade normi“. Finnemore i Sikkink tvrde da se to događa jer države žele zadržati svoj identitet člana međunarodne zajednice, pokazujući tako sukladnost. Konačno, "automatska sukladnost s normom" je internalizacija - ekstremni oblik kaskade normi.

3.3. Kibernetički kriminalitet u Republici Hrvatskoj

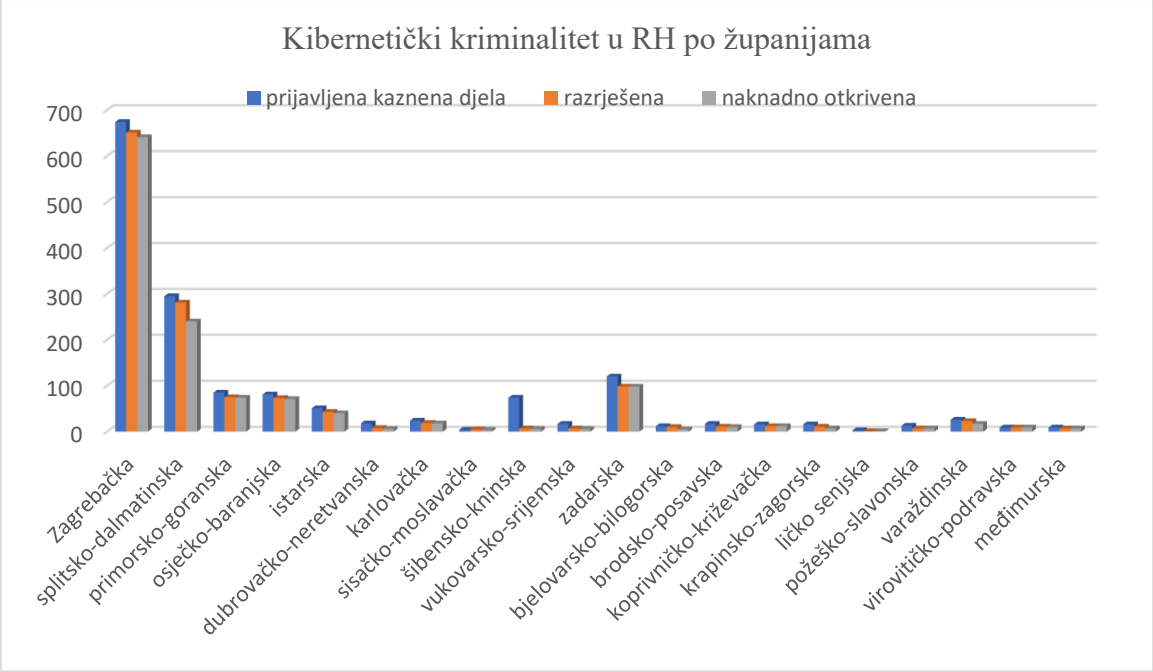
Prefiksalni morfem "kiber", izveden iz grčke riječi *kibernao* (hrv. upravljam, kormilarim), je temeljna polaznica koja opisuje sve izvedene pojmove koji opisuju radnje u prividnom računalnom svijetu, a sam pojam kibernetički odnosi se na znanost o istraživanju i automatskim sustavima kontrole u strojeva i živih bića te istraživanje procesa upravljanja raznim sustavima (biološkim, tehničkim, ekonomskim i dr.) [28]. U nastavku slijedi analiza kibernetičkog kriminaliteta u RH (Grafikon 5). Među oblike kibernetičkog kriminaliteta (prema podacima MUP-a RH) spadaju povreda prava na izum, povreda žiga, računalna prijevara, ometanje rada računalnog sustava, nedozvoljena uporaba autorskog djela, iskorištavanje djece za pornografiju, neovlašteni pristup te drugi oblici, a navedeni su u Grafikonu 5. Ono što je autor Kokot zaključio je da su u kaznenom zakonodavstvu Republike Hrvatske utemeljene odredbe utvrđene Konvencijom o kibernetičkom kriminalu VE i Direktivom EU-a o napadima na informacijske sustave i da te preuzete odredbe slabe njihovu uporabnu vrijednost. Autor Kokot objasnio je da su temeljni pojmovi, kao što su računalni podaci, programi, mreža, u bitnim dijelovima različito prevedeni, protumačeni i kroz zakonski tekst međusobno različito postavljeni [3] i tu nastaje problem. Nadalje, autori Vojković i Štambuk-Sunjić se nadovezuje na to. Oni smatraju kako je termin "kibernetički kriminal" pogrešan prijevod i da je najrazumljiviji termin računalni kriminal ali niti taj termin ne obuhvaća sve oblike društveno neprihvatljivog ponašanja koje regulira Konvencija [23]. Postoji ogroman doprinos informacijsko-komunikacijskih tehnologija razvoju društva i iz tog

razloga potrebno je slobode i prava koje ljudi imaju izvan kibernetičkog prostora osigurati i unutar kibernetičkog prostora, sa svim raspoloživim sredstvima, a kriminalizaciji napada pribjeći tek kao krajnjem sredstvu suzbijanja najtežih od njih [3].



Grafikon 5. Statistički podaci o kibernetičkom kriminalitetu na području Hrvatske [28]

Prema Izvješću Ministarstva unutarnjih poslova o statističkom pregledu temeljnih sigurnosnih pokazatelja i rezultata rada za 2018. godinu, pokazalo se da je najučestaliji oblik kibernetičkog kriminaliteta računalna prijevara (1310 prijavljenih slučajeva) u odnosu na najmanje učestali oblik kibernetičkog kriminaliteta, a to je ometanje rada računalnog sustava (1 slučaj) i nedozvoljena uporaba autorskog dijela (1 slučaj). Nije zabilježen niti jedan slučaj povrede prava na izumu u 2018. godini. Nadalje, slijedi analiza kibernetičkog kriminaliteta po županijama u Hrvatskoj.



Grafikon 6. Statistički podaci o kibernetičkom kriminalitetu po županijama [29]

Statistički podaci Ministarstva unutarnjih poslova za 2018.godinu ukazuju na to da je najveći broj slučajeva kibernetičkog kriminaliteta zabilježen u Zagrebačkoj županiji (674 prijavljenih slučajeva u 2018.godini), zatim u Splitsko-dalmatinskoj županiji (295 prijavljenih slučaja), slijedi zadarska županija (120 prijavljenih slučaja). Zanimljiv podatak je da najmanje slučajeva zabilježeno u ličko-senjskoj županiji (3 prijavljena slučaja). Ličko-senjska županija je po geografskoj konfiguraciji područje koje obiluje zabačenim mjestima te se turistima nudi odmor u izolaciji od vanjskog svijeta, što turisti sve više prihvaćaju što je jedan od glavnih uzroka ovako malog broja slučajeva.

4. POSLJEDICE I PREVENCIJA RAČUNALNOG KRIMINALITETA

Globalni promet ostvaren računalnim kriminalitetom veći je od prometa ostvarenog ilegalnom prodajom droge, tvrde vodeći stručnjaci na području računalne sigurnosti [1]. Ističe se da niti jedna država nije imuna na kibernetički kriminalitet u što je uključena korporacijska špijunaža, dječja pornografija, manipulacije dionicama, različite ucjene te se posebno ističe to da su zemlje u razvoju posebno na udaru. Još početkom dvadesetog stoljeća, Interpol je alarmantno najavio širenje računalnog kriminaliteta i upozorio na formiranje "novog kriminalnog fronta svjetskih razmjera koji se orijentira na pljačku milijunskih svota novaca pomoću računala" [1]. Računalni kriminalitet odgovoran je za milijarde dolara štete godišnje. Procjenjuje se da svake godine uspori veliki dio proizvodnje i globalnog ekonomskog razvoja samim time što postoji. Gotovo svaka tvrtka na svijetu ima problem s računalnim kriminalitetom, izravno ili neizravno. Godišnja procjena američke tvrtke McAfee, vodeće tvrtke u svijetu na području istrebljivanja računalnog kriminaliteta, izvještava o visini štete koju je svjetskome gospodarstvu prouzrokovao računalni kriminalitet u 2015. godini – vrtoglavih 112 bilijuna američkih dolara. Zbog samog postojanja računalnog kriminaliteta, baš kao i postojanja materijalnog kriminaliteta (onog u stvarnom životu), tvrtke i pojedinci prisiljeni su podizati digitalne zidove, svakoga i sve preispitivati, nikom ne vjerovati te koristiti veliku količinu zaštitnog softvera, kao i zaposliti velik broj stručnjaka sve u svrhu obrane od računalnog kriminaliteta od strane pojedinaca, neimenovane grupe ili pak konkurenata. Kazna predviđena za počinitelje računalnog kriminaliteta varira ovisno o veličini počinjenog zločina, ali može biti od obične novčane kazne pa sve do osam godina zatvora. Računalni kriminal neuhvatljiva je pojava te borba protiv njega nije jednostavna. Prvenstveno zato što se on odvija virtualnim putem te za sobom ne ostavlja neki materijalni, opipljiv dokaz. Međutim, računalo jako lako može postati dokazni materijal. Čuvanje starih datoteka ili pak elektroničkih poruka uvelike može pomoći istražiteljima. A čak i ako pojedino računalo nije bilo ono koje je korišteno za samu kriminalnu aktivnost, ono i dalje može sadržavati vrijedne informacije istražiteljima čuvajući log datoteke, koje bilježe određene aktivnosti, promet te komunikaciju između računala i udaljenog servera. U većini država su davatelji internet usluga dužni čuvati te log datoteke svojih korisnika, a nova direktiva iz Europske Unije također propisuje da bi sav promet elektroničke pošte trebalo čuvati minimalno 12 mjeseci.

S obzirom na današnji razvoj tehnologije i interneta, hakersko je znanje dostupnije nego ikad. Prije dvadesetak godina hakeri su morali imati pristup snažnim serverima, posjedovati veliko znanje kako bi uopće mogli upravljati tim serverom, mnogo novca itd. Danas su hakeri odlučili podijeliti to znanje s mlađim naraštajima, što znači da su te informacije dostupne i ostalima, pa tako i policiji i istražiteljima.

4.1. Posljedice računalnog kriminaliteta na štićena dobra i vrijednosti

Poslovni ljudi moraju uzeti u obzir ekonomski učinak računalnog kriminaliteta daleko ozbiljnije, prema riječima istraživača iz poduzeća McAfee, jer trošak računalnog kriminaliteta dostigao je 0,8% BDP-a ili 600 milijardi dolara godišnje. To je više od 0,7% BDP-a u 2014. godini i predstavlja povećanje u iznosu od 34% (445 milijardi dolara), što je prosječni rast od 11,3% za tri godine, do lipnja 2017. godine - to je veoma jak i značajan rast. Europa doživljava najveći ekonomski učinak računalnog kriminaliteta, jer procjenjuje se na 0,84% regionalnog BDP-a koji je usporediv sa 0,78% u Sjevernoj Americi. Ovi podaci su dio zadnjeg izvješća poduzeća McAfee i centra za strateške i međunarodne studije, o ekonomskom učinku računalnog kriminaliteta [31].

Najznačajniji trošak računalnog kriminala proizlazi iz štete koju čini kompanijama i nacionalnim ekonomijama (McAfee 2014). Računalni kriminalitet šteti trgovini, kompetitivnosti, inovacijama i globalnom ekonomskom rastu. Za kompanije i vlade, porast online poslovanja donosi veće sigurnosne troškove.

1. Trgovina:

Sva trgovačka poduzeća suočavaju se sa računalnim kriminalitetom na bilo koji način. Prema Nacionalnoj anketi za sigurnost računala (engl. National *Computer Security Survey*, NCSS), 2005. godine otkriveno je da 67% ispitanih poduzeća otkrilo najmanje jedan oblik računalnog kriminaliteta. Smatraju da je borba protiv računalnog kriminaliteta skupa i uvijek moraju se razvijati novi načini i metode zaštite. Sljedeći primjeri upućuju na posljedice koje računalni kriminalitet ostavlja na poduzeća i kupce. Prvo, to su troškovi zaštite. Poduzeća koja se žele zaštititi od online krađa moraju to dobro platiti. Postoje troškovi identificiranja rizika, građenje novih i sigurnijih operativnih procedura, kupnja zaštitnog softvera i hardvera. Za poduzeća sa kompleksnim i osjetljivim operacijama, ovo često uključuje iznajmljivanje stručnjaka [32]. U posljednjih nekoliko godina pojavila se nova subkultura: kiber-aktivist. To su internetski ekvivalenti prosvjednika koji se vežu za zgrade ili drveće. Njihova je svrha isključivanje mrežnih operacija tvrtke kako bi se poslala poruka o poslovnoj praksi tvrtke. U posljednje dvije godine na ovaj način su napadnute velike korporacije, poput PayPala i

MasterCarda. U prosincu 2010. godine, PayPal web stranica je napadnuta od strane desetak ljudi koji su dio skupine "Anonymous". Pokušali su izvršiti napad za odbijanje usluge u znak odmazde za PayPal gašenje usluga plaćanja putem WikiLeaksa. U tom zločinu je uhićeno više desetina hakera [32]. Paypal nije doživio potpunu blokadu za razliku od drugih poduzeća koji nisu bili te sreće. Napad kod PayPala prouzročio je to da nekoliko korisnika ne može pristupiti PayPal-u. To čak može dovesti do ostvarenja manjeg prihoda duže vrijeme ako se neki značajniji kupci odluče više ne poslovati s poduzećem koje je ranjivo za napad [32].

2.Promjena metoda poslovanja

Računalni kriminal može utjecati na poslovanje na više od financijskih načina. Poduzeća moraju izmijeniti način na koji skupljaju i čuvaju informacije kako ne bih došlo do povrede osjetljivih informacija. Veliki broj poduzeća prestalo je čuvati financijske i osobne podatke korisnika kao što su broj kreditne kartice, socijalni i sigurnosni brojevi te datumi rođenja [32]. Nadalje, takva poduzeća zatvaraju svoje online trgovine zbog toga jer nisu sigurna da ih mogu pravilno zaštititi.

4.2. Pogreške u zaštiti

Većina pogreški u zaštiti računalnih sustava rezultat je ljudskih slabosti bez obzira jesu li uzrokovane čovjekovim neznanjem, nemarom, nedovoljnom pažnjom ili namjernim radnjama. Neke od najčešćih pogrešaka u zaštiti računalnih sustava prikazane su u tablici 1.

Tablica 1 - Pogreške u zaštiti [5]

Postoji nizak stupanj informatičkog obrazovanja korisnika usluga IS-a	Situacija s pogrešnim odabirom lozinki i /ili krivo postavljanja prava (privilegija)
Pojava greški u vlastitom i/ili tuđem softveru i protokolima	Neodgovarajuće implementacije softvera i protokola
Pogrešne konfiguracije računalnog sustava i/ili računale mreže	Korištenje skabih i zastarjelih metoda fizičke zaštite
Nedostatak odgovarajućeg nadzora sustava	Korištenje zastarjelih softverskih i hardverskih metoda i sredstava zaštite
Nekomptabilnosti hardvera i softvera	Nepostojanje ili neprovođenje sigurnosne politike
Postojanje nedostatnih ulaganja u zaštitu i sigurnost informacijskih sustava	Ostalo

Prema tablici 1. može se vidjeti da su to tipične pogreške i one se često susreću u praksi. Jasno je da se hakeri koriste svim mogućim, pa i najmanjim propustima u zaštiti u svrhu postizanja vlastite koristi i materijalnog cilja. Jedna od najuočljivijih pogreški u zaštiti je neodgovarajući nadzor informacijskog sustava. Nadzor obuhvaća skup mjera i sredstava kojima se provjerava pristup i korištenje računalnog ili mrežnog sustava [5, p. 92]. Postoje različiti programi za nadzor nad radom sustava a sve ovisi o tome što određeno pravna ili fizičko lice treba u datom trenutku.

Nadalje, koje će se metode primijeniti ovisit će ponajviše o razini važnosti podataka koji se pohranjuju i obrađuju u informacijskom sustavu unutar lokalne mreže ili daljinski [5]. Dakako da svi podaci ne uživaju isti stupanj povjerljivosti, pa je zato potrebno prije same zaštite napraviti klasifikaciju [5]. Jasno je da niti jedna od danih metoda ne jamči apsolutnu sigurnost i zaštitu od sve brojnih zlouporaba. Ipak se može postići zadovoljavajući stupanj sigurnosti i zaštite inforamcijskog sustava uz kombinaciju sustava i redovitu primjenu. U potpoglavlju o metodama i sredstvima prevencije najbolje su objašnjene kvalitetne metode i sredstva prevencije.

4.3. Metode i sredstva prevencije

Bez obzira na napore koji se ulažu u prevenciji računalnog kriminala, on se i dalje događa. Budući da računalni kriminal nema uvijek vidljivih fizičkih posljedica, može potrajati dok organizacija uopće primijeti da je bila napadnuta. A kada se to i sazna, možda više neće biti u stanju saznati bilo kakvu informaciju o počinitelju. Svako djelo računalnog kriminala je različito, stoga je važno dokumentirati sve što se događa. Zabilježiti i dokumentirati tijekom istrage sve što je *uljez* učinio. To je temeljna zadaća svakog člana tima koji istražuje incident. Prikupljene informacije moći će poslužiti u daljnjem tijeku progona počinitelja, a samoj organizaciji bit će od koristi pri analiziranju sigurnosnih mjera. Djela računalnog kriminala nisu tako očita poput ostalih djela. Nekoliko je načina da znamo da se dogodilo djelo računalnog kriminala. Moguće je zateći počinitelja na djelu. Najjednostavniji primjer za to je oglašavanje alarma, te se počinitelja uhvati u provali, u zgradi ili prostoriji sa računalima. Moguće je dobiti poruku da se dogodilo djelo računalnog kriminala. Često će se počinitelji vole hvaliti pred prijateljima, te opisivati na koji način su počinili djelo. Iako ne postoje dokazi da je računalni sustav napadnut, to je svakako informacija da je sustav ranjiv. Prevencija računalnog kriminala može se promatrati sa aspekta aktivne i pasivne prevencije. U aktivnu prevenciju moguće je ubrojiti procjenu rizika računalnog sustava i njegove vrijednosti, dok se

pod pasivnom prevencijom smatra permanentno obučavanje zaposlenika. Analiza rizika je proces postavljanja pitanja, u prvom redu o prijetnjama koje se nadvijaju nad računalni sustav, zatim o ranjivosti računalnog sustava, te na kraju o protumjerama koje se mogu poduzeti u svrhu zaštite računalnog sustava. Svaki proces analize rizika moguće je opisati sa tri pojma: prijetnja, ranjivost i protumjere. Prijetnja je moguća šteta na računalnom sustavu. Šteta može biti posljedica djelovanja osobe, stvari ili događaja koji može napasti računalni sustav. Ranjivost je točka gdje je računalni sustav podložan napadu. Prijetnja je konkretna namjera ispitivanja ranjivosti računalnog sustava. Protumjere su tehnike zaštite računalnog sustava. Računalna sigurnost se može smatrati trgovinom, a s obzirom na cijenu te sigurnosti samo si najbogatije tvrtke mogu priuštiti zaštitu od svih rizika [33].

Neki od savjeta poslovnih savjetnika su:

Redovito nadograđujte svoj operacijski sustav novim "zakrpama". Isto radite i s drugim programima koje posjedujete. Ukoliko se radi o velikoj tvrtki i nije vam neophodan internet, rezervirajte nekoliko računala za internetski pristup, odnosno fizički odvojite vaše povjerljive podatke od interneta.

Programi koji koriste vatrozid su efikasni u borbi protiv upada. Posebno efikasni su se pokazali hardverski vatrozid uređaji. Obavezna je uporaba antivirusnih programa i *antispyware* programa.

Poštivanje sigurnosne politike tvrtke će isto tako pospješiti sprečavanje kriminalnih radnji nad računalnim sustavom.

Zatražite savjetovanje s tvrtkama koje se bave sigurnosnim konzaltingom, kojih, specijaliziranih samo za to područje, kod nas u Hrvatskoj nema, pa ćete pomoć morati potražiti kod tvrtki koje se bave projektiranjem, ugradnjom i administriranjem računalnih mreža neovisno o tome imate li dva ili tisuću umreženih računala.

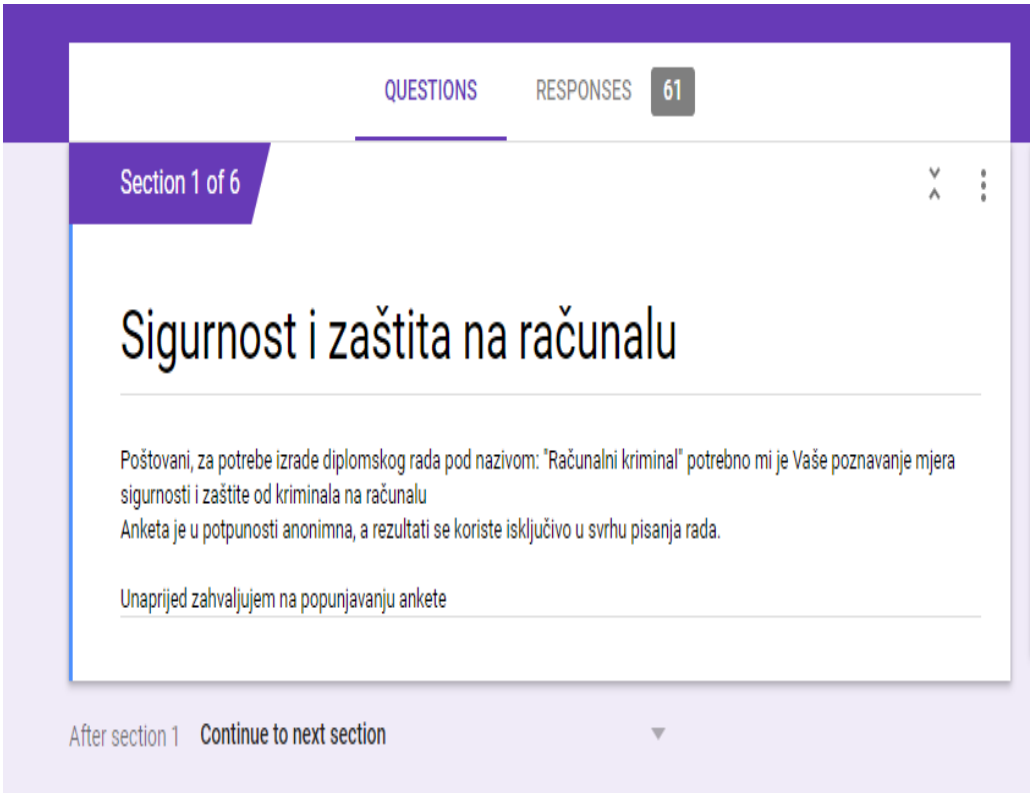
Ako je riječ o poduzeću, potrebno je voditi računa o tome da internetske transakcije, kao i podaci o vašim klijentima budu sigurni, osmisliti politiku poštene uporabe na radnom mjestu i o njoj obavijestite svoje zaposlenike pa je unijeti u pojedinačne ugovore. Iz tog razloga, potrebno je pratiti uporabu interneta kako bi bili sigurni da se ova politika poštuje [34].

5. ISTRAŽIVANJE O RAČUNALNOM KRIMINALU

Istraživanje računalnog kriminala vrlo je složen posao. Za istraživanje računalnog kriminala potrebno je bolje znanje tehničkih specifičnosti od većine ostalih informativnih istraživanja o zamkama primjene elektronike. U današnje vrijeme, računalni kriminal postaje sve raširenija pojava, pa istraživanje računalnog kriminala zahtijeva dodatne ekspertize pridržavajući se pri tome zakonskih propisa. Jedna od referentnih točaka za pristupanje nekom istraživanju je spoznaja o svijesti i običajima populacije unutar koje se istražni postupak provodi. Stoga je u okviru ovog rada izvršeno jedno pilot-istraživanje čiji rezultati bi mogli postaviti jednu takvu referentnu točku.

5.1. Metodologija istraživanja

Tijekom kolovoza 2019. godine provedeno je elektroničko istraživanje o sigurnosti i zaštiti ili, bolje rečeno o svijesti o rizicima i navilama pri korištenju računala za radno sposobne ljude (N=61). Od tog ukupnog broja, 10 ispitanika kojima je upućen poziv, nije ispunilo *online* anketu. Ovo anketno istraživanje predstavlja jezgru rada. Na početku ankete postavljena su pitanja ispitanicima koja se odnose na sociodemografske karakteristike ispitanika (spol, dob, razina obrazovanja, općenito poznavanja rada na računalu te korištenje društvenih mreža. U drugom dijelu anketnog istraživanja, postavljena su pitanja o koracima u provedbi osobne zaštite i sigurnosti na računalima gdje su ispitanici ocijenili koliko su pažljivi u provedbi zaštite i sigurnosti na računalu s rasponom odgovora je od 1 (nikad) do 5 (uvijek). Očekivano je bilo izmjeriti sposobnost ispitanika u prepoznavanju koraka za osobnu zaštitu tijekom različitih aktivnosti na računalu. Također, u trećem dijelu upitnika, očekivano je bilo saznati koje metode ispitanici koriste za održavanje zaštite i sigurnosti na računala, s tim da su imali mogućnost odabira više odgovora (primjerice metoda upotrebe tzv. prepaid kartice gdje korisnik može limitirati sredstva na računu ili prekid komunikacije pri sumnjivim oglasima). U četvrtom dijelu upitnika, očekivalo se saznati kakva su osobna iskustva ispitanika o računalnoj prijevari te na koji način su rješavali to neugodno iskustvo. Vrijeme trajanja anketiranja bilo je od 22.07.2019. do 12.09.2019. godine. Na Slici 2 prikazan je naslovni zaslon elektroničke ankete s kratkim motivacijskim pismom. Za oblikovanje upitnika, provođenje ankete i sažete grafičke obrade rezultata korištena je besplatna usluga Google obrasci, dok je za dodatne analize korišten tablični kalkulator MS Excel.



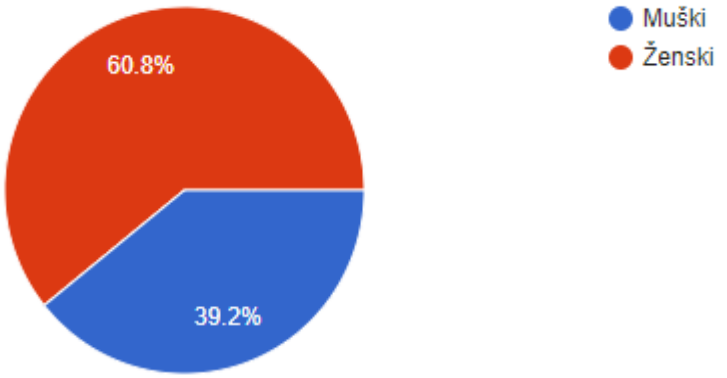
Slika 2. Zaslonski obrazac ankete

5.1. Rezultati istraživanja

Online anketa o sigurnosti i zaštiti na računalu pokazala je niz zanimljivih rezultata koji će u ovom potpoglavlju biti interpretirani te bit će ponuđeni određeni prijedlozi za poboljšanje sigurnosti i zaštite na računalu. U nastavku, slijedi interpretacija sociodemografskih podataka ispitanika o računalnoj sigurnosti i zaštiti. Tablica 2 pruža rezultate deskriptivne statistike o svojstvima ispitne populacije.

Tablica 2. Deskriptivna statistika o populaciji

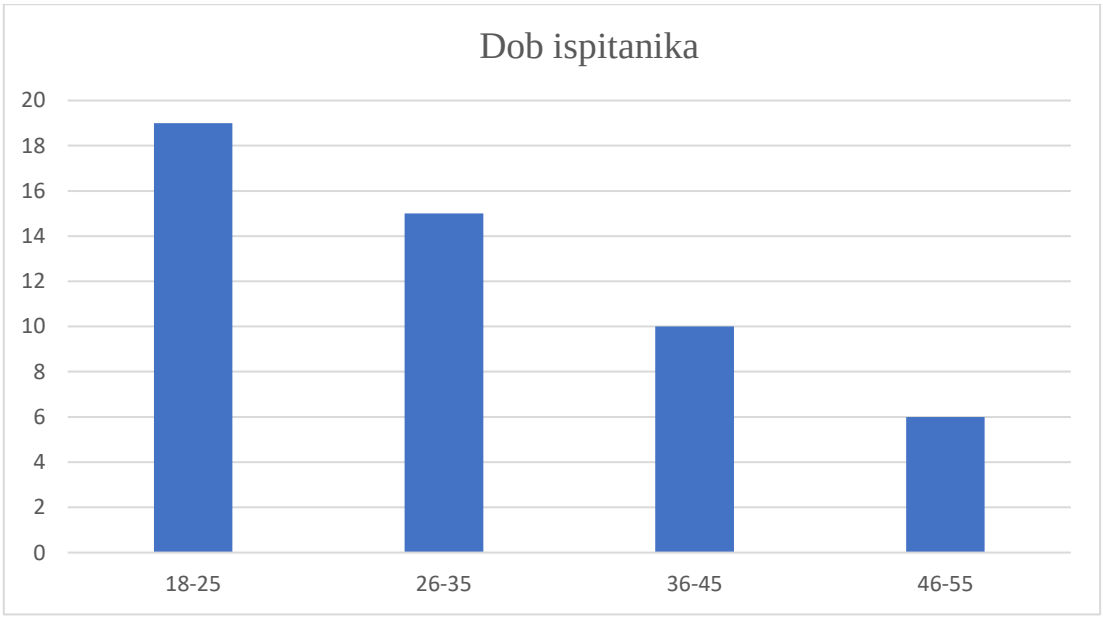
	Spol					
	Muški		Ženski		Ukupno	
dob/stručna sprema	broj	udio	broj	udio	broj	udio
18-25	**10**	**19.61%**	**9**	**17.65%**	**19**	**37.25%**
Magisterij	2	3.92%		0.00%	2	3.92%
SSS	3	5.88%	1	1.96%	4	7.84%
VSS	1	1.96%	6	11.76%	7	13.73%
VŠS	4	7.84%	2	3.92%	6	11.76%
26-35	**5**	**9.80%**	**10**	**19.61%**	**15**	**29.41%**
Magisterij		0.00%	2	3.92%	2	3.92%
SSS	1	1.96%	3	5.88%	4	7.84%
VSS		0.00%	2	3.92%	2	3.92%
VŠS	4	7.84%	3	5.88%	7	13.73%
36-45	**1**	**1.96%**	**9**	**17.65%**	**10**	**19.61%**
Magisterij		0.00%	1	1.96%	1	1.96%
SSS		0.00%	1	1.96%	1	1.96%
VSS	1	1.96%	5	9.80%	6	11.76%
VŠS		0.00%	2	3.92%	2	3.92%
46-55	**4**	**7.84%**	**3**	**5.88%**	**7**	**13.73%**
Magisterij	1	1.96%	3	5.88%	4	7.84%
SSS	2	3.92%		0.00%	2	3.92%
VSS		0.00%		0.00%	0	0.00%
VŠS		0.00%		0.00%	0	0.00%
Doktorat	1	1.96%		0.00%	1	1.96%
Ukupno	**20**	**39.22%**	**31**	**60.78%**	**51**	**100.00%**



Grafikon 7. Raspodjela ispitne populacije s obzirom na spol

Na temelju Grafikona 7, uočeno je da je veći broj ispitanika ženskog spola (60,8%) u odnosu na ispitanike muškog spola (39,2%).

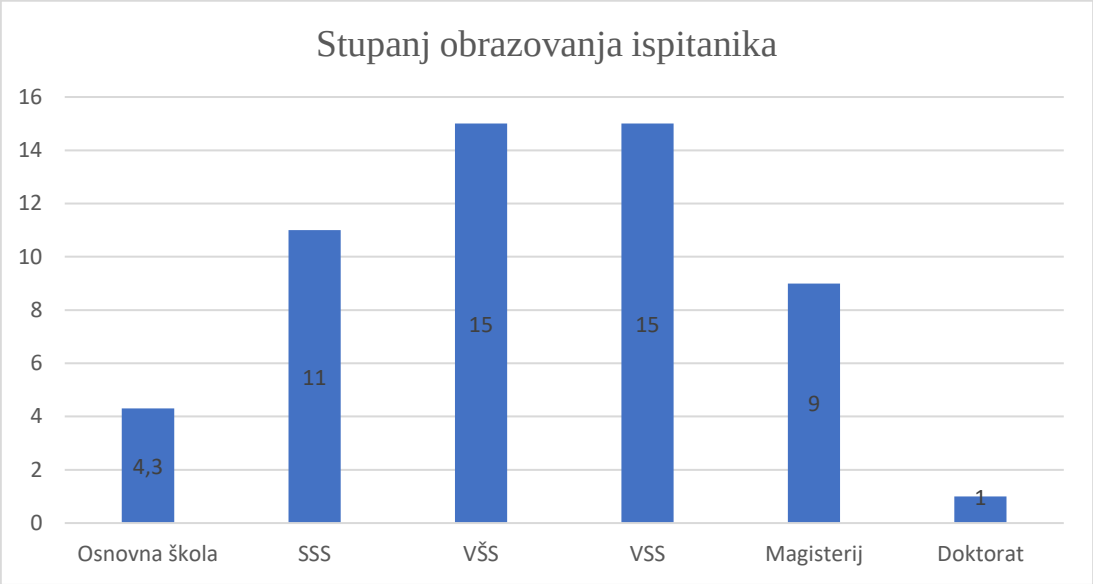
Sljedeće, razmatra se raspodjela ispitne populacije s obzirom na dob ispitanika.



Grafikon 8. Raspodjela ispitne populacije s obzirom na dob

Grafikon 8. pokazuje da najveći broj ispitanika pripada dobnoj skupini od 18-25 godina (37,3%), zatim dobnoj skupini od 26-35 godina (29,4%), slijedi dobna skupina od 36-45 godina (19,6%) i zadnje dobna skupina od 36-45 godina (11,8%). Dobna skupina od 18-25 godina

sačinjavaju populaciju koja je završila srednjoškolsko obrazovanje i krenula na daljnje školovanje, bilo da je riječ višoj ili visokoj razini školovanja.



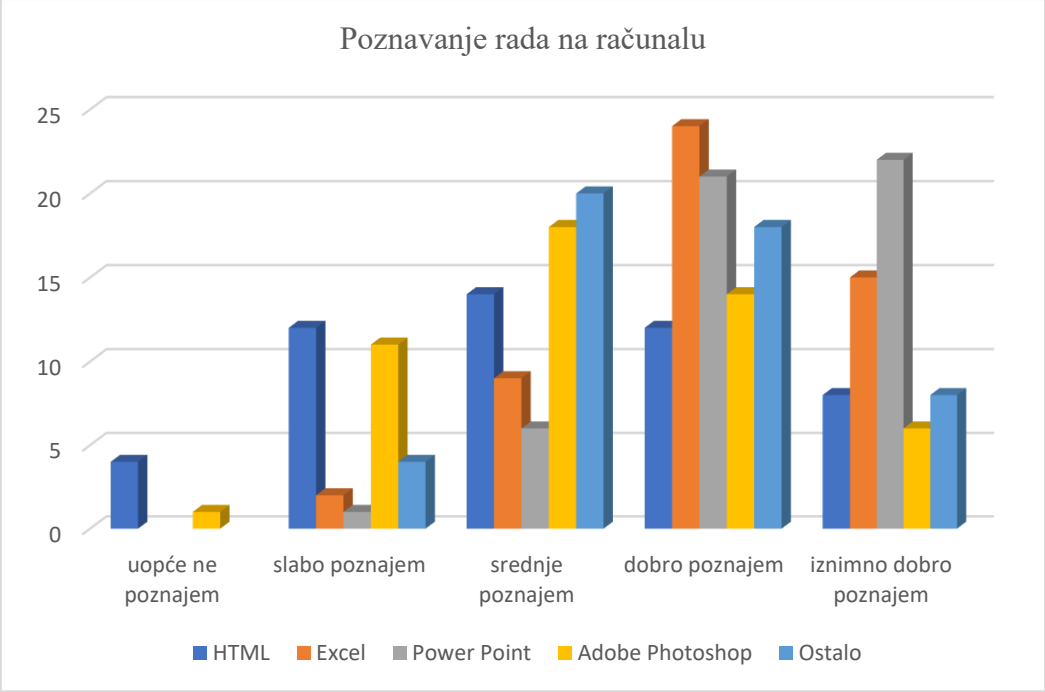
Grafikon 9. Stupanj obrazovanja ispitanika

Prema Grafikonu 9, uočava se da je većina ispitanika ima završenu VSS (29,4%) i VŠS (29,4%). Nakon navedenog stupnja obrazovanja slijede ispitanici koji imaju SSS odnosno srednjoškolsku stručnu spremu (21,6%). 17,6% ispitanika ima završen magisterij. Ispitanici sa završenim doktoratom (2%) pristupili su istraživanju, također.

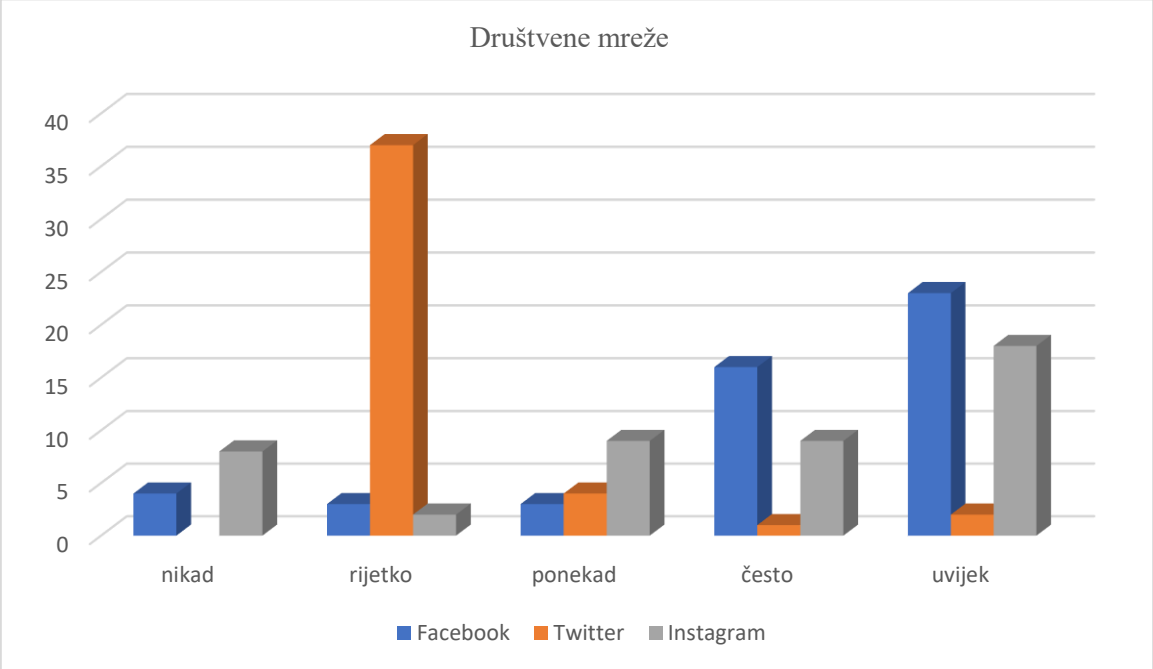
Sljedeći sociodemografski podaci odnose se na podatke o poznavanju rada na računalu, počevši od HTML i drugih programskih alata.

Grafikon 10. upućuje na to da četiri ispitanika ne poznaju HTLM te jedan ispitanik ne poznaje rad s Adobe Photoshop. Nadalje, ispitanici prosječno poznaju Adobe Photoshop i ostalo. Ispitanici dobro poznaju Excel, Power Point i ostalo te iznimno dobro poznaju Power point, Excel i ostalo.

U zaključnim razmatranjima, očito je da ispitanici dobro poznaju rad na računalu u svakodnevnom životu.



Grafikon 10. Poznavanje rada na računalu

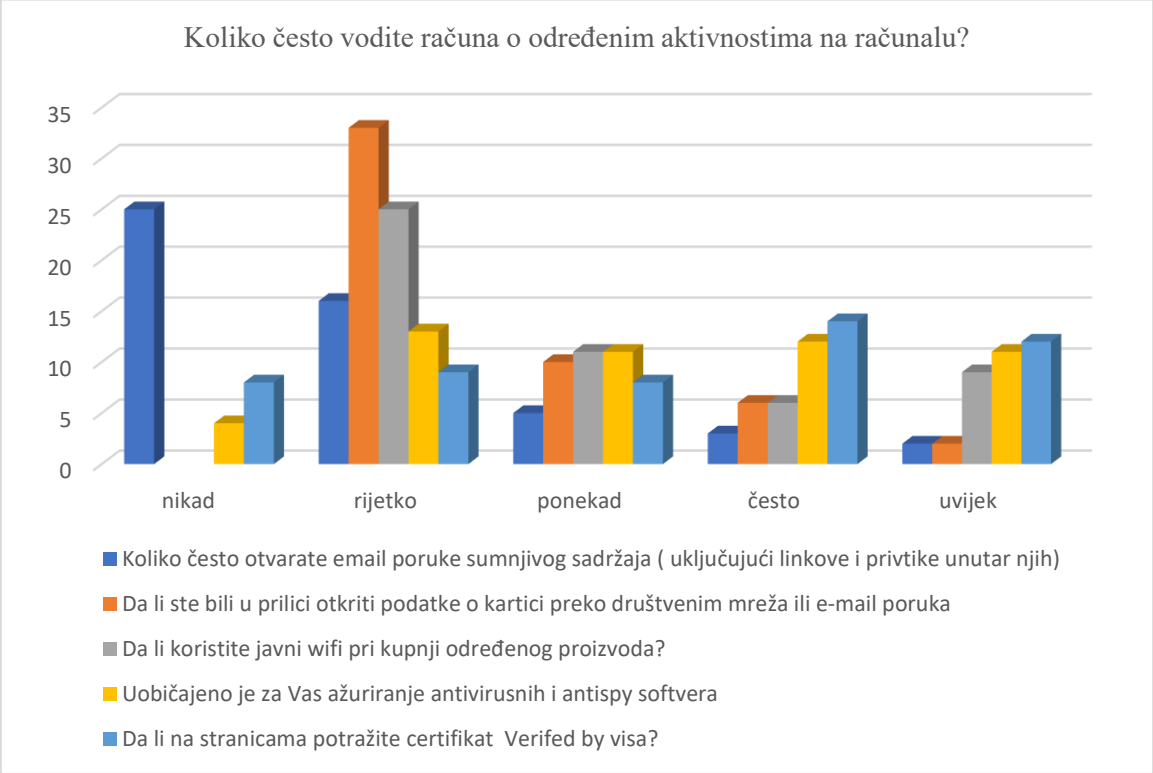


Grafikon 11. Korištenje društvenih mreža

Prema Grafikonu 11, navedene su tri najznačajnije društvene mreže (Facebook, Twitter i Instagram) preko kojih postoje bezbrojne mogućnosti online kupnje te mogućnosti za primjenu računalnog kriminaliteta. Prema podacima iz Grafikona 11, najrjeđe korištena

društvena mreža je Twitter. Nadalje, ispitanici uvijek koriste društvene mreže Facebook i Instagram. Preko Facebooka i Instagrama mogući su različiti oblici kupnje proizvoda. Nerijetko, kupac treba ostaviti određene podatke za kupnju proizvoda.

S ovim dijelom završen je prvi dio anketnog istraživanja o sociodemografskim podacima. Slijedi drugi dio istraživanja koji se odnose na korake u provedbi osobne zaštite i sigurnosti na računalima (Grafikon 12).



Grafikon 12. Skrb o aktivnostima na računalu

Glede koraka u provedbi osobne zaštite i sigurnosti na računalima te odgovora na pitanje "koliko često vodite računa o određenim aktivnostima na računalu" ispitanici su se izjasnili da nikad ne otvaraju e-mail poruke sumnjivog sadržaja, uključujući linkove i privitke unutar njih. Na pitanje o tome da li su bili u prilici otkriti podatke o kartici preko društvenih mreža ili e-mail poruka, većina ispitanika odgovorila je da rijetko otkrivaju podatke o kartici preko društvenih mreža. Na pitanje da li koristite "javni wifi pri kupnji određenog proizvoda", većina ispitanika odgovorila je da rijetko koristi javni wifi pri kupnji određenog proizvoda. Na pitanje o tome da li je uobičajeno ažuriranje antivirusnih i antispy programa, većina ispitanika odgovorila je da rijetko ažuriraju zaštitne programe (13 ispitanika). Na pitanje o tome da li na internetskim stranicama potraže certifikat "Verified by visa", većina ispitanika se izjasnila da

često potraže certifikat “Verified by Visa”. Zadnje pitanje koje su dobili ispitanici odnosilo se na pitanje “da li obraćate pažnju na pravopisne greške i upotrebu žargona”, gdje je većina ispitanika odgovorila da uvijek obrate pažnju na pravopisne greške i žargone.

Glede metoda za održavanje zaštite i sigurnosti na računalu koje ispitanici primjenjuju u svakodnevnom životu, otkriveni su veoma zanimljivi stavovi ispitanika o primjeni metoda istraživanja. U nastavku slijedi Grafikon 13.

Grafikon 13. Metode za održavanje zaštite i sigurnosti na računalu

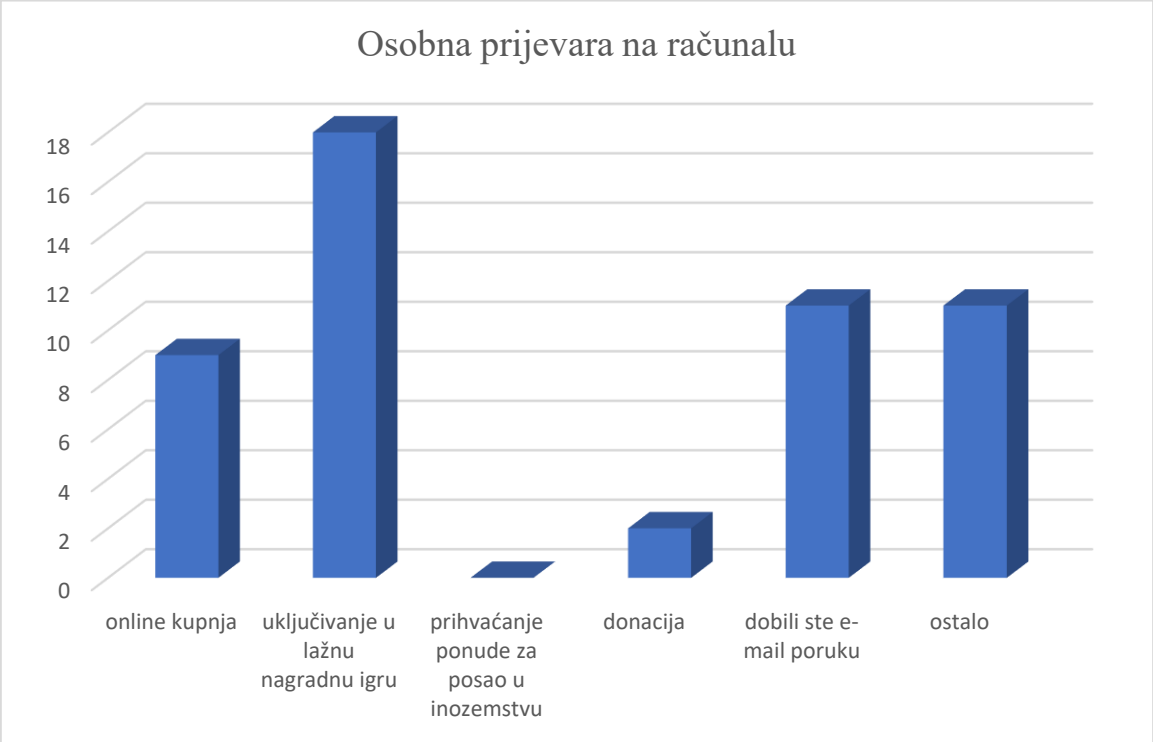
Grafikon 13 pokazuje da ispitanici smatraju da je najbolja metoda za održavanje zaštite i sigurnosti na računalu u biti kupnja na sigurnim stranicama (21,6%), zatim druga najbolja metoda za održavanje zaštite i sigurnosti na računalu je upotreba tzv. *prepaid* kartica (19,6%) Ovo je vrsta kartica kod koje klijent unaprijed "puni" karticu određenim iznosom koji kasnije troši na prodajnim mjestima i samouslužnim uređajima. Kod ove vrste kartica korisnik mora prije transakcije osigurati novac na svome računu. Najčešće su to tzv. “pametne” (engl. *smart*) kartice, odnosno kartice koje sadrže čip koji omogućuje trenutnu identifikaciju i plaćanje obveze uz pomoć odgovarajuće opreme. Ove kartice u suštini zamjenjuju gotovi novac (novčanice i kovinski novac), npr. euroček kartica [35].

Tehnika fišing (engl. *phishing)* je opisana prvi put davne 1987. godine u dokumentaciji i prezentaciji isporučenoj od strane međunarodne korisničke skupine Interex (engl. *HP User Group Interex).* U računalnom žargonu termin *phishing*, izvedenica od *fishing*, što znači

ribarenje ili pecanje, oblik je kriminalnog ponašanja, pri kome se uz upotrebu IKT-a, prikrivanjem pravog identiteta pokušavaju ukrasti, odnosno prisvojiti osjetljivi osobni podaci trećih osoba kao što su korisničko ime, šifra, broj kreditne kartice, broj socijalnog osiguranja, osobni identifikcijski broj i drugi podaci osobe [36].

Po mišljenju ispitanika treća najbolja metoda za održavanje zaštite i sigurnosti na računalu je ažuriranje antivirusnog softvera i instaliranje zaštitnog zida (13,7%). Što se tiče sigurnih metoda plaćanja, 9,8% ispitanika čine prijavu na Verified by Visa ili MasterCard secure Code kada god imaju tu opciju pri kupovini na internetu, 11,8% ispitanika izbjegava phishing poruke u kojima traže povjerljive financijske podatke (npr. pin tekućeg računa), slijedi 7,8% ispitanika koji provjeravaju bankovne izvode, 5,9% ispitanika smatra da je dobra zaštita korištenje najnovijih sigurnosnih zakrpa za pretraživače i operacijski sustav na računalu. Prema mišljenju ispitanika redovito ažuriranje OS-a je najmanje važna metoda u održavanje zaštite i sigurnosti na računalu (2%).

Glede iskustva ispitanika o osobnoj prijevari na računalu, rezultati istraživanja pokazali su zanimljivosti po pitanju osobne prijevare. U nastavku slijedi Grafikon 14.

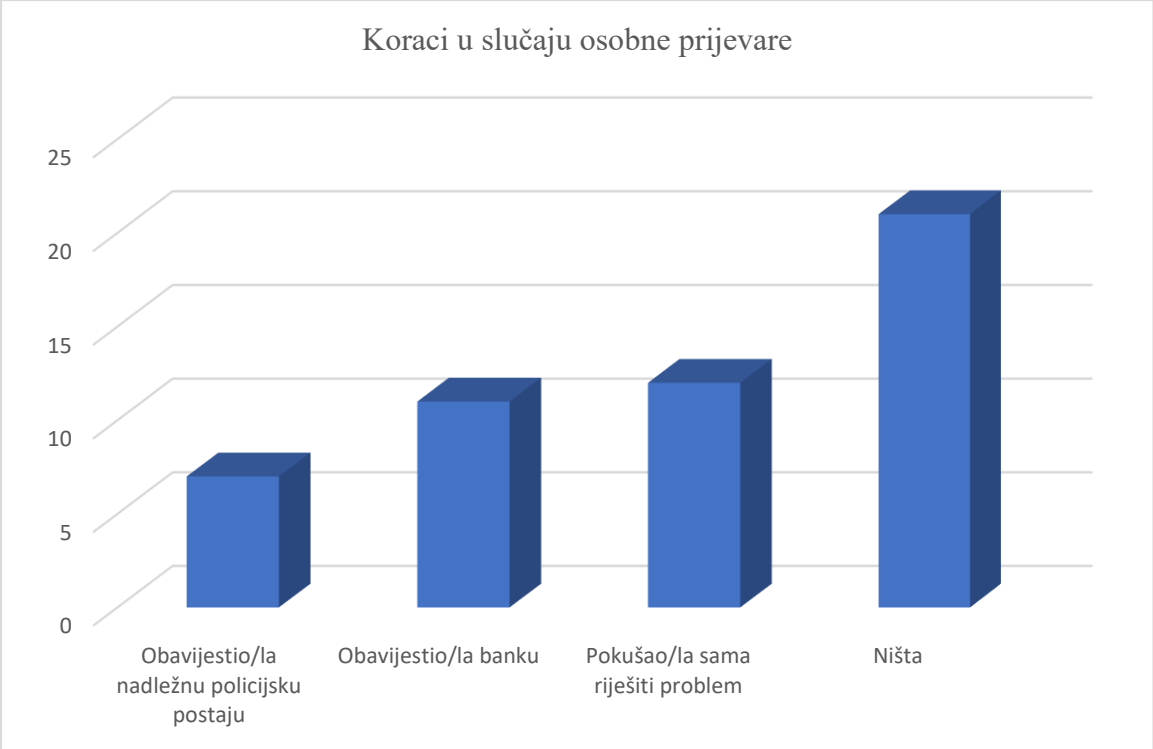


Grafikon 14. Osobna prijevara na računalu

Rezultati istraživanja, prema Grafikonu 14, pokazuju da je najveći broj ispitanika (35,3%) doživjelo osobno prijevaru na računalu u vidu uključivanja u lažnu nagradnu igru.

Često se može vidjeti na društvenim mrežama upozorenje trgovačkih lanaca o tome da oni nisu objavili nagradnu igru, nego da je riječ o lažnoj nagradnoj igri te da upozoravaju da ne daju svoje osobne podatke s osobne iskaznice. Isto to, čine i policijske postaje. Na svojim službenim stranicama upozoravaju građane na prijevare u vidu lažnih nagradnih igara i traženja osobnih podataka. Nadalje, 21,6 % ispitanika izjasnilo se da su dobili dobili e-poštu od nekoga tko tvrdi da je iz njihove banke te se u poruci traži da potvrde detalje o svom računu. Isto tako, 21,6% ispitanika izjasnilo se da je doživjelo druge oblike osobne prijevare na računalu. 17,6% ispitanika izjasnilo se da je doživjelo osobnu prijevaru u vidu online kupovine. Predzadnje zabilježene osobne prijevare na računalu su donacije (3,9%). Vrlo je uobičajena praksa traženja donacija za pomoć određenoj osobi u pitanju rješenja zdravstvenog problema ili ljudi koji su teški socijalni slučajevi pa se poduzima određena akcija. Nisu zabilježene osobne prijevare u vidu prihvaćanja posla u inozemstvu.

Glede koraka koje su ispitanici poduzeli u slučaju osobne računalne prijevare, ispitni rezultati prikazani su u Grafikonu 15.



Grafikon 15. Koraci u slučaju osobne računalne prijevare

Prema Grafikonu 15, uočeno je da, u slučaju osobne prijevare, čak 41, 2% ispitanika nije poduzelo nikakav korak u rješavanju slučaja osobne prijevare. Uz ovaj podatak nadovezuje se podatak da 23,5 % ispitanika sami probavaju riješiti problem kod osobne prijevare na računalu. U nastavku, 21,6% ispitanika obavijestilo je banku u slučaju osobne prijevare dok je

13,7% ispitanika obavijestilo nadležnu policijsku postaju. Ovi rezultati istraživanja su veoma poučni, jer ističu važnost poduzimanja određenih aktivnosti u upoznavanju građana o osobnim prijevarama na računalu i načinima kako riješiti nastali problem.

6. ZAKLJUČAK

U današnjem suvremenom svijetu sve veći broj građana Europske Unije susreće se s nekim od oblika računalnog kriminala što ne začuđuje s obzirom da svako kućanstvo posjeduje jedno ili više računala. No, počelo se sve više postavljati pitanje sigurnosti i zaštite od računalnog kriminala. Povijest računalnog kriminaliteta seže u duboku prošlost da bi ta kategorija danas dobila jedan čvrsti suvremeni okvir, s tim da su se usavršile metode računalnih napada kao na primjer hakerstvo i računalna prijevara. Tijekom pisanja rada, uz pomoć podataka koje objavljuje Ministarstvo unutarnjih poslova uočen je značajan porast računalnih prijevara i računalnog krivotvorenja na području Karlovačke županije. Isto tako, došlo se do spoznaje da SAD i Kanada imaju najmanji postotak piratstva na području krađe softvera, jer ulažu ogromna sredstva u prevenciji istih. Danas općepriznat tzv. "Tallinnski priručnik" koji pruža smjernice državama u provođenju međunarodnih politika po pitanju računalnog kriminaliteta. Posljedice koje ostavlja računalni kriminalitet sve više su nesagledive. Došlo se do spoznaje da je godišnja potrošnja za prevenciju računalnog kriminaliteta iznosi 600 milijardi dolara godišnje. Najviše stradavaju kompanije i nacionalne ekonomije te istovremeno to šteti trgovini, kompetitivnosti, inovacijama i globalnom ekonomskom rastu. U radu je opisan razvoj računalnog kriminaliteta do danas te su prepoznati oblici štetnih pojava na području primjene računala u cilju zaštite života i zdravlja ljudi - radnika te zaštite materijalnih dobara.

Elektroničko istraživanje u ovom radu otkrilo je niz zanimljivosti. Glede računalne pismenosti ispitanika, uočeno je da dobro poznaju uobičajene uredske programske alate. Ukazalo se na činjenicu da članovi ispitne skupine vrše *online* kupnju uglavnom preko tri ključne društvene mreže a to su Facebook, Twiter i Instagram. Ono što je posebno zanimljivo jesu koraci u provedbi osobne zaštite koji se očituju u tome da ispitanici otvaraju poruke sumnjiva sadržaja kao i linkove i privitke, zatim rijetko otkrivaju podatke o kartici preko društvenih mreža, vode računa da ne koriste javni *wifi* za *online* kupnju. No, ono što zabrinjava jeste da rijetko ažuriraju antivirusne programe. Očito je da su svjesni postojanja pojave računalnog kriminaliteta i upoznati su da neke stvari ne smiju činiti, ali ne idu korak dalje, a to je ažuriranje antivirusnih programa u svrhu zaštite. Nadovezujući se to, uslijedio je dio istraživanja koji se odnosi na mišljenja ispitanika o najboljoj metodi zaštite. Većina ispitanika izjasnila se da je najbolja metoda kupnja na sigurnim stranicama a druga metoda je tzv. *prepaid* kartica. Glede osobnih iskustava ispitnika o osobnoj prijevari, spominje se uključivanje u lažnu nagradnu igru. Lažne nagradne igre su veoma učestala pojava i svakodnevno se mogu vidjeti na društvenim mrežama i osim toga, javljaju se stalna upozorenja korisnicima društvenih mreža

o opasnostima lažnih nagradnih igara. Uočeno je još jedno značajno osobno iskustvo ispitanika a to je dobivanje e-mail poruke nekoga tko tvrdi da je iz njihove banke te se u poruci traži da potvrda detalja o računu. Nadalje, rezultati istraživanja ukazali su na jedan veoma zabrinjavajući podatak a to je da velika većina ispitanika ne poduzima nikakve korak u slučaju osobne prijevare ili sami probavaju riješiti nastali problem. Ovo ukazuje ne neophodnu dodatnou edukaciju građana po pitanju prevencije i zaštite od računalnog kriminaliteta. Ovaj rad opisao je značaj računalnog kriminaliteta te doprinjeo prepoznavanju štetnih pojava.

U cilju zaštite života i zdravlja ljudi i radnika te materijalnih dobara, rad je ponudio metode i sredstva prevencije poput savjeta poslovnih savjetnika. Na primjer, redovita nadogradnja operacijskog sustava novim zakrpama. Potvrđena je glavna hipoteza da ispitivanjem navika i stupnja svjesnosti potencijalnih prijetnji od digitaliziranih metoda socijalnog inženjeringa, dobivamo sliku o stanju pojedinca koja se izravno projicira na kolektivnu svijest zajednice. Pogreške u zaštiti su uobičajeno rezultat ljudske pogreške. Iz toga proizlazi nužnost provedbe edukacije građana o zaštiti od računalnog kriminaliteta jer napadi provedeni kroz virtualni svijet računalnih transakcija mogu prouzročiti velike štete u materijalnom tj. stvarnom svijetu. Troškovi iavnih i institucionaliziranih oblika eduakcije vrlo su mali, a mogu spriječiti vrlo teške posljedice koje osim velikih financijskih šteta mogu izazvati ugrozu života i zdravlja ljudi – radnika i znatna oštećenja materijalnih dobara.

Poželjno bi bilo u narednom periodu načiniti novo istraživanje o računalnom kriminalitetu koje bi obuhvatilo još veći broj ispitanika i verificiralo rezultate ovog istraživanja.

7. LITERATURA

[1] V. Babić, Kompjuterski kriminal: metodologija kriminalističkih istraživanja, razjašnjavanja i suzbijanja kompjuterskog kriminala, Sarajevo, BiH: RABIC Sarajevo, 2009.

[2] S. Šimundić, S. Franjić i K. Vdovjak, »HOAX,« *Zbornik radova Pravnog fakulteta u Splitu,* svez. 49, br. 3, pp. 459.- 480., 2012.

[3] I. Kokot , »Kaznenopravna zaštita računalnih sustava,« *ZPR,* svez. 3, br. 3, p. 303-330, 2014.

[4] I. Vuletić i T. Nedić, »Računalna prijevara u hrvatskom kaznenom pravu,« *Zb. Prav. fak. Sveuč. Rij.,* svez. 35, br. 2, pp. 679-692, 2014.

[5] D. Dragičević, Kompjuterski kriminalitet i informacijski sustav, Zagreb: IBS, 2004.

[6] S. Šimundić i S. Franjić, Računalni kriminalitet,, Split: Sveučilište u Splitu, Pravni fakultet, 2009.

[7] P. Hunter, »Computer espionage,« *Computer fraud and security,* br. 7, p. 16, 2003.

[8] »Keylogger,« Raymond computer makes easy, 2019. Dostupno na: https://www.raymond.cc/blog/free-and-simple-keylogger-to-monitor-keystrokes-in-windows/. [Datum pristupanja 7. 9. 2019].

[9] B. Ranabhat, J. Clements, J. Gatlin, T. Kuang-Ting i M. Yampolskiy, »Optimal sabotage attack on composite material parts,« *International Journal of Critical Infrastructure Protection,* svez. 26, 2019.

[10] Središnji državni portal, »Računalne prijevare,« Središnji državni portal, 19 3 2019. Dostupno na: https://gov.hr/moja-uprava/pravna-drzava-i-sigurnost/sigurnost-na-internetu/racunalne-prijevare/1647. [Datum pristupanja: 15. 9. 2019].

[11] Kazneni zakon: Članak 271., *Zakon o računalnim prijevarama,* Zagreb: Narodne novine, 2019.

[12] »Statistika,« 2019. Dostupno na: https://karlovacka-policija.gov.hr/statistika/81. [Datum pristupanja 6. 9. 2019].

[13] »Statistika,« 2019. Dostupno na:https://karlovacka-policija.gov.hr/statistika/81. [Datum pristupanja 6. 9. 2019].

[14] Ž. Panian, Poslovna informatika za ekonomiste, Zagreb: MASMEDIA, 2005.

[15] O. Manuilenko, *Manuilenko, O. (2004). Zaštita softvera i djelovanje BSA u Hrvatskoj.* Zagreb: BSA, 2004.

[16] *Crime-Software piracy rate: Countries Compared*, Nationmaster, 2007.

[17] »Softversko piratstvo,« Nationmaster, 2019. Dostupno na: https://www.nationmaster.com/country-info/stats/Crime/Software-piracy-rate#.. [Datum pristupanja 7. 9. 2019].

[18] O. Manuilenko, *Zaštita softvera i djelovanje BSA u Hrvatskoj.,* BiH, 2012.

[19] Europska komisija - Informativni pregled, *Preporuka Komisije za učinkovito suzbijanje nezakonitog sadržaja na internetu,* EU: EU, 2018.

[20] S. Roksandić Vidlička i K. Mamić:, »Zlouporaba društvenih mreža u javnom poticanju na nasilje i mržnju,« *Hrvatski ljetopis za kaznene znanosti i praksu (Zagreb),* svez. 25, br. 2, pp. 329-357, 2018.

[21] *Europska komisija neće zakonski regulirati govor mržnje na internetu,* EU: EU, 2'017.

[22] R. Prpić, »Osvrt na Tallinnski priručnik o međuarodnom pravu,« *ZPR,* svez. 6, br. 1, pp. 41-59, 2017.

[23] G. Vojković i M. Štambuk-Sunjić, »Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske,« *Zbornik radova Pravnog fakulteta u Splitu,* svez. 43, br. 1, pp. 123-136, 2006.

[24] M. N. Schmitt, »Tallinn manual on the International Law applicable on cyber warfare,« Cambridge University Press, New York, 2013.

[25] I. Stadnik, »What is international cyber security regime and how can we achieve it ?,« *Masaryk University Journal of Law and Technology,* svez. 11, br. 1, pp. 129-154, 2017.

[26] China's Central Military Commission, »Opinion on Further Strengthening Military,« *Information Security Work.,* 2014.

[27] C. S. I. L. Group, »Opinions for Strengthening,« *Information Security Assurance Work,* 2003.

[28] Hrvatski jezični portal, *Kibernetički,* Zagreb, 2019.

[29] »Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018.godini,« Ministarstvo unutarnjih poslova, 2019. Dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%20i%20r. [Datum pristupanja 8. 9. 2019].

[30] »Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2018.godini,« Ministarstvo unutarnjih poslova, 2019. Dostupno na: https://mup.gov.hr/UserDocsImages/statistika/2018/Statisticki%20pregled%20temeljnih%20sigurnosnih%20pokazatelja%. [Datum pristupanja 10 9. 2019].

[31] A. Warwick, »Economic impact of cyber crime is significant and rising,« ComputerWeekly.com, SAD, 2018.

[32] A. Mohr, »3 Ways Cyber-Crime Impacts Business,« Investopedia.Dostupno na. https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx. [Datum pristupanja 13. 9. 2019].

[33] J. Lončar, *Procjena rizika,* Karlovac: Veleučilište u Karlovcu, Odjel sigurnosti i zaštite, 2016.

[34] Plavi ured, »ZICER,« Zagrebački inovacijski centar d.o.o., Dostupno na: https://plaviured.hr/vodici/kako-se-boriti-protiv-e-kriminala/. [Datum pristupanja 11. 9. 2019].

[35] Moj bankar.hr, »PrePaid kartica - definicija - moj-bankar,« 2012. Dostupno na. http://www.moj-bankar.hr/Kazalo/P/PrePaid-kartica.[Datum pristupanja 14. 9. 2019].

[36] B. Miroslav i Ć. Jasmin, »Prevencija računalnog kriminaliteta,« *Policijska sigurnost Zagreb,* svez. 22, br. 1, pp. 146-158, 2013.

8. PRILOZI

8.1. Upitnik

Sigurnost i zaštita na računalu

Poštovani, za potrebe izrade diplomskog rada pod nazivom „Računalni kriminalitet" potrebno mi je Vaše poznavanje mjera sigurnosti i zaštite od kriminala na računalu. Anketa je u potpunosti anonimna a rezultati se koriste isključivo pisanja rada.

Unaprijed zahvaljujem na popunjavanju ankete

Opći demografski podaci

M

Ž

Dob

18-25

26-35

36-45

46-55

66 i više

Stupanj obrazovanja

Osnovna škola ili manje

SSS

VŠS

VSS

Magisterij

Doktorat

Poznavanje rada na računalu

Uopće ne poznajem, slabo poznajem srednje poznajem dobro poznajem iznimno dobro poznajem

HTML

Power Point

Adobe Photoshop

Ostalo

Koje društvene mreže najčešće koristite?

Nikad rijetko ponekad često uvijek

Facebook

Twitter

Instagram

Pinterest

Koraci u provedbi osobne zaštite i sigurnosti na računalima

Za svaku navedenu varijablu na skali od 1 do 5 ocijnite koliko ste pažljivi i provedbi zaštite i sigurnosti na računalu. Raspon odgovora je od 1 (nikad) do 5 (uvijek).

Koliko često otvarate e-mail poruke sumnjivog sadržaja (uključujući linkove i privtike unutar njih)

Da li ste bili u prilici otkriti podatke o kartici preko društvenim mreža ili e-mail poruka

Da li koristite javni wifi pri kupnji određenog proizvoda

Uobičajeno je za Vas ažuriranje antivirusnih i antispy softvera

Da li na stranicama potražite certifikat Verifed by visa

Prilikom kupnje provjerate da svoje podatke ostavljate na sigurnoj stranici koja ima oznaku https://

Obraćate li pažnju na pravopisne pogreške i upotrebu žargon

Metode za održavanje zaštite i sigurnosti na računala

za svaku navedenu varijablu na skali od 1 do 5 ocijenite koje metode primjenjuete u provedbi zaštite i sigurnosti na računalu, s tim da imate mogućnost odabira više odgovora

Koja je metoda po Vašem mišljenju najbolja za održavanje zaštite i sigurnosti na računalu?

upotreba tzv. prepaid kartice gdje korisnik može limitirati sredstva na računu

prekid komunikacije pri sumnjivim oglasima

ažuriranje antivirusnog softvera i instaliran zaštitni zid

korištenje najnovijih sigurnosnih popravki za vaše pretraživače i operativni sustav

izbjegavanje pishing poruka u kojima Vas traže povjerljive financijske podatke (npr. vaš pin)

Kupujete samo na sigurnim stranicama

prijava na Verified by Visa ili MasterCard secure Code kada god imate tu opciju pri kupovini na internetu

svakodnevno provjeravate svoje bankovne izvode i izvode kreditnih kartica

ostalo

Osobna prijevara na računalu

online kupnja

uključivanje u lažnu nagradnu igru

prihvaćanje ponude za posao u inozemstvu

donacija

dobili ste e-poštu od nekoga tko tvrdi da je iz Vaše banke. Poruka može izgledati kao prava i sadržavati logo i obrazac Vaše banke. U poruci se traži da potvrdite detalje o svom računu. Vjerovatno ćete dobiti link putem kojeg trebate poslati poruku ili koji će Vas preusmjeriti na web stranicu gdje će se od Vas tražiti da ostavite lozinku i PIN broj.

Ostalo

Koraci koje ste poduzeli u slučaju osobne računalne prijevare

Obavijestio/la nadležnu policijsku postaju

Obavijestio/la banku

Pokušao/la sama riješiti problem

Ništa

8.2. Popis tablica

Tablica 1. Pogreške u zaštiti……..24

Tablica 2. Deskriptivna statistika o populaciji……..…29

8.3. Popis slika

Slika 1. Keylogger 6
Slika 2. Zaslonski obrazac ankete…….……28

8.4. Popis grafikona

Grafikon 1. Statistički pokazatelji o računalnim prijevarama na području Karlovačke županije 9
Grafikon 2.Statistički pokazatelji računalnog krivotvorenja na području Karlovačke županije 10
Grafikon 3. Softversko piratstvo po zemljama u svijetu.....11
Grafikon 4. Softversko piratstvo prema regijama.....11
Grafikon 5. Statistički podaci o kibernetičkom kriminalitetu na području Hrvatske ..20
Grafikon 6. Statistički podaci o kibernetičkom kriminalitetu po županijama 21
Grafikon 7. Raspodjela ispitne populacije s obzirom na spol.....30
Grafikon 8. Dob ispitanika.....30
Grafikon 9. Stupanj obrazovanja ispitanika.....31
Grafikon 10. Poznavanje rada na računalu 31
Grafikon 11. Korištenje društvenih mreža.....32
Grafikon 12. Skrb o aktivnostima na računalu 33
Grafikon 13. Metode za održavanje zaštite i sigurnosti na računalu 34
Grafikon 14.Osobna prijevara na računalu.....35
Grafikon 15. Koraci u slučaju osobne računalne prijevare.....36