Sigurnost marketinških informacijskih sustava i računalni kriminal

Misir, Eva

Sveučilište Josipa Jurja Strossmayera

Ekonomski fakultet u Osijeku

Sveučilišni diplomski studij Marketing

Eva Misir

SIGURNOST MARKETINŠKIH INFORMACIJSKIH SUSTAVA I RAČUNALNI KRIMINAL

Diplomski rad

Osijek, 2024.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni diplomski studij Marketing

Eva Misir

SIGURNOST MARKETINŠKIH INFORMACIJSKIH SUSTAVA I RAČUNALNI KRIMINAL

Diplomski rad

Kolegij: Marketing informacijski sustav

JMBAG:0010229311

e-mail: emisir@efos.hr

Mentor: prof.dr.sc. Antun Biloš

Osijek, 2024.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
University Graduate Study of Marketing

Eva Misir

SECURITY OF MARKETING INFORMATION SYSTEMS AND COMPUTER CRIME

Graduate paper

Osijek, 2024.

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je diplomski (navesti vrstu rada: završni/diplomski/specijalistički/doktorski) rad isključivo rezultat osobnoga rada koji se temelji na vlastitim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska.* (cc) BY-NC-SA
3. Kojom izjavljujem da sam suglasan/suglasna trajnom pohranjivanju i objavljivanju mog rada u Institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, Repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom Repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).
4. Izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan s dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Eva Misir

JMBAG: 0010229311

OIB:00151790208

e-mail za kontakt: evamisir8@gmail.com

Naziv studija: Diplomski studij Marketing

Naslov rada: Sigurnost marketinških informacijskih sustava i računalni kriminal

Mentor/mentorica rada: prof.dr.sc. Antun Biloš

U Osijeku, 2024 godine

Potpis Eva Misir

SAŽETAK

U radu se definira marketinški informacijski sustav kao suština i temelj svakog marketinškog procesa unutar organizacije, te se analizira računalni kriminal i njegov utjecaj na marketinški informacijski sustav. Kroz analiziranje osnovnih pojmova i predstavljanje istraživanja o sigurnosti na internetu svrha je educirati čitatelje te podići svijest o riziku koji ima računalni kriminal. Moderna tehnologija današnjice osim mnogobrojnih prednosti donosi i neke nedostatke gdje do izražaja posebno dolazi zlouporaba računalnih sustava. Računalni kriminal čine prekršaji tj. ilegalne aktivnosti koje se odvijaju uz pomoć računala, računalnih mreža ili bilo kojih drugih oblika informacijsko-komunikacijske tehnologije. Sa razvojem tehnologije napredovale su i metode uz pomoć kojih napadači vrše ilegalne radnje na računalima. U radu se opisuju metode uz pomoć kojih se napadaju računalni sustavi. Napadači ili izvršitelji mogu imati razne motive kao što su zabava, materijalni interes, ideološki ciljevi ili nestabilno mentalno zdravlje. Osim metoda, objašnjava se i napadačev put do dolaska željenih informacija te načini na koje se treba osigurati i zaštiti računalni sustav kako do ilegalnih napada ne bi došlo. Kako bi se uvidjelo koliko su ljudi informirani o računalnom kriminalu provedeno je istraživanje s ciljem prikazivanja trenutnog stanja u Republici Hrvatskoj s ciljem edukacije i podizanja svijesti o računalnom kriminalu.

Ključne riječi: marketinški informacijski sustav, računalni kriminal, sigurnost na internetu, ilegalne aktivnosti, edukacija i podizanje svijesti

SUMMARY

The paper defines a marketing information system as the essence and foundation of every marketing process within an organization and analyzes computer crime and its impact on the marketing information system. By analyzing basic concepts and presenting research on internet security, the purpose is to educate readers and raise awareness about the risks posed by computer crime. Modern technology today, despite its numerous advantages, also brings some disadvantages, particularly the misuse of computer systems. Computer crime includes offenses, that is, illegal activities conducted with the help of computers, computer networks, or any other forms of information and communication technology. With the advancement of technology, the methods used by attackers to perform illegal actions on computers have also progressed. The paper describes the methods used to attack computer systems. Attackers or perpetrators can have various motives, such as entertainment, financial gain, ideological goals, or unstable mental health. Besides the methods, the paper explains the attacker's path to obtaining desired information and the ways in which a computer system should be secured and protected to prevent illegal attacks. To understand how informed people are about computer crime, a study was conducted to show the current state in the Republic of Croatia, with the aim of educating and raising awareness about computer crime.

Keywords: marketing information system, computer crime, internet security, illegal activities, education and awareness raising

ZAHVALE

Od srca se zahvaljujem svojim roditeljima na neizmjernoj podršci i razumijevanju koje su mi pružili tijekom svih godina mog studiranja. Hvala što ste uvijek vjerovali u mene i omogućili mi da ostvarim svoje snove i dođem do ovog trenutka.

Iskreno se zahvaljujem svom bratu i njegovoj supruzi na podršci i ohrabrenju tijekom svih godina studiranja. Vaši savjeti i prisutnost su mi puno značili na mome putu. Hvala što ste uvijek bili uz mene i dijelili sa mnom svaki korak ovog puta.

Posebno se želim zahvaliti svom voljenom na bezuvjetnoj podršci, ljubavi i strpljenju. Tvoja vjera u mene pomogla mi je da se susretnem sa svim izazovima i ostvarim svoj cilj. Hvala što si uvijek bio uz mene i što si moj najveći oslonac

Neizmjerno sam zahvalna svim svojim prijateljicama i prijateljima na stalnoj podršci. Vaša prisutnost i nesebična pomoć tijekom svih ovih godina studiranja pomogli su da ostvarim svoj cilj i na tome Vam hvala.

Također, zahvala i mome mentoru prof.dr.sc Antunu Bilošu na pruženoj podršci i pomoći tijekom pisanja ovog diplomskog rada.

Sadržaj:

1. Uvod

Cilj ovog rada jest upoznati čitatelje sa temom na način da se pruži jasna slika o marketinškim informacijskim sustavima te računalnom kriminalu. Za početak fokus će biti na oblicima računalnog kriminala , a nakon toga predstavit će se alati i metode uz pomoću kojih se suzbija računalni kriminal. Svrha ovog rada jest analizom i opisivanjem pridonijeti razumijevanju računalnog kriminala kao i podizanje same svijesti o istome. Razrađivanjem osnovnih pojmova, opisivanjem i analizom te provedenom istraživanju ovaj rad želi predstaviti kako računalni kriminal utječe na marketinški informacijski sustav, te u konačnici, ono najvažnije odnosno podizanje svijesti o računalnom kriminalu i njegovo suzbijanje. Fokus analize ovog rada jest na marketinškom informacijskom sustavu i računalnom kriminalu. Marketinški informacijski sustav Harmon (2003) definira kao računalni sustav koji služi za redovit, i na neki način sistematičan protok informacija unutar marketinške organizacije. Uz pomoć marketinškog informacijskog sustava može se postići širok spektar zadovoljavanja informacijskih potreba unutar marketinških organizacija. Među takvim aktivnostima posebno se izdvaja komuniciranje na raznim razinama menadžmenta te dijeljenje informacija, suradnja marketinških stručnjaka s kupcima što rezultira analizama tržišta koje služe za razumijevanje kupčevih preferencija i mnoge druge. Sama digitalizacija koja je danas sveprisutna donijela je jako puno tehnoloških promjena u svijetu, ali osim pozitivnih aspekata stvorio se i prostor za negativne aspekte gdje se posebno ističe računalni kriminal i sve prijetnje koje nosi sa sobom. U akademskoj literaturi popularne su dvije definicije računalnog kriminala. Prvu definiciju oblikovali su Thomas i Loader (2000) koji sugeriraju kako je računalni kriminal niz aktivnosti koje se odvijaju uz pomoć računala koje su ilegalne tj. smatraju se nezakonitima i odvijaju se putem globalnih elektroničkih mreža. Drugu definicije sugeriraju Gordon i Ford (2006) koji govore kako je računalni kriminal oblik kriminalnih radnji koji se odvija uz pomoć računala, mreže ili hardverskog uređaja. Kako bi se čitatelja uvelo u samu temu, u drugom poglavlju pojmovno će se odrediti MIS te računalni kriminal. Nadalje, treće poglavlje će se pozabaviti identifikacijom računalnog kriminala, dok će se u četvrtom poglavlju nastaviti opisivati najznačajniji oblici računalnog kriminala. U petom poglavlju prikazat će se metode i alati za suzbijanje računalnog kriminala. U šestom poglavlju rada predstavit će se istraživanje na temu sigurnosti na internetu. U pretposljednjem poglavlju, raspravi, diskutirat će se o predmetu i problemu istraživanja. U konačnici, u zadnjem poglavlju prikazat će se zaključak.

2. Osnovna obilježja MIS-a i računalnog kriminala

Povezanost između marketinškog informacijskog sustava i računalnog kriminala je velika, te su te dvije stavke ključni predmeti kojima se ovaj rad bavi. U ovom poglavlju analizirat će se definicija, razvoj te podsustavi Marketinškog informacijskog sustava. Također, predstavit će se definicija računalnog kriminala, kako se računalni kriminal razvijao te tko su njegovi izvršitelji. Osim toga, ukratko će se opisati zašto su marketing i računalni kriminal povezani s ciljem predstavljanja teorijske podloge ovog istraživanja kako bi se u konačnici u istraživanju koje će biti predstavljeno nakon teorijske podloge stekao uvid u praktičnu primjenu računalnog kriminala sa željom podizanja svijesti o istome.

2.1 Pojmovno određenje MIS-a

Ružić (2007) smatra kako marketinški informacijski sustav u suvremenom poimanju informacijskog hardvera i softvera nastaje izvorno u SAD 70-ih godina, sa stalnim trendom daljnjeg razvoja. Iz ovoga možemo zaključiti kako trend razvoja marketinških informacijskih sustava eksponencijalno raste i u današnjem, suvremenom poslovanju. Dobiti informaciju u pravo vrijeme je ponekad ključ uspjeha, a to upravo omogućuju marketinški informacijski sustavi. U sljedećih nekoliko poglavlja predstavit će se definicije te razvoj kao i podsustavi marketinškog informacijskog sustava.

2.1.1 Definicija MIS-a

Može se zaključiti kako je pojam marketinški informacijski sustav nastao je spajanjem dvaju pojmova a to su marketing i informacijski sustavi. Za početak razgraničit će se i opisati pojmovi marketing te informacijski sustavi.

Čutura (2018) predstavlja definiciju marketinga prema kojoj se marketing provodi uz pomoć različitih institucija kao aktivnost uz pomoću koje se komunicira, isporučuje i razmjenjuje tržišna ponuda koja donosi vrijednost potrošačima, marketinškim stručnjacima i društvu općenito. Marketing spaja potrošače, marketinške stručnjake i društvo općenito tako da sve strane od toga imaju koristi.

Hrvatska enciklopedija (2024) kaže kako je informacijski sustavi prije svega skup postupaka koji je organiziran, a služi za prikupljanje, pohranu, obradu, prikazivanje i pretraživanje informacija i podataka općenito koji su značajni za državu, društvo, ustanovu ili organizaciju. Iz prethodnoga, može se zaključiti kako informacijski sustavi služe organizacijama za

adekvatno upravljanje informacijama odnosno disperziju informacija prema svim razinama organizacije.

Ružić, Biloš i Turkalj (2014:228) sugeriraju kako je marketinški informacijski sustav odnosno MIS „uspostavljeni sustav opreme, ljudi i organizacije radi podmirenja potreba za marketinškim informacijama. Obuhvaća prikupljanje informacija, njihovo analiziranje i distribuciju donositeljima marketinških odluka“ .

Sljedeća definicija marketinškog informacijskog sustava kako navode Kotler, Keller i Martinović (2014) ukazuje kako je MIS suština i temelj svakog marketinškog procesa unutar organizacije. Uz pomoć marketinškog informacijskog sustava prikupljaju se, analiziraju i isporučuju relevantne informacije donositeljima odluka, služeći kao vrijedno sredstvo u planiranju, provedbi i kontroli marketinških aktivnosti. Ključna odrednica marketinškog informacijskog sustava jest prepoznavanje informacija koje su u datom trenutku potrebne donositeljima odluka pri donošenju odluka. Može se zaključiti kako je MIS u suvremenom poslovanju neizostavan alat upravo zbog svoje odrednice vezano za prepoznavanje informacija koje su potrebne donositeljima odluka. Marketinški informacijski alat pomaže organizacijama postaviti trendove na tržištu, kao i u postavljanju konkurentske prednosti.

Lačić (2016) smatra kako postoje tri temeljna utjecaja na razvoj MIS-a a to su:

- Nezadovoljenje potreba za informacijama;
- Tehnička revolucija;
- Pad cijene računalne opreme tijekom vremena.

Prethodno navedene tri stavke naglašavaju važnost prilagodbe i unaprjeđenja MIS-a suvremenom poslovanju u skladu s promjenama u okruženju.

Proces stvaranja marketinškog informacijskog sustava dugotrajan je proces, te je za njegovo postojanje nužno (Ružić, 2007):

- Viša razina razvijenosti tržišnog gospodarstva;
- Potpuna tržišna usmjerenost gospodarskog subjekta;
- Visoka razina međusobnog komuniciranja unutar i izvan gospodarskog subjekta;
- Prikladne financijske i kadrovske mogućnosti.

Iz prethodno navedenih stavki, može se zaključiti kako proces stvaranja marketinškog informacijskog sustava zahtijeva određeno vrijeme.

Marketinški informacijski sustavi povećavaju broj opcija za donositelje odluka i podržavaju sve aspekte marketinške strategije. Prema Harmon (2002) neke od prednosti MIS-a su:

- Praćenje tržišta;
- Razvoj strategije;
- Implementacija strategije;
- Funkcionalna integracija.

Uzevši u obzir prethodno napisane prednosti može se zaključiti kako marketinški informacijski sustav značajno doprinosi funkcioniranju organizacije, kao i donositeljima odluka pri donošenju odluka.

2.1.2 Razvoj informacijskih sustava

U ovome dijelu rada opisat će se evolucijske razine tj. razvoj informacijskih sustava. Kako bi uopće došlo do samog razvoja MIS-a potrebno je zadovoljiti određene stavke koje organizacija mora posjedovati, a prema Lačić (2016) to su:

- Visoka razina razvijenosti tržišnog gospodarstva (ekonomije);
- Potpuna tržišna orijentacija organizacije;
- Integracija marketinga s ostalim poslovnim funkcijama;
- Visoka razina interne i eksterne komunikacije;
- Odgovarajuće kadrovske i financijske mogućnosti.

Iz navedenih stavki može se zaključiti kako je za kvalitetan i uspješan razvoj informacijskih sustava potrebno uskladiti sve gore navedeno kako bi organizacija djelovala i na pravi način iskoristila sve pogodnosti (marketinških) informacijskih sustava. Stoga, bez svih gore navedenih preduvjeta razvoj samog marketing informacijskog sustava ne bi bio moguć.

Razlikujemo 4 vrste razvojnih oblika informacijskih sustava u koje se ubraja i marketing informacijski sustav. Dakle prema Sveučilištu Minnesota Libraries Publishing (2016) razlikujemo:

1. Transakcijski informacijski sustavu;
2. Izvještajni informacijski sustavi;
3. Sustavi podrške pri odlučivanju;
4. Ekspertni sustavi.

1. Transakcijski informacijski sustavi

Prema Laudon i Laudon (2004) transakcijski informacijski sustavi pružaju informacijske poput prodaje, prihoda, novčanih depozita, obračuna plaća, odluka o kreditu te protoka materijala u tvornici, a navedene informacije služe operativnoj razini menadžmenta za praćenje osnovnih aktivnosti. Dakle, može se zaključiti kako je transakcijski informacijski sustav vrsta računalnog sustava koji obavlja i bilježi rutinske transakcije potrebne za svakodnevno poslovanje. Dvije su glavne svrhe transakcijskog informacijskog sustava. Prva je odgovaranje na uobičajena pitanja, dok je druga praćenje toka transakcija unutar organizacije. Najbolji primjer transakcijskog informacijskog sustava jest sustav za obračun plaća. Osim toga, ovi sustavi mogu pružiti podatke o povijesti isplata zaposlenika za izračun osiguranja, mirovina i dr. Ukoliko dođe do neuspjeha ovog sustava posljedice mogu biti ozbiljne te dovesti do zatvaranja tvrtke. Stoga, iz navedenog može se zaključiti kako transakcijski informacijski sustavi predstavljaju najveću prednost za operativnu razinu upravljanja, iz jednostavnog razloga što je to razina koja je zadužena za svakodnevne (rutinske) aktivnosti.

2. Izvještajni informacijski sustav

Prema Laudon i Laudon (2004) izvještajni informacijski sustavi pružaju redovite informacije koje služe za donošenje odluka u organizaciji. Glavni cilj izvještajnih informacijskih sustava jest formiranje pravodobnih izvještaja koji pomažu menadžerima da surađuju na operativnoj i taktičkoj razini. Ova vrsta sustava pomaže u poboljšanju svakodnevnih situacija u poslovanju, a sama primjena može poboljšati usklađenost poslovnih ciljeva sa organizacijskim. Prethodno se utvrdilo kako je operativna razina zadužena za svakodnevne (rutinske) aktivnosti, dok je taktička zadužena za analiziranje podataka za planiranje aktivnosti. Primjena izvještajnih sustava može biti npr. praćenje kako prodajno osoblje radi na različitim područjima.

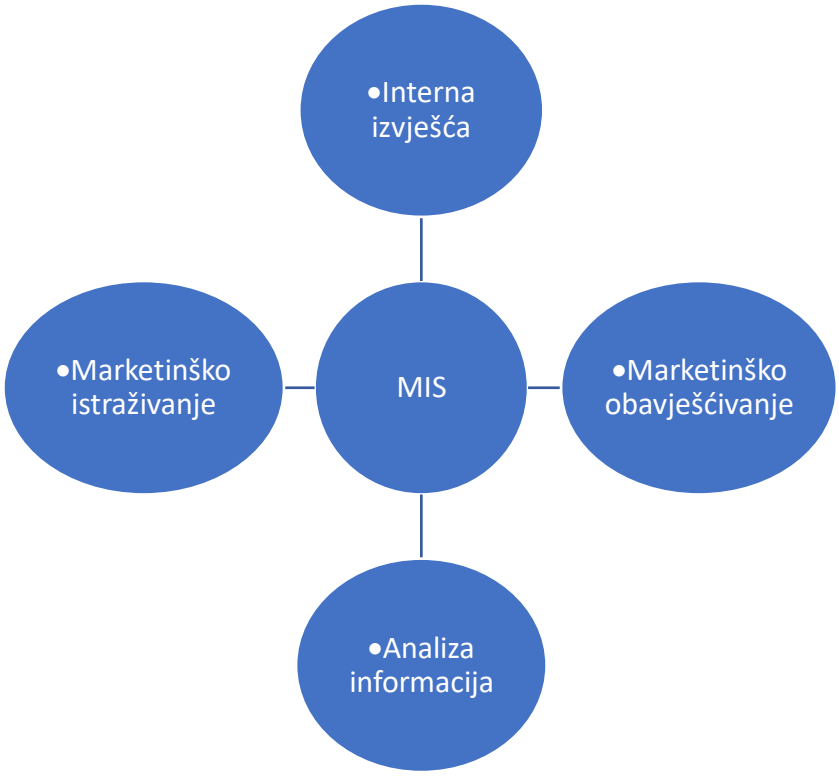
3. Sustavi podrške pri odlučivanju

Uz pomoć informacijskih sustava donošenje odluka se proširilo na sve razine menadžmenta pa tako i niže razine zaposlenika mogu sudjelovati u procesu donošenja odluka. Laudon i Laudon (2004) smatraju da poboljšanje u procesu donošenja odluka pomaže poduzećima kroz uštede troškova i povećanja prihoda. Postoje tri vrste odluka, a to su strukturirane, polustrukturirane i nestrukturirane. Viši menadžment se suočava sa nestrukturiranim odlukama, srednji menadžment sa polustrukturiranim, dok niži menadžment donosi nestrukturirane odluke.

4. Ekspertni sustavi

Prema Laudon i Laudon (2004) ekspertni sustavi su inteligentna tehnika za hvatanje implicitnog znanja u specifičnom i ograničenom području ljudske stručnosti. Ovi sustavi služe za prikupljanje znanja kvalificiranih zaposlenika u obliku skupa pravila u softverskom sustavu koji mogu koristiti drugi u organizaciji. Osim toga, ekspertni sustavi su podložni umjetnoj inteligenciji i zbog toga nemaju širinu znanja i razumijevanje temeljnih principa kao ljudski stručnjaci. Ekspertni sustavi obično obavljaju zadatke kao što su dijagnosticiranje neispravnog stroja ili odobravanje kredita. Također, problemi koji su složeni i koje ljudski stručnjaci ne mogu riješiti u kratkom vremenskom periodu preteški su za ekspertne sustave. S druge strane ekspertni sustavi pomažu organizacijama u donošenju odluka s manje ljudi.

2.1.3 Podsustavi MIS-a



Grafikon 1: Podsustavi MIS-a

Izvor: Izrada autora prema Khosrow-Pour (2017)

1. Interna izvješća

Podsustavi internih izvješća služe kako bi marketinški menadžeri otkrili važne prilike i potencijalne probleme o narudžbama, prodaji, cijenama, troškovima, visini zaliha, primicima i

plaćanjima. Identificiramo nekoliko vrsta internih izvješća a to su ona o narudžbama, prodaji, cijenama, troškovima, visini zaliha, primicima i plaćanjima, prema Kotler, Keller i Martinović (2014).

Prema Khosrow-Pour (2017) podsustav internih izvješća prikuplja, analizira, interpretira i distribuira potrebne informacije iz raznih odjela tvrtke. Za upravljanje internom bazom podataka neke tvrtke imenuju odbor koji se bavi svim aspektima internih funkcija kroz sljedeće funkcije. Prema Khosrow-Pour (2017) to su:

a) Odgovori na zahtjeve za svim vrstama informacija od strane menadžera;
b) Određivanje izvora informacija i alata potrebnih za prikupljanje, evaluaciju i analizu informacija;
c) Prezentacija, distribucija i ažuriranje informacija;
d) Rješavanje pritužbi zaposlenika;
e) Sve vezano za informacije.

2. Marketinško obavješćivanje

Khosrow-Pour (2017) smatra da marketinško obavješćivanje opskrbljuje menadžere podacima o događanjima. Osim toga, pomaže u sprječavanju iznenađenja i problema zaposlenika zbog promjena u okruženju te minimizira rizik za tvrtku.

Kotler, Keller, Martinović (2014:71) navode da „sustav marketinškog obavješćivanja čini niz postupaka i izvora koje menadžeri koriste kako bi dobili svakodnevne informacije o događajima u marketinškom okruženju.“ Svrha ovog podsustava je stvoriti podatke o onome što se u stvarnosti dogodilo. U ovome podsustavu do informacija se dolazi u knjigama, novinama te publikacijama ali i razgovorima s klijentima, distributerima ili dobavljačima prema mišljenju autora Kotler, Keller i Martinović (2014). Ovaj podsustav MIS-a mora imati legalne i etične informacije, a do same njihove kvalitete može se poboljšati uz pomoć motivacije osoba koje sudjeluju u samome procesu. Prethodno navedeno može utjecati na samu konkurentnost poduzeća, a ista se može poboljšati osim motiviranjem i edukacijom osoba koje sudjeluju u procesu. Prema Kotler, Keller i Martinović (2014) postoji 8 koraka uz pomoć kojih se radi na poboljšanju i kvaliteti samih marketinških podataka a to su:

- Obuka i motiviranje prodajnog osoblja da uočava nova događanja i o njima izvješćuje;
- Motivirati distributere, maloprodavače i druge posrednike da prenose važne informacije;

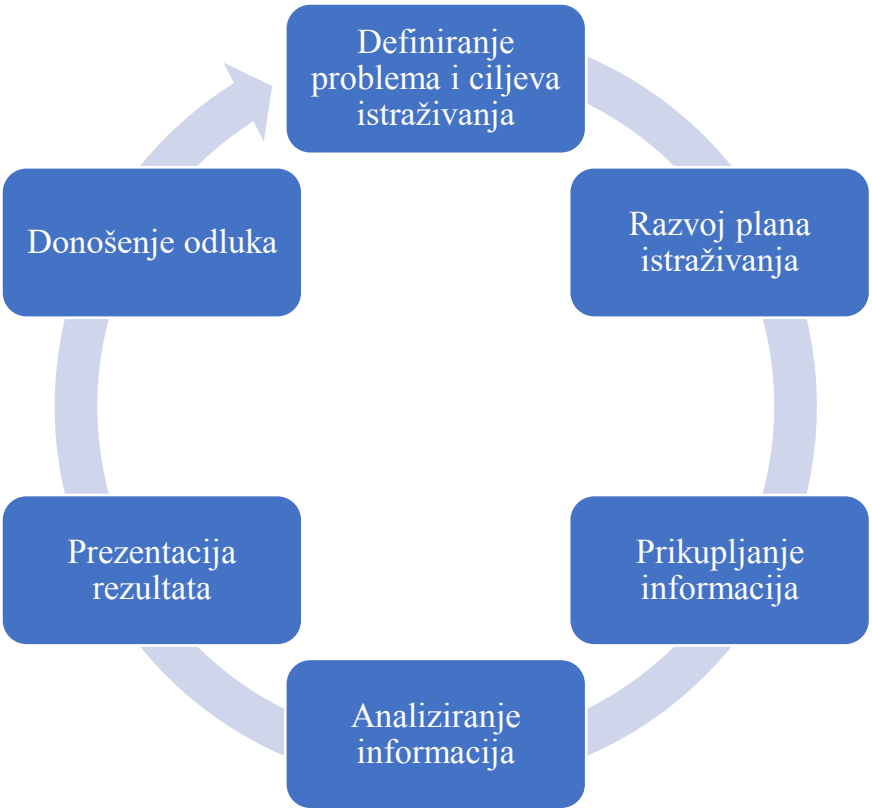
- Kako bi se prikupili podaci treba zaposliti pomoć izvana;
- Širenje vanjske i unutrašnje mreže;
- Osnovati savjetodavni odbor koji čine kupci;
- Iskoristiti vladine izvore podataka;
- Kupnja informacija od vanjskih poduzeća za istraživanje tržišta i vanjskih dobavljača.

Provođenje ovih osam koraka zasigurno dovodi do razvoja marketinškog informacijskog sustava, a kontroliranje i kontinuirano prilagođavanje i poboljšanje u ovim koracima dovodi do konkurentske prednosti same organizacije.

3. Marketinško istraživanje

U situaciji kada menadžeri trebaju specifične informacije o nekom problemu sa marketinškog područja koriste se marketinška istraživanja. Prema Khosrow-Pour (2017) marketinško istraživanje jest sustavno osmišljavanje prikupljanja, analize i izvještavanja o podacima za specifične marketinške situacije u kojima se određena tvrtka nalazi.

„Marketinško istraživanje definiramo kao sustavno oblikovanje, prikupljanje, analizu i izvješćivanje o podacima i nalazima relevantnim za specifičnu marketinšku situaciju s kojom je poduzeće suočeno.“ (Kotler, Keller, Martinović, 2014:98). Osim toga, koristi se i kod prenošenja dobivenih rezultata menadžmentu. Može se zaključiti kako je ovaj podsustav ključan u procesu donošenja odluka u marketing informacijskom sustavu. Sam proces marketinškog istraživanja sastoji se prema Kotler, Keller i Martinović (2014) od 6 koraka. U nastavku slijede prikazani koraci.



Grafikon 2: Proces marketinškog istraživanja

Izvor: izrada autora prema Kotler, Keller i Martinović (2014)

Na grafikonu je predstavljen proces marketinškog istraživanja koji pomaže pri prikupljanju, analizi i izvješćivanju informacija koje su od velike važnosti za marketinške situacije u organizaciji.

4. Analiza informacija

Podsustav analize informacija naziva se još i sustav podrške u odlučivanju za marketing. Za razliku od prethodna tri podsustava koji opskrbljuju podatke, sustav podrške u odlučivanju bavi se analizom dostupnih informacija. Prema Khosrow-Pour (2017) analiza dostupnih informacija može poboljšati učinkovitost i korisnost cijelog marketinškog informacijskog sustava. Ovaj podsustav je zapravo proširenje i nastavak na prethodne, te se u sklopu njega koriste razni statistički alati, novi modeli i softveri kako bi se pomoglo menadžerima u analizi, planiranju i kontroli njihovih operacija.

2.2 Pojmovno određenje računalnog kriminala

U nastavku opisat će se računalni kriminal kao nastavak na temu marketinških informacijski sustavi. U nastavku opisat će se pojam računalnog kriminala, kako je nastao računalni kriminal te tko su njegovi izvršitelji. Za kraj kratko će se opisati poveznice između marketinškog

informacijskog sustava i računalnog kriminala. Razvojem računalne tehnologije došlo je i do njezine zlouporabe što je dovelo do pojave računalnog kriminala.

2.2.1 Definicija računalnog kriminala

Prema McGuire i Dowling (2013) računalni kriminal su prekršaji koji se mogu počiniti isključivo upotrebom računala, računalnih mreža ili bilo kojih drugih oblika informacijsko-komunikacijske tehnologije. Računalni kriminal uključuje širenje virusa ili sličnih zlonamjernih softvera, hakiranje te mnoge druge slične napade. Iz prethodnoga može se zaključiti kako je važno razumjeti sve prijetnje koje donosi računalni kriminal kako bi se razvile strategije zaštite od istih.

Prema Šimundić i Franjić (2009) razlozi iz kojih dolazi do računalnog kriminala jest jednostavna upotreba moderne informacijske tehnologije i sama činjenica da je ona niskog cjenovnog ranga. Također, autori navode još neke od „želja za bavljenjem računalnim kriminalom“ a to su jednostavnost, dostupnost, želja za dokazivanjem i brzom zaradom. Iz prethodnoga može se zaključiti kako je današnja tehnologija napredovala pa je i suzbijanje računalnog kriminala zasigurno lakše, brže i jednostavnije no što je to bilo u prošlosti. „Računalni kriminalitet je svako kazneno djelo počinjeno posredstvom posebnog znanja ili stručne uporabe računalne tehnologije. Praksa kaže da je kaznenih djela počinjenih posredstvom posebnog znanja sve manje, a da ih je sve više počinjenih izravnom ili neizravnom uporabom računalne tehnologije.“ (Šimundić i Franjić, 2009:31)

Šimundić i Franjić (2009), također navode najjednostavniju definiciju računalnog kriminala, a to je ona koja ukazuje da je računalni kriminal vrsta zločina počinjena na računalu ili računalnom sustavu.

Iz svih definicija može se zaključiti kako računalni kriminal predstavlja ozbiljnu prijetnju današnjoj modernoj informacijskoj tehnologiji. Naravno, danas je tehnologija napredovala pa je tako napredovao i sam računalni kriminal. Zbog navedenoga važno je podizanje svijesti o kibernetičkom kriminalu kako za pojedince ukoliko gledamo privatno korištenje računala, tako i za organizacije i poslovni svijet.

2.2.2 Nastanak i razvoj računalnog kriminala

Zanimljiva činjenica koju navode autori Šimundić i Franjić (2009) jest da je računalni kriminal nastao pojavom električnog tabulatora 1887. godine. Ukratko, to je stroj koji je radio na bušene kartice, a koristio se za dobivanje statističkih podataka. U tadašnje vrijeme to je bilo veliko

otkriće i sa samom pojavom električnog tabulatora stvorena je podloga za njegovu zlouporabu, u tom slučaju na financijski dio poslovanja.

Ukoliko promatramo konkretno računalni kriminal modernijeg doba, on je zabilježen prema Šimundić i Franjić šezdesetih godina 20. stoljeća kada su se pojavili tzv. *phreakeri* (osobe koje rabe različite metode kako bi besplatno koristile telekomunikacijske usluge). Tzv. *phreakeri* su otkrili kako zloupotrijebiti telekomunikacijske usluge, a nedugo nakon toga otkrili su kako zloupotrijebiti informacijsku tehnologiju.

Prema Šimundić i Franjić (2009) početkom sedamdesetih godina pojavile su se provale u osobna računala uz pomoć malicioznih programa. Također, tada su se stvorili i prvi hakeri, tj. osobe koje su ukazale na bezbroj načina zloupotrebe računalnog kriminala. Stoga, iz svega navedenog može se zaključiti kako računalni kriminal seže u daleku prošlost te se može od samog početka tehnologija može zloupotrjebljavati.

Nažalost, računalni kriminal je tijekom vremena napredovao i postao globalnim problemom. Prema Šimundić i Franjić (2009) računalni kriminal je napredovao pojavom interneta, te su u novije vrijeme i terorističke organizacije počele zloupotrebljavati Internet. Zbog niza problema koji su se počeli javljati zbog napretka tehnologije razvijene zemlje svijeta su odlučile pronaći rješenje za računalni kriminal te su se u nacionalna zakonodavstva uvela nova kaznena djela. Prema Šimundić i Franjić (2009) prvi rezultat je Konvencija o kibernetičkom kriminalu (dokument Vijeća Europe). Dokument je potpisan od strane članica Europske unije, te država koje žele postati (među njima je bila i Republika Hrvatska).

Babanina et al. (2021) sugeriraju kako je razvojem informacijske tehnologije došlo do pojave računalnog kriminala, što je rezultiralo potrebom za analizom , proučavanjem i razvijanjem protumjera. Pitanja informacijske sigurnosti, zaštite i osiguranja informacija na računalu od velikog su značaja u cijelome svijetu. Jedan od ključnih faktora za razvoj računalnog kriminala jest internet, zbog čega je postao jednim od većih problema današnjice. Tvrtke i podjedinici ne mogu zamisliti danas svoje živote bez interneta, dok su druge strane izvršitelji računalnog kriminala uvidjeli u tome priliku za zlonamjernim stjecanjem novca.

Osim toga, prema Babanina et al. (2021) povijest računalnog kriminala se dijeli na dva razdoblja. Prvo razdoblje je od stvaranja prvog računala pa do 1990., dok je drugo razdoblje od 1990. pa sve do danas.

2.2.3 Izvršitelji računalnog kriminala

U digitalnoj eri u kojoj se društvo nalazi tehnologija je dio svakodnevnice. Sa sobom nosi svoje prilike i prijetnje. Prijetnje mogu biti osobe koje nazivamo izvršiteljima računalnog kriminala koji koriste ilegalne radnje i prijevarom dolaze do informacija i podataka za koju nemaju dozvolu dobiti ih. Prema Šimundić i Franjić (2009) u počecima takve osobe su rabile neke od najjednostavniji tehnika kao što su lozinke i pogrešne konfiguracije. Kako je tehnologija napredovala, i Internet se razvijao tako su napredovale i osobe koje se bave izvršenjem računalnog kriminala. Razvojem tehnologije oprema je postala svima dostupna, te uz osnovno informatičko znanje razvio se i računalni kriminal. Kada su se podaci (u velikim) količinama počeli pohranjivati na jednom mjestu otvorio se veoma jednostavan put izvršiteljima računalnog kriminala. Prema Šimundić i Franjić (2009) počinitelji računalnog kriminala mogu se podijeliti u pet skupina:

1. Osobe koje to čine iz puke zabave;
2. Osobe koje to čine iz materijalnih pobuda;
3. Oni koji se rukovode nekakvim ideološkim ciljevima;
4. Psihički nestabilne osobe;
5. Profesionalni kriminalci.

Iz gore navedenog može se zaključiti da sve osobe imaju isti cilj a to je počinjenje ilegalnih radnji koje su štetne za okolinu.

Prema Babanina et al. (2021) izvršitelje računalnog kriminala možemo klasificirati u dvije skupine. Prva skupina su oni napadači koji imaju visoku razinu znanja o računalnom kriminalu, tzv. elita. Druga skupina napadača su osobe koje su dobile unaprijed pripremljeni algoritam koji osigurava provedbu određenih procedura. Najveću prijetnju današnjice predstavlja prva kategorija napadača, a njihove karakteristike su prema Babanina et al. (2021:16):

- „sposobnost izvršenja kriminalnih djela anonimno, tajno;
- kriminalna djela najbolje se odvijaju u prekograničnoj jurisdikciji različitih država;
- visoke profesionalne i intelektualne sposobnosti hakera;
- mogućnost kombiniranja raznih računala u jedan mehanizam za izvršenje kriminalnih djela u automatiziranom režimu;
- odsutnost ili dugotrajno kašnjenje žrtve u shvaćanju da je izvršeno kriminalno djelovanje;
- prisutnost velikog broja žrtava hakerskog napada;

- nema potrebe da haker dođe u izravan kontakt s žrtvom svog ilegalnog djelovanja.“

2.2.4 Marketinški informacijski sustav i računalni kriminal

U samome početku ovog rada navedeno je kako marketing informacijski sustav služi za prikupljanje informacija, njihovo analiziranje i distribuciju donositeljima marketinških odluka. Također, MIS se predstavlja kao temelj svakog marketinškog procesa unutar organizacije. Ono što se može zaključiti iz ovog poglavlja jest da je poveznica između računalnog kriminala i MIS-a upravo u prikupljanju informacija. Marketing informacijski sustav prikuplja, analizira i na kraju donosi informacije donositeljima odluka, dok se računalni kriminal definira kao ilegalno prikupljanje informacija te zlouporaba istih. Zaključak je da se Marketing informacijski sustav mora zaštiti od računalnog kriminala. Za početak edukacijom i prepoznavanjem istog te u konačnici primjenom metoda i alata za suzbijanje računalnog kriminala. Kako sve to učiniti, i koji su sve oblici računalnog kriminala prikazat će se u nastavku.

3. Identifikacija i reakcija na računalni kriminal

Samo otkrivanje računalnog kriminala je složen proces, koji ukoliko se dogodi zahtjeva niz mjera koje se moraju provesti u svrhu suzbijanja računalnog kriminala. Računalni kriminal predstavlja ozbiljnu prijetnju današnjem modernom i digitaliziranom svijetu te su iz tog razloga identifikacija i reakcija na računalni kriminal ključni elementi u procesu njegova suzbijanja koji će se predstaviti u ovom poglavlju.

3.1 Identificiranje računalnog kriminala

Računalni kriminal je izrazito učestao na globalnoj razini te je stoga važno uložiti velike napore u njegovo suzbijanje. Kod računalnog kriminala jako je teško ući u trag osobama koje to čine iz razloga što nerijetko nema fizičkih dokaza. Prema Šimundić i Franjić (2009) potrebno je voditi računa o tri situacije a to su sljedeće:

- Definirati određene mjere kako bi se moglo što brže prepoznati da je došlo do ilegalne radnje, točnije računalnog kriminala;
- Definirati tim ljudi koji su zaduženi za krizne situacije kao što je računalni kriminal;
- Definirati reakcije prethodno „stvorenog“ time na različite situacije.

Iz prethodnoga da se zaključiti kako je zapravo najvažnija stavka formiranje tima koji je stručan za suzbijanje računalnog kriminala. Također, tim mora imati određenu strategiju u procesu suzbijanja i osim toga tu strategiju s vremenom mijenjati i prilagođavati u zavisnosti od situacije. Bača (2004) navodi od kojih se sve članova treba sastojati tim koji upravlja kriznim situacijama. Članovi tima su sljedeći:

1. Voditelj tima;
2. Operater na sustavu;
3. Nadzornik;
4. Istražitelj;
5. Tehnički savjetnik.

Također u samom procesu identifikacije pa sve do trenutka kada se otkrije počinitelj potrebno je sačuvati svu dokumentaciju kako bi nadležni organi mogli na što jednostavniji način utvrditi počinitelja. Prema Šimundić i Franjić (2009) postoje dvije mjere detekcije računalnog kriminala. Prve mjere su proaktivne i one detektiraju računalni kriminal tijekom izvršavanja ili prije nego što se dogodi radnja koja se naziva računalni kriminal. Druge mjere su reaktivne i detektiraju računalni kriminal u tijeku ili nakon što se dogodi kazneno djelo. Naravno, kako

napreduje tehnologija tako napreduju i djela iz područja računalnog kriminala pa se mjere s vremenom moraju usavršavati i prilagođavati. Autori Šimundić i Franjić (2009) navode kako je potrebno provoditi kontrole kao što su usporedbe podataka kod sudionika transakcija, ovjere isprava osoba koje unose podatke, kontrole pribavljača podataka, provjere računala i analiziranje spisa. Iz navedenih elemenata može se zaključiti da je uz dovoljno velike mjere opreza računalni kriminal moguće i spriječiti. Ukoliko se gore navedeni elementi implementiraju rizik od računalnog kriminala može se značajno smanjiti.

3.2 Postupci u borbi protiv računalnog kriminala

Sukladno napretku današnje tehnologije i njezinim razvijanjem pojavljuje se sve više stručnjaka sa istim ciljem, a to je razvijanje metoda sprječavanja računalnog kriminala. Izazov u tome je što se razvijanjem metoda sprječavanja računalnog kriminala razvija te napreduje i računalni kriminal. Autori Šimundić i Franjić (2009) navode nekoliko mjera kojih bi se trebalo pridržavati u situaciji računalnog kriminala a one su sljedeće:

1. Pridržavanje mjera identifikacije;
2. Sastavljanje tima stručnjaka koji su zaduženi za odgovore na kaznena djela;
3. Spremnost na mijenjanje planova tijekom vremena.

Osim prethodno navedenog važno je u timu imati ljude različitih stručnosti kako bi se što bolje odgovorilo na računalni kriminal. Naravno da je logičan slijed da kako raste stopa računalnog kriminala tako će rasti i broj stručnjaka koji se bave ovim područjem. Također, osim pridržavanja tri koraka u situaciji kada dođe do računalnog kriminala i tima u kojemu je važno da se sastoji od ljudi različitih stručnosti, autor Bača (2004) navodi tri glavna pravila ukoliko dođe do napada na računalni sustav:

1. Poštivanje mjera za otkrivanje;
2. Formiranje tima za upravljanje kriznim situacijama;
3. Fleksibilnost u izmjeni postojećih planova.

Pristup samom suzbijanju računalnog kriminala, kada do njega dođe zahtijeva određena znanja i vještine tima predviđenog za takve situacije. Osim toga, nakon što se identificira računalni kriminal i provede nekoliko mjera sljedeći korak jeste prijavljivanje računalnog kriminala.

U Republici Hrvatskoj postoje 2 vrste sankcioniranja računalnog kriminala a to su kazna zatvora i novčana kazna. Osim ove vrste koja je i najrigoroznija postoje i mjere koje se izriču

maloljetnicima a to su mjere upozorenja, sigurnosne mjere te odgojne mjere prema autorima Šimundić i Franjić (2009).

3.3 Pogreške u računalnoj sigurnosti

U današnjem modernom i digitaliziranom svijetu svakodnevnica je prožeta korištenjem tehnologije. Samim time povećava se i rizik korištenja, tj. dolazi do računalnog kriminala. Pogreške u računalnoj sigurnosti mogu imati velike posljedice kako za pojedinca tako i za velike organizacije. U nastavku će se navesti deset najčešćih pogrešaka koje se uz educiranje i podizanje svijesti o računalnoj sigurnosti mogu izbjeći. Prema mišljenju Muncaster (2022) neke od najčešćih pogrešaka u računalnoj sigurnosti su sljedeće:

1. Kliktanje na sumnjive poveznice i otvaranje nepoznatih privitaka;
2. Preskakanje ažuriranja uređaja;
3. Spajanje nasumičnih USB uređaja;
4. Korištenje jednostavnih lozinki duži vremenski period;
5. Nedostatak dvofaktorskog autentifikacijskog sustava (2FA);
6. Odbijanje izrade sigurnosnih kopija na uređajima;
7. Odvlačenje pažnje;
8. Korištenje poslovnih uređaja u poslovne svrhe;
9. Nepažnja;
10. Izostanak sigurnosnih softvera na svim uređajima.

Iz prethodno navedenih pogrešaka u računalnoj sigurnosti može se zaključiti kako one predstavljaju velike izazove u današnjem svijetu digitalizacije. Ovih deset pogrešaka predstavlja stvari koje korisnici najčešće čine uglavnom zbog nedovoljno edukacije. Sve ove pogreške mogu utjecati na stvari poput gubitka osobnih podataka ili financijskih sredstava.

3.4 Posljedice računalnog kriminala

Prema Milnsbridge (2024), tvrtki koja pruža IT usluge postoje 4 vrste posljedica računalnog kriminala.

1. Prekid poslovanja

Kao prva posljedica izdvaja se prekid poslovanja. Ukoliko dođe do bilo koje vrste računalnog kriminala ukoliko gledamo sa pozicije jedne organizacije moguće je da će biti nedostupna nekoliko sati, možda čak i dani. To bi značilo da svaki proveden sat ili dan označava velike financijske gubitke u poslovanju.

2. Osobni i financijski gubitak

Može doći i do osobnih gubitaka ukoliko osoba koja je podvrgnuta napadu nema dovoljno znanja i vještina o računalnom kriminalu. Financijski gubici mogu biti na razini pojedinca ili organizacije. Ukoliko promatramo organizaciju to bi značilo da su mogući zastoji kod isplata plaća djelatnicima, troškovi samog rješavanja računalnog kriminala i gubitak prihoda općenito.

3. Uništena reputacija

Osim prekida poslovanja, osobnih i financijskih gubitaka moguće je i dugoročna uništena reputacija. Ukoliko promatramo sa stajališta organizacije, jako je važno da suradnici, klijenti ili krajnji korisnici imaju povjerenje u vaše poslovanje. Ukoliko dođe do računalnog kriminala samim time reputacija je uništena i gubi se povjerenje.

4. Zakoni i kazne

Od svi prethodno navedenih posljedica, ova se može promatrati kao najteža i najozbiljnija. Zemlje diljem svijeta su donijele zakone koji govore o tvrtkama koje nepravilno postupaju ili zloupotrebljavaju osjetljive podatke.

4. Oblici računalnog kriminala

U prethodnom poglavlju zaključilo se kako se tehnologija može zloupotrijebiti i kako se takve situacije identificiraju. Postoji bezbroj načina na koji se računala mogu zloupotrijebiti a u ovom poglavlju predstavit će se neki od najčešćih oblika manipuliranja računalima. Prema Karabašić (2002) računalni kriminal se očituje kroz sljedeće stavke:

- Neovlašteno korištenje sredstava komunikacije radi pristupa udaljenim računalnim sustavima;
- Neovlašteni pristup računalnim sustavima;
- Krađa, izmjena ili kopiranje podataka;
- Softversko piratstvo (kopiranje i korištenje tuđih autorskih programa);
- Korištenje resursa računalnog sustava za osobne potrebe od strane osoba ovlaštenih za njihovo korištenje;
- Izrada i širenje zlonamjernih programa s ciljem ostvarenja materijalne štete;
- Fizičko onesposobljavanje računalnih ili telekomunikacijskih sustava s ciljem ostvarenja materijalne štete.

Prema gore navedenim stavkama može se zaključiti kako računalni kriminal obuhvaća pregršt aktivnosti koje narušavaju sigurnost računalnih sustava, a samim time i mnogih organizacija te pojedinaca.

Prema Dragičević (1999) postoji 7 ciljeva napada na računalne sustave na internetu a oni su sljedeći:

1. Korisničke lozinke- služe za pristup internetu općenito te su zbog toga jedan od najučestalijih ciljeva;
2. Podaci i informacije- pohranjeni su na memoriji računala ili mreži, a cilj napada može biti izmjena ili brisanje podataka;
3. Datoteke- odnosi se na datoteke s brojevima kreditnih i kartica za identifikaciju. Ciljevi mogu biti neovlašteno kupovanje roba i usluga i krađa putem bankovnih računa;
4. Računalni programi- cilj napada u situaciji kada napadač želi neovlašteno kopirati ili distribuirati podatke bez dozvole vlasnika;
5. Web stranice i News grupe- cilj ovakvih napada je promjena sadržaja;
6. Onemogućavanje korištenja računalnog sustava- cilj ovakvih napada je blokiranje; glavnog računala uglavnom slanjem crva uli velikih količina poruka. Ova vrsta napada može prouzrokovati ogromne financijske posljedice.

7. Materijalno- tehnički resursi- ova vrsta napada više nije toliko učestala, a odnosi se na klasične krađe uređaja kao što su prijenosna računala.

Prema istraživanju Cert.hr (2018) ciljevi napada na računalne sustave su usko povezani sa ponašanjem korisnika na internetu, stoga postoji nekoliko ciljeva napada koji se mogu identificirati:

1. Impulzivna *online* kupnja- impulzivna kupnja je idealan trenutak koji napadači iskorištavaju na način da korisnici slučajno kliknu na sumnjive linkove koji su prijevara, krađa identiteta ili zlonamjerna preuzimanja;
2. Ilegalno preuzimanje sadržaja- korisnici često ne razmišljaju prilikom ilegalnog preuzimanja glazbe ili filmova, a napadači upravo ciljaju na takve mete za napade zlonamjernim softverima
3. Pretjerano korištenje e-pošte- ishitrenost korisnika u otvaranju zlonamjernih vrsta e-pošte može dovesti do računalnih napada
4. Nedostatak samokontrole- korisnici sa niskom razinom samokontrole ne primjećuju znakove zlonamjernih napada kao što su skočni prozori ili usporeni rad računala
5. Odnosi s pojedincima koji su motivirani za kršenje zakona- podjedinici s niskom razinom samokontrole češće ulaze u odnose s onima koji su motivirani za kršenje zakone.

Postoje mnoge podjele oblika računalnog kriminala, a u ovom poglavlju opisat će se put od samog početka nastajanja računalnog kriminala pa sve do uklanjanja dokaza o počinjenju istoga. Prema Dragičević (1999) postoje 4 koraka koja čine počinitelji koji imaju namjeru napada putem računala a to su:

1. Pristupiti računalnom sustavu- metode napada;
2. Proširenje prvog pristupa kako bi se napad mogao odvijati;
3. Poduzeti druge radnje ovisno o motivu napada (prikupiti, izmijeniti, uništiti podatke ili programe);
4. Uništavanje dokaza o prisustvu.

Prema Gašić (2022) provedeno je istraživanje o najvećim kibernetičkim napadima u 2022. godini i zašto je do njih došlo.

1. Rackspace Ransomware napad- ovaj napad bio je uzrokovan neaktualiziranom verzijom Exchange klastera, što je napadačima omogućilo da iskoriste ranjivost ProxyNotShell;

2. Cisco napad- vjerodajnice Cisco zaposlenika su kompromitirane na način da su napadači preuzeli kontrolu nad osobnim Google računom na kojem su se vjerodajnice spremljene u pregledniku žrtve sinkronizirale;
3. Uber napad- napad je bio usmjeren na zaposlenike Ubera uz pomoć metode socijalnog inženjeringa. Zbog ovog hakerskog napada neki od internih sustava su privremeno onemogućeni;
4. Napad u kojemu su otkriveni NATO podaci- korišteni kanali za prijenos podataka od strane portugalske novinske organizacije bili su nesigurni;
5. Napadi na internetske stranice američkih aerodroma- napad je proveden od hakerske grupe uz DoS (odbijanje usluga) i DDoS(distribuiriano odbijanje usluga) načine;
6. Napad na Tiktok- ovaj napad je ispočetka negiran, no Microsoft je otkrio visokorizičnu ranjivost u Tiktok aplikaciji za android koja bi mogla biti korištena od napadača za brzo kompromitiranje korisničkih računa;
7. Napad na Twitter- platforma Twitter pretrpjela je ranjivost koja je napadačima omogućila pristup osobnim informacijama. Ranjivost je omogućila dobivanje Twitter ID-a bez autentifikacije;
8. Curenje 2,4 TB podataka- ovaj napad uzrokovan je Microsoftovom pogrešnom konfiguracijom;
9. Napad na Samsung- u ovom napadu su kompromitirani imena, kontakti, demografski podaci te datumi rođenja korisnika vezano za registraciju proizvoda;
10. Hakiranje *SpaceX*-ove *Starlink* antene- belgijski istraživač hakirao je *Starlink* antenu korištenjem uređaja od 25 dolara i napada "*Voltage Fault Injection*" za učitavanje modificiranog *firmwarea.*

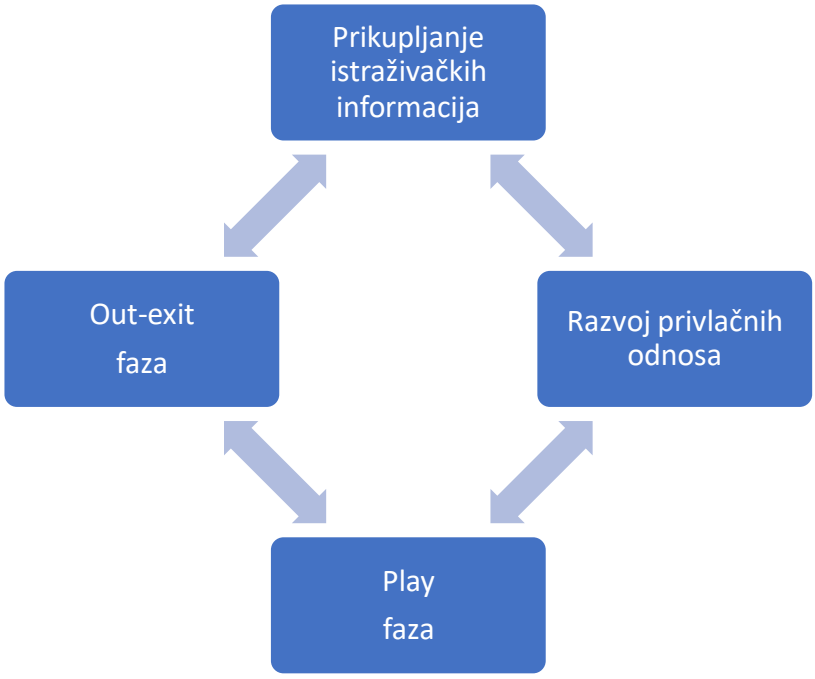
4.1 Metode napada računalnog sustava

Moderna tehnologija je sa sobom donijela i niz rizika među kojima se nalaze i napadi na računalne sustave. U ovome poglavlju opisat će se pristupi uz pomoću kojih počinitelji (napadači) na neovlašteni način dolaze do računalnih sustava. U nastavku će se opisati neke od najčešćih metoda napada na računalne sustave:

4.1.1 Socijalni inženjering

Prema autorima Šimundić i Franjić (2009) svrha socijalnog inženjeringa je da napadači manipuliraju drugim osobama koje mogu neizravno biti upotrjebljene za nedopušteno djelovanje u računalnom sustavu. Jednostavnije rečeno osobe koje se nazivaju socijalni inženjeri dolaze do podataka s ciljem kasnije prodaje podataka do kojih su došli ilegalnim

putem. Žrtva (vlasnik računala na kojemu se izvršava napad) u datom trenutku nije svjesna napada, dok napadač dolazi na neovlašteni tj. ilegalan način do podataka. Niti jedan napad socijalnog inženjeringa nije isti, ali postoji nekoliko faza prema kojima se najčešće socijalni inženjering odvija a one su prikazane na grafikonu 3:



Grafikon 3: Faze napada u socijalnom inženjeringu

Izvor: Izrada autora prema Kamiš et al. (2023)

U prvoj fazi prikupljanja istraživačkih informacija napadač odabire žrtvu napada. U drugoj fazi razvoja privlačnih odnosa napadač kroz razne kanale komunikacije pokušava zadobiti povjerenje od ciljane žrtve. U *play* fazi utječe na žrtvine emocije na način pružanja osjetljivih informacija. U posljednjoj ili *out-exit* fazi napadač odlazi bez ostavljanja dokaza. Kod socijalnog inženjeringa napadi se mogu provoditi na ljudima i na računalima. Kod napada na ljude napadači sprovode napad osobno na način da prikupljaju informacije od žrtava. Kod napada koji su temeljeni na računalima, kao što samo ime govori napadači napadaju uz pomoć raznih pametnih uređaja i mogu napasti više žrtava u jednom trenutku. Prema autorima Kamiš et al. (2023) postoje dvije glavne kategorije napada a to su izravne i neizravne. Izravni napadi se odnose na one koji se odvijaju fizičkim kontaktom (pozivom ili kontaktom „oči u oči“). Primjeri za ovakve napade mogu biti lažni telefonski pozivi, ronjenje u kontejner, krađa važnih dokumenata i sl. Neizravni napadi ne mora značiti prisutnost žrtve ali i napadača jer je napad

moguć i putem jednog klika. Najčešći primjeri za ovakve napade su *phishing*, lažni softver, skočni prozori i slično.

4.1.2 Maskiranje

Maskiranje se naziva se još i lažno predstavljanje. Počinitelj uzima identitet druge osobe s ciljem pristupa važnim podacima Šimundić i Franjić (2009). Čest primjer ovakvom obliku je putem lozinke koje omogućavaju pristup računalnom sustavu. Također, predstavljanje kao da ste druga osoba (krađa identiteta) ili telefonske prijevare su još jedni od primjera ovog oblika. Ono što karakterizira ovaj oblik jest zloupotreba povjerenja. Pod zlouporabom povjerenja smatra se lažan pristup sustavu na način da se žrtvi predstavlja da je riječ o nekom drugom sustavu s kojim je ovaj povezan.

4.1.3 *Spoofing* (varanje)

Prema Šimundić i Franjić (2009) *spoofing* je oblik varanja u kojemu se kreira lažna verzija najčešće lokacije na internetu ili adrese e-pošte. Korisnik se sa svojim podacima prijavi i odmah nakon prijave korisnikovi podaci dođu u ruke napadača koji ih zloupotrebe.

4.1.4 Ispitivanje ili pogađanje

Prema Varga (2011) ispitivanje ili pogađanje odnosi se na lozinke. Ova metoda se odnosi na pokušaj pristupu računalnom sustavu unošenjem nasumičnih lozinki, pri čemu se koriste metode pokušaja ii grešaka. Ova vrsta napada na prvi pogled može izgledati jednostavno, no ponekad može biti vrlo učinkovita.

4.1.5 Prisluškivanje sustava

Prema Šimundić i Franjić (2009) ovo je metoda u kojoj se kao što samo ime govori prisluškivanjem dolazi do podataka. Zanimljivo je to da je dovoljno snimiti zvuk pisača kako radi da bi se kasnije došlo do teksta koji je napisan. Na svim izvorima komuniciranja moguć je napad uz pomoć ove metode pa se iz tog razloga podaci šifriraju uz pomoć uređaja i algoritama.

4.1.6 Prerušavanja tj. ulaženje u sustav uz pomoć ukradene šifre

Ova metoda se odnosi na krađu odgovarajućih kartica (dokumenata koji su ukradeni ili kopirani) uz pomoć kojih se ulazi u sustave. Ovaj način može biti opasan jer je teško ući u trag napadaču zbog toga što se ne zna vrijeme a ni način napada prema Šimundić i Franjić (2009).

4.1.7 Druženje (*pretexting*)

Prema Dragičević (1999) ova metoda se odvija na način da napadač kroz opuštene razgovore nakon radnog vremena dolazi do informacija koje su mu potrebne za izvršavanje samog napada. Napadaču je cilj dobiti informacije o sustavu, sigurnosnim mjerama i sličnim stavkama.

Neformalni razgovori pružaju mogućnosti da napadači saznaju detalje koje u formalnom okruženju ne bi saznali.

Metoda druženja usko je vezana uz *pretexting* metodu koja se prema Salahdine i Kaabouch (2019) sastavlja od lažnih i uvjerljivih scenarija koje natjeraju žrtvu da vjeruje i povjerava se napadaču. Ovi napadi se mogu sprovoditi putem e-pošte, telefonskih poziva te fizičkih medija, a temelje se na pretpostavkama koje natjeraju žrtvu da vjeruje i povjerava se napadaču.

4.1.8 Kompromitiranje

Prema Dragičević (1999) ova metoda se koristi taktikama kao što su podmićivanje, prijetnje ili manipulacije kako bi se utjecalo na ranjivost ciljane žrtve napada. Uz pomoć ove metode napadači žele doći do informacija zaposlenika na neformalan način.

Prema Holm (2014) kompromitiranje se definira kao metoda uz pomoću koje napadači na neovlašten način stječu pristup podacima ili sustavu. Ova metoda uključuje niz sigurnosnih incidenata gdje se vrijeme koje je potrebno za kompromitiranje može prikazati statističkim raspodjelama.

4.2 Proširenje metoda napada računalnog sustava

Nakon što je napadač uspio uz pomoć prethodno objašnjenih metoda pristupiti računalnom sustavu žrtve (običnog korisnika) čiji je identitet zlouporabljen. Obični korisnici uglavnom imaju ograničena prava, a napadač kako bi ostvario svoje ciljeve nastoji proširiti metode napada na računalni sustav na sljedeći način prema Šimundić i Franjić (2009).

4.2.1 Pregledavanje (*Browsing*)

U ovoj metodi napadač pregledava dostupne datoteke i memoriju računala s ciljem pronalaska informacija koje će mu omogućiti proširenje prava pristupa računalnom sustavu. Korisnici (žrtve) nisu svjesni da se svaka njihova aktivnost bilježi te da se ti podaci pohranjuju u memoriji računala i dostupni su svima koji koriste to računalo prema Dragičević (1999).

Prema Sinha (2012) u ovoj metodi napadači pokušavaju pročitati pohranjene datoteke, pakete poruka te memoriju drugih procesa bez mijenjanja podataka. Mehanizmi uz pomoću kojih se kontrolira pristup koriste se za sprječavanje neovlaštenog čitanja pohranjenih datoteka i sadržaja memorije drugih procesa.

4.2.2 Stražnja vrata

Prema Šimundić i Franjić (2009) ova vrsta se sastoji od prevladavanja sigurnosnih sustav. Također, autori programske podrške služe stražnja vrata u svrhu kvalitetnije programske

procedure ali i za preskakanje nekih dijelova. Napadač može promijeniti neke programske stavke. A na samome kraju stražnja vrata je potrebno potpuno ukloniti ali nekad dođe do propusta i to ne bude učinjeno.

4.2.3 Nadzor rada sustava

Ovaj oblik je najjednostavnije objasniti tako što određeni programi izgube svoju prvotnu svrhu i u rukama napadača postanu metoda za napad računalnog sustava. Prema Cynet (2020) ima mnogo primjera za ovu metodu jedan od njih je Cobalt Strike koji je prvotno bio namijenjen za simulacije različitih vrsta zlonamjernih softvera i napada općenito. Način na koji napadači zloupotrebljavaju ovaj alat je da se stvarni mrežni promet na vrlo jednostavan način može imitirati i to otežava njegovo otkrivanje i napadačima omogućuje da ostanu u mreži duže vrijeme.

4.2.4 Superzapping

Superzapping je prema Kabay (2008) alat koji se koristi u većini centara za računalne sustave. To je alat koji u slučajevima kada računalo prestane raditi ili je u kvaru pomaže naređenim osobama da zaobiđu sigurnosne mjere s ciljem što bržeg rješavanja kvara. Ovakvi alati mogu biti jako opasni ukoliko se nađu u rukama napadača jer ih obično koriste programeri sustava i operateri sustava koji su zaduženi za održavanje sustava računala. Ovaj alat se može zloupotrijebiti na način da napadač izvršava određeni niz promjena u datotekama podataka.

4.3 Sljedeći koraci napadača u računalnom sustavu

Nakon što je došlo do napada na računalni sustav uz pomoć osnovnih metoda napada, a nakon toga napadač je proširio svoje metode dodatnim alatima sljedeći koraci ovisit će o željama i motivima napadača. Moguće je nekoliko rezultata. Jedan od njih može biti kraj napad jer je napadač ostvario svoj cilj. A drugi može biti nastavak napada jer su sve ostale radnje bile preduvjeti za one koje slijede. Sljedeće radnje koje počinitelj poduzima mogu biti manipulacije podacima, uskraćivanje usluga i maliciozni programi.

4.3.1 Manipuliranje podatcima

Ova metoda odvija se na način da se do podataka dolazi prilikom prikupljanja ili unosa podataka u sustav, ali moguće je i ranije. Svrha ove metode jest stjecanje imovinske koristi. Prema Šimundić i Franjić (2009) najčešća primjena ove metode jest kod stanja bankovnog računa, neovlaštenog ažuriranja dugovanja ili dobivanje krivotvorenih dokumenata.

Može se zaključiti kako je metoda manipuliranja podacima kao i sve do sada zabrinjavajuća jer postoji veliki rizik od prijevare i zlouporabe. Ukoliko se podaci manipuliraju prilikom unosa ili

prikupljanja, iz toga se može zaključiti kako je pouzdanost cijelog sustava ugrožena od samog početka.

4.3.2 Napadi uskraćivanjem usluga (*Denial of Service*)

Prema Šincek i Vrbanec (2010) napadi uskraćivanjem usluga ili tzv. DoS su aktivnosti sprovedene od strane korisnika koji imaju zle namjere ,a to je onemogućavanje korištenja i funkcioniranja računalnih ili mrežnih resursa. Na taj način usluge postanu nedostupne legalnim korisnicima, a napadači to rade na način da u kratkom vremenskom periodu ponavljano zahtijevaju neku obično legitimnu uslugu s naglaskom na to da ne očekuju odgovor od poslužitelja ili mreže. Ono što možda ovu metodu izdvaja od drugih je cilj napada. Cilj napada nije financijska korist, DoS napadači izvršavaju ovakve napada kako bi se međusobno dokazali ili nanijeli nekakvu štetu organizaciji. Naravno, šteta koja je nanesena može biti financijska (nemogućnost poslovanja ili ulaganja u sigurnosne sustave) i nefinancijska (gubitak ugleda organizacije). Napade uskraćivanjem usluga možemo podijeliti u dvije kategorije prema Šnicek i Vrbanec (2010):

1. Napadi koji su sumjereni na aplikacijski sloj;
2. Napadi usmjereni na mrežni sloj.

4.3.3 Maliciozni programi

Prema Raićević et al. (2014) definiraju maliciozne programe kao programe koji izvršavaju namjerne radnje na štetu korisnika. Maliciozni programi su jedni od najčešćih prijetnji moderno-tehnološkom svijetu. Maliciozni programi čine velike štete računalnim sustavima u vidu brisanja, oštećenja, kvarenja ili zadržavanja takvih programa u tajnosti bez prava na to. Posljedice malicioznih programa mogu biti prema Raićević et al. (2014) sljedeće :

- Brisanje ključnih datoteka sa tvrdog diska;
- Učiniti korisnički uređaj izvorom infekcije na način da se inficira korisničko računalo; kako bi se stvorila baza uz pomoću koje će se inficirati kontakti od korisnika;
- Snimanje svih pritisaka na tipkovnici inficiranog računala;
- Prikupljanje detaljnih informacija o korisniku (njegove navike te web stranice koje posjećuje i sl.);
- Snimanje uz pomoć kamere i mikrofona na računalu bez znanja korisnika čije je računalo inficirano;
- Izvršavanje svih naredbi kao da ih je zadao i sam korisnik;

- Krađa osobnih i financijskih podataka;
- Korisnikovo računalo može postati spremište za zlonamjerne aktivnosti ukoliko napadač na njemu skladišti dodatne maliciozne kodove, ukradene informacije ili koristi piratske softvere;
- Računalo od korisnika služi samo kao sredstvo za daljnje napade;
- Napadač na računalo od korisnika postavi dokaze koje upućuju da je krivac sam korisnik;
- Napadač konstantno provodi napade i skriva svoje tragove maskiranjem datoteka i procesa.

U nastavku će se objasniti vrste malicioznih programa.

1. Računalni virusi

Prema Jaiswal (2017) virusi su vrsta malicioznih programa koji se jako brzo šire zato što ih je teško otkriti. Virus je nepoželjna računalna greška koja je napravljena da uzrokuje štetu na računalima u velikoj mjeri. Virusi su priloženi uz program, datoteku ili dokument i skriveni su sve dok nešto ne uzrokuje izvršenje njegovog koda. Postoji nekoliko vrsta virusa a prema Jaiswal (2017) to su:

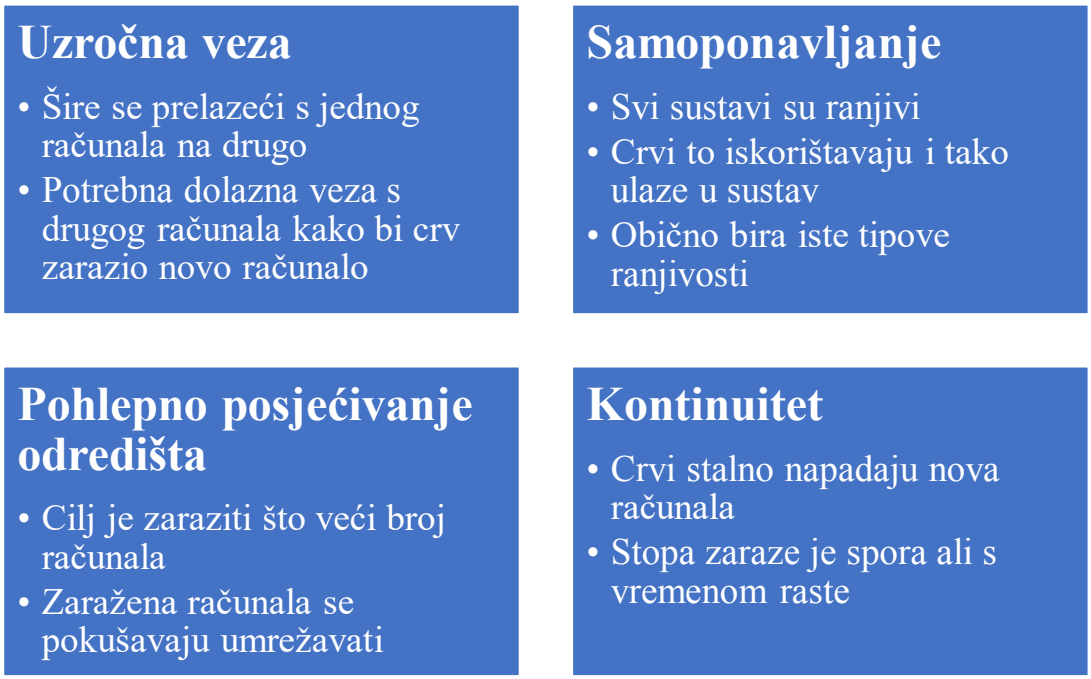
1. Virus datoteka;
2. Virus *boot* sektora;
3. Makro virus;
4. Virus izazovnog koda;
5. Polimorfni virus;
6. Šifrirani virus;
7. Tunelski virus;
8. Multipartitni virus.

Svi prethodno navedeni virusi mogu se skriti u prerušene privitke sadržaja koji se dijeli poput smiješnih slika, čestitki ili audio i video datoteka. Neki virusi mogu imati namjeru napada u svrhu zabave, dok s druge strane drugi mogu imati ozbiljne posljedice poput brisanja podataka ili trajnog oštećenja diska.

2. Računalni crvi

Prema Shah et al. (2017) računalni crvi definiraju se kao programi koji su osmišljeni za zarazu računala pojedinačnim umnožavanjem preko mreže. Još jedna od karakteristika računalnog

crva jest da se jako brzo šire s jednog računala na drugo i ne trebaju glavni program ili datoteku za širenje. Ukoliko sumiramo sve prethodno računalnog crva možemo definirati kao zlonamjerni kod koji se širi putem internetskih ili lokalnih mreža. U nastavku će se prikazati obrazac kretanja crva u grafičkom prikazu prema Prema Shah et al. (2017):



Grafikon 4: Obrazac kretanja crva

Izvor: Izrada autora Prema Shah et al. (2017)

Prema Shah et al. (2017) postoji 5 glavnih vrsta računalnih crva a to su sljedeći:

a) Crvi e-pošte - računalo je zareženo čim se e-pošta otvori tj. preuzme privitak;
b) Crvi za aplikacije za razmjenu poruka- aplikacije poput Yahoo-a i AOL-a izvor su ove vrste crva;
c) Internet crvi- ovdje se crvi šire jako velikom brzinom tako što se kreću i utječu na drugi sustav putem interneta;
d) IRC (Internet Relay Chat)- šire se uz pomoć zlonamjernih poveznica ili datoteka kroz internetske chatove;
e) Crvi na mrežama za dijeljenje datoteka- šire se tako da svoje kopije postavljaju u zajedničke mape koja je dostupna svim korisnicima na mreži za dijeljenje sadržaja (P2P mreže). U trenutku kada drugi korisnici preuzmu zaraženu datoteku njihovi sustavi su zaraženi a crv se i dalje širi na isti način.

U svijetu računalnog kriminala virusi i crvi predstavljaju dvije različite vrste malicioznih programa. U nastavku će se tabličnim prikazom predstaviti koje su to ključne razlike između crva i virusa.

	VIRUS	CRVI
DEFINICIJA	programi koji napadaju i druge programe prilagođavajući ih tako da se u njih uključi njegova vlastita kopija	programi koji su osmišljeni za zarazu računala pojedinačnim umnožavanjem preko mreže
POTREBA ZA DOMAĆOM DATOTEKOM	Potrebna mu je datoteka domaćina da bi se premještao i aktivirao	Nije mu potrebna datoteka domaćina da bi se premještao i aktivirao
NAČIN ZARAZE	Umetne se u datoteku ili program i aktivira se kad se datoteka ili program pokrenu	Iskorištava slabosti na računalu i tako se množi i zaraza se širi
BRZINA	Sporije	Brže
ŠIRENJE	Uz pomoć korisnika se širi na druga računala	Koristi mrežu da se raširi na druga računala
U PRILOGU SA	.EXE,.DOC, .XLS itd.	Bilo kojom datotekom e-pošte ili bilo kojoj datoteci na mreži
PRIMJERI	C-Brain, Macmag, Cascade itd.	Slammer, Morris itd.

Tablica 1: Razlike između virusa i crva

Izvor: Izrada autora Prema Shah et al. (2017)

3. Trojanski konj

Prema Šimundić i Franjić (2009) trojanski konj predstavlja oblik napada koji manipulira podacima na način da se prikriveni dio instrukcija umeće u neki od programa koji se izvode na sustavu. Na prvi pogled ovaj oblik napada se može činiti kao nekakva igra tj. da ima inačice dobronamjernog programa. Zamka se krije u tome što ovaj oblik korisnici uglavnom sami instaliraju na svoja računala i onda trojanski konj vrši napad ili isporuči neki drugi oblik malicioznog programa kao što je virus ili crv.

4. *Spyware* programi

Prema Easttom i Taylor (2011) osnovni cilj *spyware* je dobivanje i prikupljanje osobnih podataka sa računala korisnika. *Spyware* funkcionira na način da se učitava na računalo korisnika bez njegova znanja. Softver koji se učita na računalo korisnika može zabilježiti korisnička imena i lozinke ili posjećene web stranice i mnoge druge podatke. Prema Easttom i Taylor (2011) postoje dva razloga zbog kojih je *spyware* čest u području računalnog kriminala:

- Lako ga je za nabaviti- većina proizvoda koja je napravljeni za zakonito korištenje mogu se koristiti kao špijunski softver;
- Lako se isporučuje- isporučuje se često uz pomoć nekog softvera koji ima neku drugu svrhu (npr. trojanski konj).

5. Scareware

Scareware se odnosi na zastrašivanje korisnika raznim prijetnjama i ucjenama. Prema Sabelli (2022*) scareware* funkcionira na način da korisnici misle da je njihov sustav zaražen sa nekim od zlonamjernih softvera i onda skinu softver koji bi im trebao u tome pomoći, a zapravo to bude prevarantski softver. Ovaj oblik malicioznih programa u praksi često vidimo u obliku banera koji se pojavljuju na ekranima računala. Još neki od oblika u kojima se *scareware* može pojaviti jest putem e-pošte ili da se korisniku nudi instalacija softverskog alata (koji je zaražen).

6. Keylogger

Prema Jakobsson i Ramzan (2008) *keyloggeri* su programi koji na neki način prate podatke koje korisnik unosi u stroj. Funkcioniraju na način da se sami instaliraju u internetski preglednik ili u upravljački program računala. Ono na što se cilja ovom metodom jesu krađa PIN-ova te brojeva kreditnih kartica i slično.

7. Rokkit

Prema Jakobsson i Ramzan (2008) *Rokkit* su softveri koji skrivaju prisutnosti i aktivnosti zlonamjernih softvera. Postoje dvije vrste *Rokkita* a to su jednostavni (kao zamjena za administrativni) i složeni (čine zlonamjerni kod nevidljivim). Postoje mnogi načini za otkrivanje *rokkita* ,a jedan od njih je pokretanje operativnog sustava unutar virtualnog stroja, dok sigurnosni softver radi izvan nje. Moderne vrste procesora s podrškom u virtualizaciji mogu pomoći u napadima kao što je *rokkit*.

4.4 Uništavanje dokaza

Ovo je posljednji korak u procesu provođenja računalnog kriminala od strane napadača na korisnike. Glavna karakteristika računalnog kriminala ukoliko se gleda sa stajališta napadača jest anonimnost. Cilj svakog napadača je ostati anoniman, a tu anonimnost je moguće ostvariti kroz uništavanje svih dokaza tj. radnji koje su opisane u prethodnim poglavljima.

Prema Dragičević (1999) svaka radnja na računalu se pohranjuje u obliku tzv. logičkih datoteka koje predstavljaju dnevnik pristupa računalu i korištenja njegovih resursa. Upravo zbog tog razloga napadači uklanjaju sve dokaze kako ne bi bili otkriveni. Obujam i volumen dokaza koji se uklanjaju ovise o operativnom sustavu koji se koristi.

Prema Montesano (2019) uništavanje dokaza definira se pojmom antiforenzika. Kako bi se napadači otkrili koriste se razne digitalne forenzičke tehnike, a s druge strane napadači koriste antiforenziku koja se definira kao pokušaj negativnog utjecaja na postojanje, količinu ili kvalitetu dokaza s mjesta zločina, ili da se ispitivanje ili analiza dokaza učine nemogućima.

Za napadače je korak uništavanja dokaza ključan, ali također može biti odlučujući jer se čak i u ovome koraku mogu razotkriti. Zaključno, borba protiv računalnog kriminala zahtjeva provedbu i korištenje metoda i alata za suzbijanje računalnog kriminala koja će se definirati u nastavku ovog rada. Osim toga, stalna edukacija korisnika i podizanje svijesti o računalnom kriminalu može pomoći u suzbijanju istog.

5. Osiguranje sigurnosti računalnog sustava i zaštita podataka

Iz prethodnih poglavlja može se zaključiti kako se samim razvojem računala razvila i njegova zlouporaba. Zbog masovne pojave računalnog kriminala od velike je važnosti da se pojedinci, ali i organizacije osiguraju od zlonamjernih napada i zaštite svoje podatke. Kako tehnologija napreduje, nažalost napreduje i računalni kriminal pa je od velike važnosti konstantno unaprjeđivati i poboljšavati metode zaštite računalnih sustava.

Šimundić i Franjić (2009) smatraju da se standardni način čuvanja podataka po arhivima i slično odnosi se uglavnom na fizičku zaštitu. Ovaj oblik je star koliko i povijest njihova prikupljanja. S druge strane, elektronička obrada sa sobom donosi novi način prikupljanja podataka, a samim time i novi način zlouporabe istih. U ovom poglavlju će se predstaviti metode koje se provode s ciljem zaštite podataka i cijelog sustava općenito. Metode za osiguravanje sigurnosti računalnog sustava i zaštitu podataka prema Šimundić i Franjić (2009) su sljedeće:

1. Fizička i organizacijska zaštita;
2. Komunikacijska zaštita;
3. Hardware/software zaštita;
4. Pravna zaštita podataka;
5. Zaštita većih sustava- vatrozidi i dr.;
6. Antivirusna zaštita.

5.1 Fizička i organizacijska zaštita

Prema Šimundić i Franjić (2009) fizička i organizacijska zaštita su osnovne metode kod zaštite podataka i općenito gledajući prva dva osnovna koraka u ovom vidu zaštite su:

1. Mjere zaštite podataka koje donose nadležni organi izvan računalnog centra;
2. Mjere zaštite koje donose u samom računalnom centru.

Fizičke i organizacijske mjere zaštite iz prve grupe reguliraju se pravilnicima i zakonima. Tim pravilnicima i zakonima regulira se (Šimundić i Franjić, 2009:60):

- „Osiguranje i očuvanje objekata, prostorija i druge imovine;
- Sprječavanje i otkrivanje pojava koje mogu ugroziti sigurnost djelatnika, objekata i imovine;
- Onemogućavanje pristupa nepozvanim osobama u objekte i druge prostore koje koristi računalski centar;
- Kretanje i odgovornost osoba koje nisu djelatnici računalskog centra;

- Kontrola računalne opreme prije ulaska u prostorije računalskog centra;
- Postavljanje alarmnih uređaja za požar i postupci zaduženja u slučaju požara;
- Postavljanje nezavisnog izvora električnog napajanja;
- Provjera povjerljivosti osoba koje dolaze u dodir s važnim podatcima;
- Odgovornost pojedinih osoba za provođenje propisanih mjera zaštite izvan računalskog centra;
- Kontrola provođenja tih zaštitnih mjera.“

Prethodno navedene mjere treba provesti i u drugoj grupi tj. u samom računalskom centru. Njima je potrebno regulirati sljedeće: (Šimundić i Franjić, 2009:61)

- „Klasificiranje podataka prema potrebnom nivou zaštite;
- Propisivanje ovlaštenje pojedinih osoba (uređaja) za pristup pojedinim podatcima;
- Kopiranje važnijih podataka i programa i način njihova čuvanja (po mogućnosti izvan računalskog centra);
- Kontroliranje važnih i osjetljivih izlaza (tiskanih lista i sl.);
- Postojanje procedura za ažuriranje podataka;
- Kontrola promjena programa u produkciji;
- Kontrola modifikacije sustavnog software-a;
- Kontrola korištenja određenih sustavnih programa;
- Puštanje u rad programa tek nakon dobrog testiranja;
- Planiranje svih poslova na sustavu;
- Dokumentacija i standardizacija;
- Svakodnevno uzimanje i kontroliranje konzolne liste;
- Praćenje rada terminala;
- Evidentiranje i kontrola tijeka obrazca (za one koji nemaju terminal);
- Definiranje postupaka i ponašanja u redovitim i izvanrednim okolnostima;
- Plan za vraćanje računalnog sustava u normalno radno stanje nakon ispada nastalog usred grješke (recovery);
- Obuku i uvježbavanje osoba odgovornih za zaštitu;
- Periodično testiranje, ažuriranje i unapređivanje sustava za zaštitu;
- Propisivanje načina uništavanja izlaznih lista i brisanje traka s važnim podatcima prije oslobođenja traka;
- Propisivanje načina praćenja provođenja svih mjera zaštite;

- Redovitu kontrolu provođenja EOP mjera zaštite;
- Određivanje posebne grupe odgovorne za zaštitu i sigurnost podataka u računalskom centru;
- Određivanje (ako je moguće) posebne osobe odgovorne da prati provođenje mjera zaštite i promjene parametara zaštite;
- Definiranje odgovornosti za zaštitu podataka svih učesnika u tehnološkom lancu i dr.“

Prema Mishra et al. (2021) fizička zaštita najčešće se koristi u zrakoplovstvu i zdravstvu. Smatra se kako osim zrakoplovne i zdravstvene industrije i financijske trebaju imati veću pažnju prilikom fizičke zaštite. Prema istraživanjima Mishra et al. (2021) trebao bi postojati zakon o fizičkoj zaštiti kako bi se osigurali zdravstveni, zrakoplovni, financijski ali i ostali sektori.

5.2 Komunikacijska zaštita

Prema Šimundić i Franjić (2009) komunikacijska zašita se odnosi na zaštitu podataka pri prijenosu komunikacijskim putem. Ključna stavka ove vrste zaštite jest kriptografija kojom se uz pomoć algoritama štite podatci na način da se obični tekst transformira u šifrirani tekst koji nije razumljiv svima. Osnovna zadaća kriptografije jest zaštiti podatke koji se prenose na relaciji računalo- terminal. Još jedna od mogućnosti koje nudi kriptografija jest da ta šifrirana poruka može sadržavati i od koga je poslana te da je neizmijenjena.

Proces same kriptografije je sljedeći. Prema Šimundić i Franjić (2009) koriste se dva čitača papirne trake, s time da jedan koristi papirnu traku s čistim podatcima, a drugi s krivim podacima. Krivi podatci se dodaju u čiste i na taj način nastaje tehnika online šifriranja podataka. Uređaji koje izvode transformaciju krivih u čiste podatke mogu biti hardware ili software.

Prema Mishra et al. (2021) komunikacijska zaštita podrazumijeva informacijsku sigurnost. Informacijski resursi u poduzećima bi trebali biti zaštićeni. Cilj informacijske sigurnosti jest zaštititi sve fizičke i digitalne resurse od ilegalnog pristupa kao što su kopiranja, izmjene, otkrivanja, uništavanja i slično. Dakle, zaključuje se kako informacijska sigurnost ima svrhu zaštiti informacije unutar mreže poduzeća.

5.3 Hardware/software zaštita

Ova vrsta zaštite nudi mogućnost zaštite podataka koju pruža hardware i mogućnost zaštite podataka koju pruža software.

1. Mogućnost zaštite podataka koje pruža hardware prema Šimundić i Franjić (2009):

a) Računalo

Prema Šimundić i Franjić (2009) zaštita računala odnosi se na zaštitu memorije. Osim zaštite memorije, zaštitni ključ na konzoli omogućava operateru da obavlja samo jednu funkciju, a ukoliko se to promijeni oglasit će se zvučni alarm. I na posljetku, ukoliko se otkrije greška za vrijeme izvođenja instrukcija, pokušava se ponovno izvođenje istih.

b) Magnetske trake

Kod ovog modela moguće je upisivanje na magnetske trake samo ukoliko je postavljen prsten za pisanje, i prilikom pisanja na traku vrši se provjera.

c) Diskovi

Kod ovog modela neovlašteno upisivanje u disk je moguće spriječiti prebacivanjem računala na način rada „samo za čitanje“.

d) Terminali

Podatci koji se unose preko terminala, ponajviše lozinke ne prikazuju se na ekranu i na taj način nude veliku razinu zaštite.

e) Uređaji za šifriranje podataka

Na posljetku, važno je postavljanje uređaja za šifriranje podataka prilikom prijenosa podataka između računala i centralnog sustava.

2. Mogućnost zaštite podataka koje pruža software

U zaštiti računala od računalnog kriminala veliku ulogu igra i software, pri čemu operativni sustav ima dominantnu ulogu. Mogućnosti zaštite koje pruža operativni sustav i njegovi programi su mnogobrojni a samo neki od njih mogu biti prema Šimundić i Franjić (2009) to da korisnici mogu pisati vlastite procedure u svrhu zaštite svojih programa i podataka, korisnicima se može dodijeliti jedna ili više od sedam mogućih klasa itd.

Prema Ramakić i Bundalo (2013) glavni dio koji se koristi za zaštitu softvera i hardvera zove se hardverski ključ ili tzv. *dongle*, a koristi se na način da se povezuje na računalo. U prošlosti se to povezivanje odvijalo uz pomoć serijskog ili paralelnog porta, a danas se povezuje putem USB-a. Glavna zadaća tih uređaja je sprječavanje kopiranja i neovlaštenog korištenja softvera i pristupa podacima općenito.

5.4 Pravna zaštita podataka

Prema Šimundić i Franjić (2009) masovno korištenje moderne tehnologije omogućava pristup dostupnosti podataka, što u konačnici povećava opasnost o sigurnosti i pouzdanosti tih informacija. Upravo je prethodno navedeno razlog zbog kojeg su zakonodavne aktivnosti usmjerene na pravnu zaštitu podataka. Naime, tehnologija i komunikacija je tijekom vremena rasla eksponencijalnom brzinom i samim time prijenos informacija je postao jeftiniji i brži.

Prema Šimundić i Franjić (2009) stopa zlouporabe informacija i podataka je velika zbog toga što ne postoji apsolutna zaštita, a tehnologija je s vremenom postala sve dostupnija. Pitanja zaštite podataka i zaštite autorskih prava su jako važna. Zemlje poput Hrvatske moraju se prilagoditi ekonomskim tijekovima, također trebale bi uskladiti zakone s ciljem zaštite podataka i informacija. Prema mišljenju autora Šimundić i Franjić (2009) pravna regulacija podataka započela je već sedamdesetih godina, a sam rezultat bio je da velike banke podataka mogu biti zlouporabljene od strane državnih institucija, privatnih kompanija, banaka i pojedinaca.

5.5 Zaštita većih sustava- vatrozida i dr.

Prema mišljenju autora Šimundić i Franjić (2009) za pristup internetu moderna računala koriste UNIX te se često moraju suprotstaviti neprijateljskim ili napadima pojedinca. Jedan od najpoznatijih i najučinkovitijih sustava za zaštitu računalnih mreža jest vatrozid. Osnovna zadaća vatrozida je omogućiti pristup internetu bez opasnosti za podatke na mreži s koje se pristupa. Osim toga vatrozidi smanjuju mogućnosti nastanka štete, jer su postavljeni između vanjske i unutrašnje mreže i na taj način sprječavaju napadače koji su već uspjeli ući u mrežu da ostanu unutar nje. Dakle, može se zaključiti kako je osnovna funkcija vatrozida kontrola tijeka informacija između dvaju mreža.

Također, prema Šimundić i Franjić (2009) postoje dva osnovna načina konfiguriranja vatrozida:

1. Određivanje dozvola- postavlja se skupina uvjeta koji u konačnici završe blokiranjem podataka. Prednost ovog načina jest jednostavnija konfiguracija;
2. Određena zabrana- upisuje se određeni protokol koji omogućava ulaz određenim posjetiteljima, dok su ostali odbijeni.

Zaključno, vatrozid je važan element obrambene strategije koji postavlja više prepreka između računala i potencijalnih prijetnji. Prema Ramakić i Bundalo (2013) vatrozid predstavlja sigurnosti element koji se nalazi između lokalne i javne mreže. Svrha vatrozida je zaštiti povjerljive, korporativne i korisničke podatke. Osim toga, postavljanjem vatrozida između dva

ili više mrežnih segmenata kontroliraju se prava pristupa pojedinih korisnika, pojedinim dijelovima mreže. Postoje dvije vrste vatrozida prema Ramakić i Bundalo (2013):

1. Softverski vatrozid: štiti jedno računalo, osim u slučaju kada to računalo ima namjenu štiti cijelu mrežu;
2. Hardverski vatrozid- olakšana je konfiguracija te maksimizirana brzina provjere mrežnih paketa.

5.6 Antivirusna zaštita

Prema Šimundić i Franjić (2009) pojava virusa, crva te trojanskih konja i sličnih malicioznih programa stvara sve veće probleme. U daljnjem tekstu opisat će se koji su to mogući načini zaštite od virusa.

Postoje mnoge metode zaštite računalnih sustava od virusa, kao što su (Šimundić i Franjić, 2009:71):

- „Kontrola pristupa, tj. onemogućavanje nepozvanim osobama, odnosno korisnicima pristup sustavu;
- Kriptografska zaštita;
- Korištenje programa za kontrolu integriteta sustava;
- Korištenje programa za praćenje operacija;
- Korištenje programa za eliminiranje virusa iz sustava;
- Izrađivanje sigurnosnih kopija;
- Nabavka i korištenje samo originalnog (autoriziranog software-a i programa i dr.“

Prema Samociuk (2023) antivirusni programi skeniraju datoteke i uspoređuju njihov sadržaj za crnom listom poznatih zlođudnih kodova. Ukoliko antivirusni programi otkriju bilo kakve prijetnje uklanjaju ih. U nastavku će se objasniti nekoliko modernih tehnika antivirusnih softvera koji se koriste za identifikaciju zlođudnih softvera i zaštitu računalnih sustava općenito prema Samociuk (2023):

1. Potpisi- zlonamjerni softver detektira se uz pomoć potpisa (kratak fragment koji ne otkriva ništa korisno) usporedbom jedinstvenih obrazaca virusa s bazom podataka poznatih prijetnji. Ova metoda ograničena je na poznate prijetnje i nije najučinkovitija za moderne vrste virusa.
2. Detekcija ponašanja- ova metoda temelji se na analizi ponašanja programa pri pokretanju te omogućuje identifikaciju problema bez baze podataka.

3. Heuristička detekcija- metoda heuristike koristi skup pravila za analizu progrma uz pomoću koje se utvrđuje sadrži li virus na način a se koriste tehnike strojnog učenja i rudarenja podataka za identifikaciju modernih virusa.
4. *Sandboxing*- ova metoda simulira ponašanje glavnog računala unutar virtualnog okruženja kako bi se identificirale potencijalno štetne datoteke i pratilo njihovo ponašenje.

5.5. Kako zaštiti svoj identitet na internetu

Ukoliko promatramo sa današnjeg stajališta sigurnost na internetu je globalna tema, a krađa identiteta na internetu. S povećanjem digitalne aktivnosti korisnika raste i rizik od računalnog kriminala te računalnog kriminala općenito. U nastavku će se opisati što učiniti ukoliko se kao pojedinac nađete u situaciji krađe identiteta prema Easttom i Taylor (2011):

1) *Phishing* e-pošta

Kao jedan od ključnih oblika prijevare, važno je prepoznati lažne poruke koje se predstavljaju kao formalni izvori. Najčešće e-pošta ovog tipa sadržavaju poruke poput onih da postoji problema sa vašim računom te da kliknete na poveznicu kako biste te iste probleme riješili. Ukoliko se klikne na stranicu doći će do prikupljanja osobnih podataka. Kako bi se zaštitilo od ovakvog oblika potrebno je sljedeće:

a) Provjeriti poveznicu (URL): npr. ako poveznica sadrži drugačiji niz znakova poput www.facebok.com.sazzawy.eu to je znak lažne stranice
b) Izgled e-pošte: ovakva e-pošta obično izgledaju realistično i iz tog razloga treba biti na oprezu
c) Kratko trajanje stranice: *phishing* stranice postoje kratko vrijeme pa ukoliko sumnjate da se radi o prijevari ne treba odmah kliktati na poveznicu

2) *Phishing* internetske stranice

Kako bi se zaštitio identitet od internet stranica koje se bave *phishingom* potrebno je slijediti nekoliko koraka:

a) Provjeriti legitimnost internetske stranice

Prije unošenja bilo kakvih osobnih podataka važno je pregledati internet stranicu te koristiti sigurnosne mjere kao što su *site key*, a to uključuje da prilikom prijave stranica mora prikazati određenu sliku i lozinku, ukoliko dođe do nepodudaranja radi se o prijevari.

b) Lažne prodajne stranice

Ovo je jedan od vrlo čestih oblika u kojima *phisheri* mogu stvoriti lažne internetske trgovine sa niskim cijenama kako bi privukli korisnike. Zato prije same kupovine potrebno je učiniti neke sigurnosne mjere poput provjere koliko dugo je stranica aktivna, potražiti recenzije ili informacije na internetu, procjena same ponude asortimana i slično.

3) Spyware

Zaštita identiteta od strane *spywarea* je također važna za održavanje sigurnosti i privatnosti osobnih podataka na internetu. U nastavku će se predstaviti neke od situacija u kojima kao korisnik interneta treba biti oprezan u svrhu zaštite.

a) S oprezom otvarati datoteke priložene u e-pošti

Poslovni mailovi (oni koji su poslani od stvarnih osoba koje nemaju skrivene loše namjere) uglavnom ispod maila imaju potpis sa imenom, titulom i nazivom institucije u kojoj rade te kontaktom, a ukoliko mail to ne sadrži treba biti na oprezu. Također, nekakvi općeniti pozdravi koji su generički napravljeni mogu ukazivati na prisutnost *spywarea*. Osim toga, ukoliko u tekstu ima puno gramatičkih grešaka to može biti znak za sumnjivu e-poštu.

b) Koristiti i redovito ažurirati *anti-spyware* programe i alate

Prema Stouffer (2023) postoji nekoliko načina kako bi se minimizirali *spyware* napadi a to su:

- Koristiti provjereni antivirusni softver za zaštitu od *spyware;*
- Koristiti blokator skočnih prozora ili izbjegavati klikanje skočnih oglasa;
- Redovito ažurirati operativne sustave računala;
- Ne otvarati sumnjivu e-poštu;
- Ne otvarati neželjene privitke e-pošte;
- Ne otvarati veze u tekstualnim porukama od nepoznatih pošiljatelja.

4) Prikupljanje osobnih podataka
   a) Easttom i Taylor (2011) smatraju da je potrebno ograničiti dostupnost osobnih podataka na društvenim mrežama na način da;
      - Većinu informacija treba držati privatnima;
      - Izbjegavati davanje specifičnih informacija;
      - Paziti koga prihvaćate za prijatelje/pratitelje na društvenim mrežama;
      - Biti na oprezu pri dijeljenju informacija na javnim forumima, oglasnim pločama i slično;
      - Smanjiti količinu osobnih podataka koji su dostupni na internetu.

5) Opće protumjere

U nastavku će se opisati nekoliko općih mjera koje kao korisnik interneta možete poduzeti kako biste izbjegli postati žrtvom krađe identiteta: Prema mišljenju autora Easttom i Taylor (2011)

- Osjetljive i povjerljive dokumente treba prije bacanja u otpad uništiti;
- Potrebno je uništiti stare CD-ove, diskete, tvrde diskove i slično prije bacanja;
- Motiv napada je često financijskog tipa te je iz tog razloga potrebno provjeravati stanje bankovnih računa, kredita i slično;
- Izbjegavati korištenje komercijalnih alata za zaštitu identiteta koji nude minimalnu zaštitu poput LifeLocka i IdentityProtect.com.

Osim prethodno navedenih općih protumjera Matejowski (2023) smatra kako su neke od novijih metoda prevencije od krađe identiteta sljedeće:

1. Održavanje sigurnosti uređaja;
2. Korištenje snažnih lozinki;
3. Edukacije o krađi identiteta;
4. Izbjegavanje sumnjivih veza;
5. Korištenje sigurnih mreža;
6. Redovito ažuriranje softvera;
7. Primjena dvostruke autentifikacije;
8. Provjera SSL certifikata;
9. Korištenje upravitelja lozinki;
10. Održavanje povjerljivosti podataka.

Razina svijesti o kibernetičkom kriminalu je tijekom godina eksponencijalno rasla. Samim time i zaštita identiteta korisnika interneta. S jedne strane moderna tehnologija ubrzava procese u poslovanju, dok s druge strane jedan trenutak nepažnje može dovesti do ozbiljnih posljedica. Podizanje razine svijesti o kibernetičkom kriminalu općenito, te samoj zaštiti identiteta temelj je za njegovo sprječavanje.

6. Istraživanje o sigurnosti na internetu

Naposlijetku ovog rada s ciljem donošenja što boljeg zaključka prikazat će se rezultati istraživanja o sigurnosti na internetu i navikama korisnika prilikom korištenja interneta. Uz pomoć istraživanja dobit će se ključne informacije o tome koliko su korisnici zabrinuti za svoju sigurnost na internetu, ali i koliko znanja imaju o istoj.

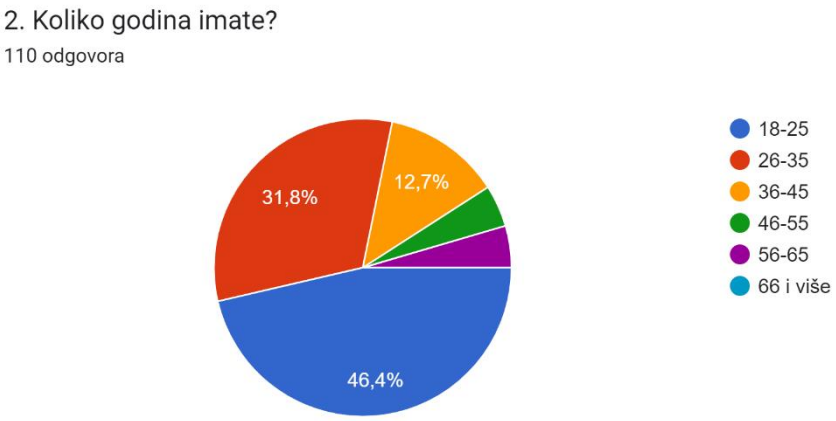
6.1 Metodologija rada

U radu se istražuje tema sigurnosti na internetu u Republici Hrvatskoj, s naglaskom na svijesti korisnika interneta o rizicima kibernetičkog kriminala i situacijama istoga u praksi. Istraživanje je provedeno na ciljanoj skupini punoljetnih korisnika interneta odnosno društvenih mreža u Hrvatskoj. Ispitivanje je provedeno na 110 ispitanika i svi ispitanici su ispunili anketu u cijelosti. Provođenje istraživanja odvijalo se digitalnim putem. Primarni cilj bio je prikupiti ispitanike sa Instagrama na način da je anketa objavljena putem Instagram priče te putem Facebooka gdje je anketa bila postavljena kao objava na profilu te u trima grupama koje se primjenjuju za dijeljenje anketa gdje korisnici jedni drugima pomažu rješavanjem anketa međusobno. Nadalje, istraživanje se provodilo putem računala u obliku ankete koja je kreirana uz pomoć alata Google Forms od 12.6.2024. do 15.6.2024. godine. Primarni cilj ovog istraživanja bio je utvrditi svijest, iskustva i reakcije ispitanika na kibernetički kriminal, s ciljem boljeg razumijevanja sigurnosti i ponašanja korisnika u digitalnom svijetu kako bi se u konačnici podizala svijest o računalnom kriminalu s ciljem njegova smanjenja. Kako bi se interpretirali rezultati koristili su se statistički pokazatelji poput aritmetičke sredine, a istraživačka anketa koja je provedena u svrhu ovog rada temelji se na prethodnom istraživanju koje je proveo Eurobarometar 2019. godine na temu Računalne sigurnosti i što Europljani misle o tome (European Commission, Directorate-General for Communication, 2020).

Anketa se sastojala od 22 pitanja, a odgovori su bili strukturirani sa više ponuđenih odgovora, u nekim pitanjima je bilo moguće dati više odgovora, dok u nekima samo jedan. Također, korištena je Likertova skala od 1 do 4 gdje je 1 označavalo stav Uopće se ne slažem, 2 stav uglavnom se ne slažem, 3 stav uglavnom se slažem, 4 stav Slažem se u potpunosti, uz dodatnu opciju pozicije 5 koja je označavala stav Ne znam. Osim toga korištena je Likertova skala s 4 pozicije gdje je 1 označavalo stav Vrlo zabrinut, 2 stav donekle zabrinut, 3 stav Ne naročito zabrinut i 4 Uopće nisam zabrinut.

6.2 Rezultati istraživanja

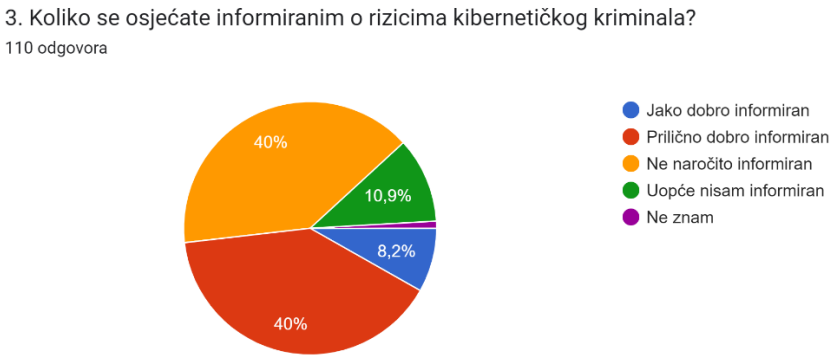
Ispitanici su iz Republike Hrvatske te je istraživanju pristupilo 59,1% žena, a 40,9% muškaraca, iz čega zaključujemo kako je istraživanju pristupilo više osoba ženskog spola negoli muškog.



Slika 1: Prikaz ispitanika ankete prema starosnoj dobi

Izvor: Istraživanje autora

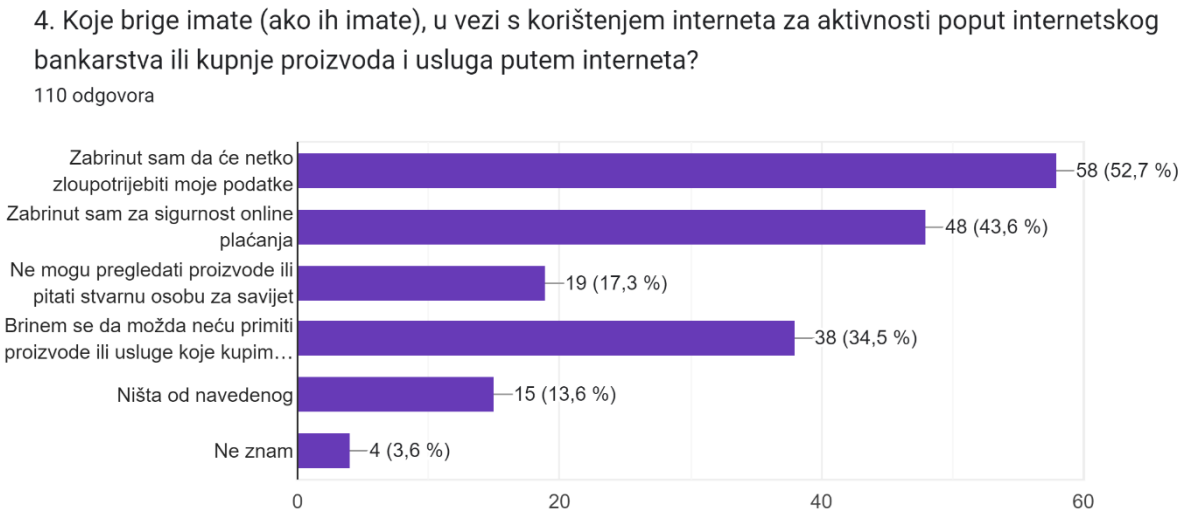
Slika 1 prikazuje da je starosna dob ispitanika koji su pristupili istraživanju između 18 i 65 godina. Prevladavaju ispitanici starosne dobi između 18 i 25 godina s čak 46,4%.



Slika 2: Prikaz informiranosti ispitanika o rizicima kibernetičkog kriminala

Izvor: Istraživanje autora

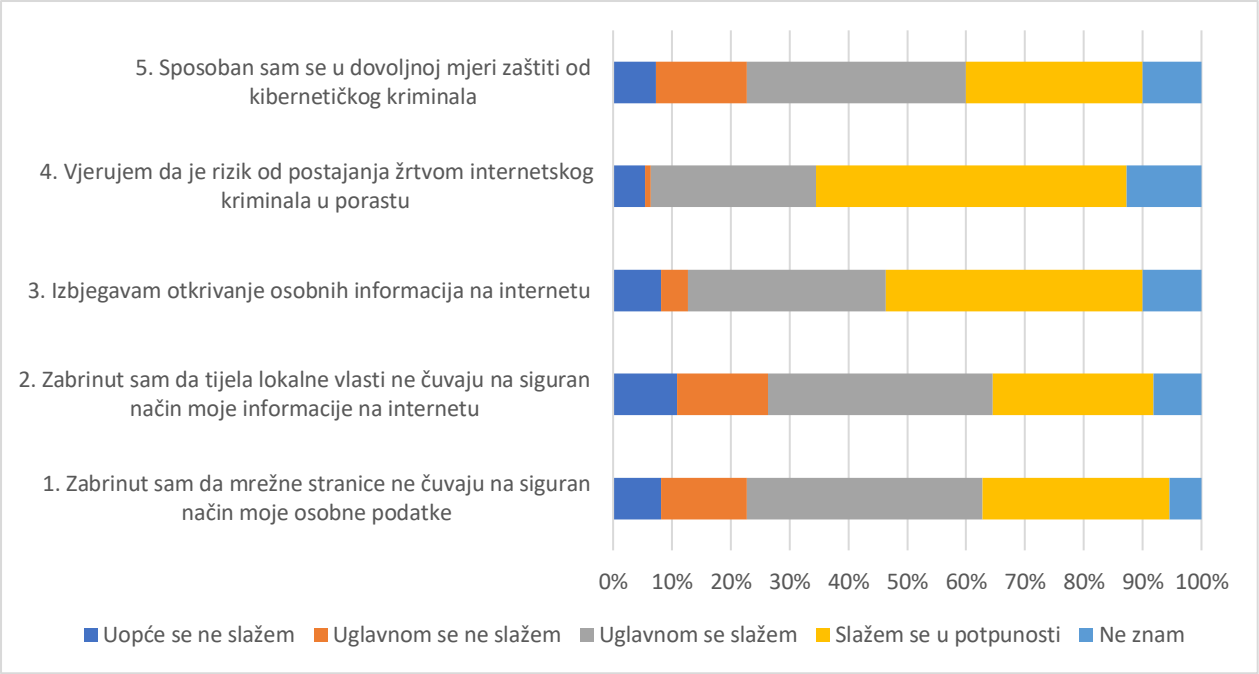
Slika 2 prikazuje informaciju o tome koliko su ispitanici informirani o kibernetičkom kriminalu. Prema dobivenim rezultatima zaključuje se kako jednak broj ispitanika smatra da nije naročito informiran i da je prilično informiran (40% za oba odgovora). Samo 10,9% ispitanika smatra kako uopće nije informiran, no zabrinjavajuća je činjenica podatka od 8,2% ispitanika koji su jako dobro informirani. Ovi podaci ukazuju na potrebu za povećanjem svijesti i informiranosti o kibernetičkom kriminalu kroz edukacije.



Slika 3: Prikaz zabrinutosti korisnika u vezi korištenja internetskih aktivnosti

Izvor: Istraživanje autora

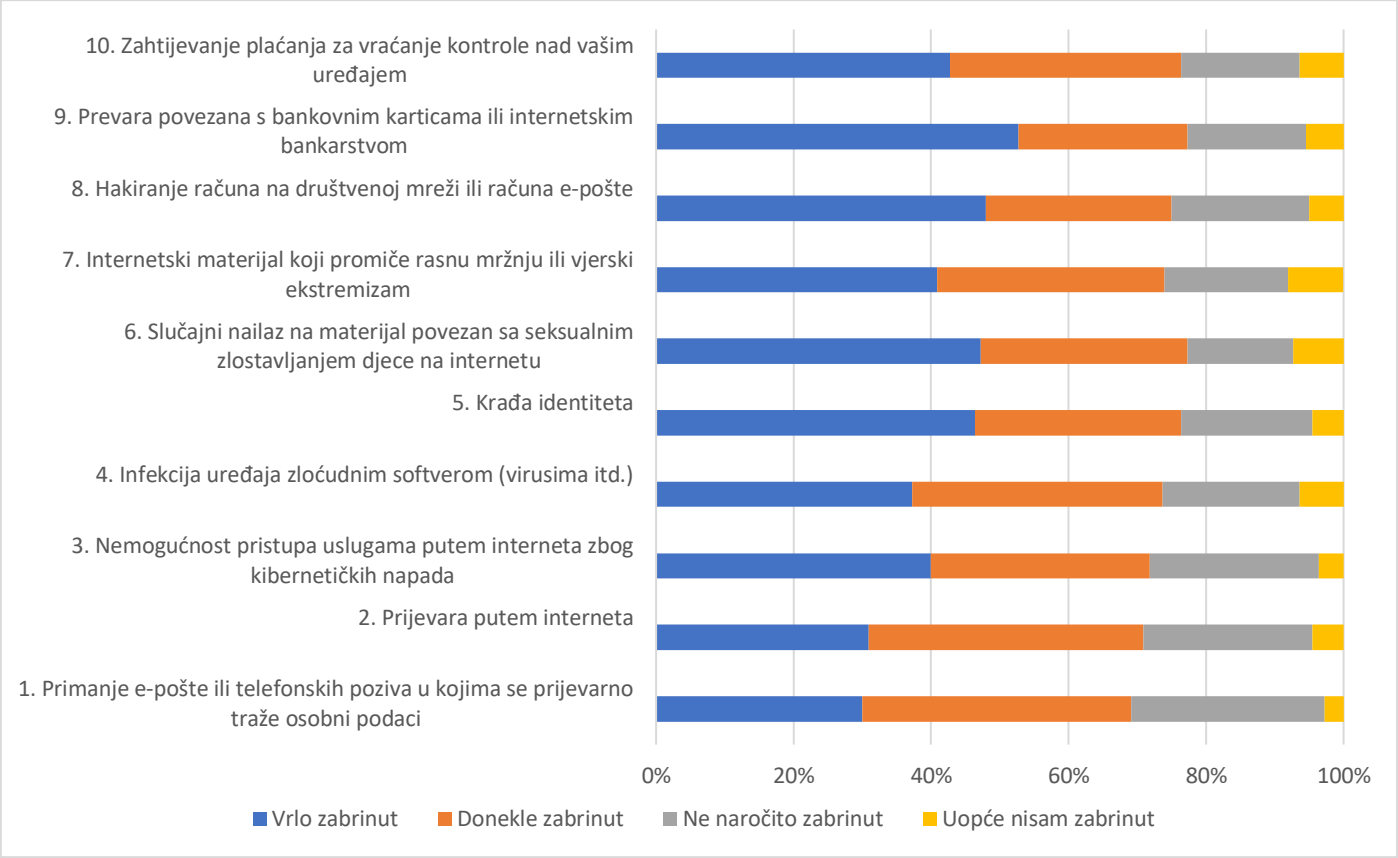
Slika 3 prikazuje zabrinutost u vezi sa korištenjem interneta za aktivnosti kao što su internetsko bankarstvo ili kupnja proizvoda i usluga putem interneta. Najveći postotak ispitanika, njih 52,7% je zabrinuto da će netko zloupotrijebiti njihove podatke, dok je nešto manji postotak tj. 43,6% ispitanika zabrinuto za sigurnost *online* plaćanja. Nadalje, 17,3% ispitanika je zabrinuto zbog toga što ne mogu pregledati proizvode ili pitati stvarnu osobu za savjet, dok je 34,5% ispitanika zabrinuto hoće li dobiti proizvode koje su kupili internetskim putem. Dakle, može se zaključiti kako su ispitanici izrazito zabrinuti za sigurnost u pogledu korištenja internetskih aktivnosti. Potrebno je poraditi na poboljšanju sigurnosnih mjera u Republici Hrvatskoj ukoliko gledamo internetske aktivnosti (uglavnom internertskih trgovina i slično).



Slika 4: Stajališta o različitim aspektima

Izvor: Istraživanje autora

Na slici 4 prikazana su stajališta o različitim aspektima. Prilikom računanja prosječne ocjene i standardne devijacije izuzeli su se ispitanici koji su na ponuđene tvrdnje odgovorili odgovorom Ne znam. U prvoj tvrdnji najveći broj ispitanika uglavnom se slaže da su zabrinuti da mrežne stranice ne čuvaju na siguran način osobne podatke, prosječna ocjena za prvu tvrdnju je 3,01 (SD=0,91), dok je 5,45% ispitanika odgovorilo sa Ne znam. Također, u drugoj tvrdnji najveći broj ispitanika, njih 38% se uglavnom slaže kako su zabrinuti da tijela lokalne vlasti ne čuvaju na siguran način informacije na internetu. Prosječna ocjena za drugu tvrdnju je 2,89 (SD=0,94), dok je 8,18% ispitanika odgovorilo s Ne znam. Na treću tvrdnju najveći broj ispitanika je odgovorio da se slaže u potpunosti sa izbjegavanjem otkrivanja osobnih informacija na internetu, njih 43%, dok je prosječna ocjena za tu tvrdnju 3,25 (SD=0.85), a 10% ispitanika odgovorilo sa Ne znam. 52% ispitanika vjeruje kako je rizik od postajanja žrtvom internetskog kriminala u porastu, dok je prosječna ocjena četvrte tvrdnje 3,47 (SD= 0,71), dok je 12,73% ispitanika odgovorilo s Ne znam. Ispitanici se uglavnom slažu kako su sposobni u dovoljnoj mjeri zaštiti se od kibernetičkog kriminala, njih 37%, dok je prosječna ocjena posljednje tvrdnje 3,00 (SD=0,88), a 10% ispitanika je odgovorilo s Ne znam.



Slika 5: Zabrinutost zbog kibernetičkog kriminala

Izvor: Istraživanje autora

Ispitivanje je pokazalo kako je 39,09% ispitanika donekle zabrinuto zbog primanja e-pošte ili telefonskih poziva u kojima se prijevarno traže njihovi podaci. Prosječna ocjena zabrinutosti za prvu tvrdnju je 2,96 (SD=0,83). 40% ispitanika je donekle zabrinuto za prijevare putem interneta u kojima kupljena roba nije dostavljena ili je krivotvorena ili ne odgovara onome što je navedeno kod oglašavanja. Prosječna ocjena zabrinutosti za drugu tvrdnju jest 2,97(SD=0,86). Osim toga, 40% ispitanika je vrlo zabrinuto za nemogućnost pristupa internetskim uslugama zbog kibernetičkih napada, te je prosječna ocjena zabrinutosti za treći tvrdnju 3,29 (SD=0,91). Za infekcije uređaja sa zloćudnim softverima vrlo je zabrinuto 37% ispitanika, dok je prosječna ocjena zabrinutosti za četvrtu tvrdnju 3,22 (SD=0,93).Ispitanici su vrlo zabrinuti za krađu identiteta, njih 46 %. Prosječna ocjena zabrinutosti za petu tvrdnju jest 3,18 (SD=0,89). 47% ispitanika vrlo je zabrinuto u svezi slučajnog nailaska na materijal povezan sa seksualnim zlostavljanjem djece na internetu, prosječna ocjena zabrinutosti za šestu tvrdnju jest 3,17 (SD=0,91). Istraživanje je također pokazalo kako 41% ispitanik je vrlo zabrinut za slučajni nailazak na materijal povezan sa seksualnim zlostavljanjem djece na internetu, prosječna ocjena za sedmu tvrdnju jest 3,06 (SD=0,94). Ispitanici su vrlo zabrinuti za hakiranje računa na društvenoj mreži ili računima e-pošte, njih 48%. Prosječna ocjena

zabrinutosti za osmu tvrdnju jest 3,19 (SD=0,88). Za prijevare povezane s bankovnim karticama ili internetskim bankarstvom vrlo je zabrinuto 53% ispitanika, dok je prosječna ocjena za devetu tvrdnju 3,24 (SD=0.90). Na posljetku, 43% ispitanika je vrlo zabrinuto za zahtijevanje plaćanja određenog iznosa u zamjenu za vraćanje kontrole nad njihovim uređajem. Prosječna ocjena za desetu tvrdnju jest 3,13 (SD=0,92).

Slika 6: Prikaz promjene korisničkih zaporki

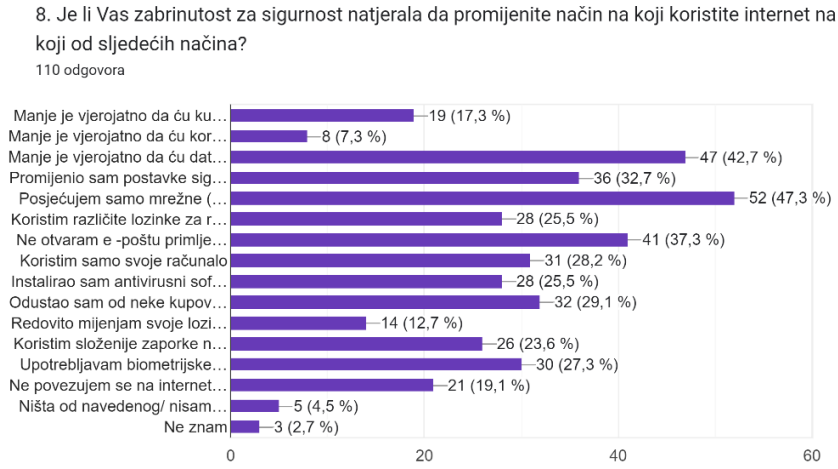
Izvor: Istraživanje autora

Slika 6 prikazuje odgovor na pitanje jesu li ispitanici promijenili svoju zaporku na nekim od internetskih usluga. Najveći broj ispitanika je u proteklih 12 mjeseci promijenio zaporku na društvenim mrežama, čak 41,8% ispitanika. 30,9% ispitanika promijenilo je lozinku na e-pošti, dok je 18,2% ispitanika promijenilo zaporku na internetskom bankarstvu. Također, 12,7% ispitanika promijenilo je zaporku na mrežnim mjestima za kupovinu, dok je 8,2% ispitanika promijenilo zaporku na mrežnim mjestima javnih usluga. Osim toga, najmanji broj ispitanika promijenio je zaporku na igrama koje se igraju putem interneta, točnije njih 3,6%. Iz prethodnoga može se zaključiti kako ispitanici najčešće mijenjaju zaporke na društvenim mrežama na internetu što ukazuje na veću osjećaj rizika ili nesigurnosti u svezi istih. Mijenjanje zaporki zbog sigurnosti od velike je važnosti, a čak 31,8% korisnika ne mijenja zaporke na navedenim internetskim uslugama što bi se zbog prevencije računalnog kriminala trebalo smanjiti.

Tvrdnje koje su ponuđene kao odgovor u slici sedam su sljedeće:

A. Manje je vjerojatno da ću kupovati proizvode ili usluge putem interneta
B. Manje je vjerojatno da ću koristiti Internet bankarstvo
C. Manje je vjerojatno da ću dati svoje osobne informacije na mrežnim mjestima

D. Promijenio sam postavke sigurnosti (npr. u svom pregledniku, na internetskoj društvenoj mreži, u tražilici)
E. Posjećujem samo mrežne (web) stranice koje poznajem i kojima vjerujem
F. Koristim različite lozinke za različite stranice
G. Ne otvaram e -poštu primljenu od ljudi koje ne poznajem
H. Koristim samo svoje računalo
I. Instalirao sam antivirusni softver
J. Odustao sam od neke kupovine putem interneta zbog sumnje u prodavača ili mrežnu (web) stranicu
K. Redovito mijenjam svoje lozinke
L. Koristim složenije zaporke nego inače
M. Upotrebljavam biometrijske značajke (npr. prepoznavanje lica, otisak prsta)
N. Ne povezujem se na internet putem nezaštićenih pristupnih točki
O. Ništa od navedenog/ nisam zabrinut za sigurnost na internetu

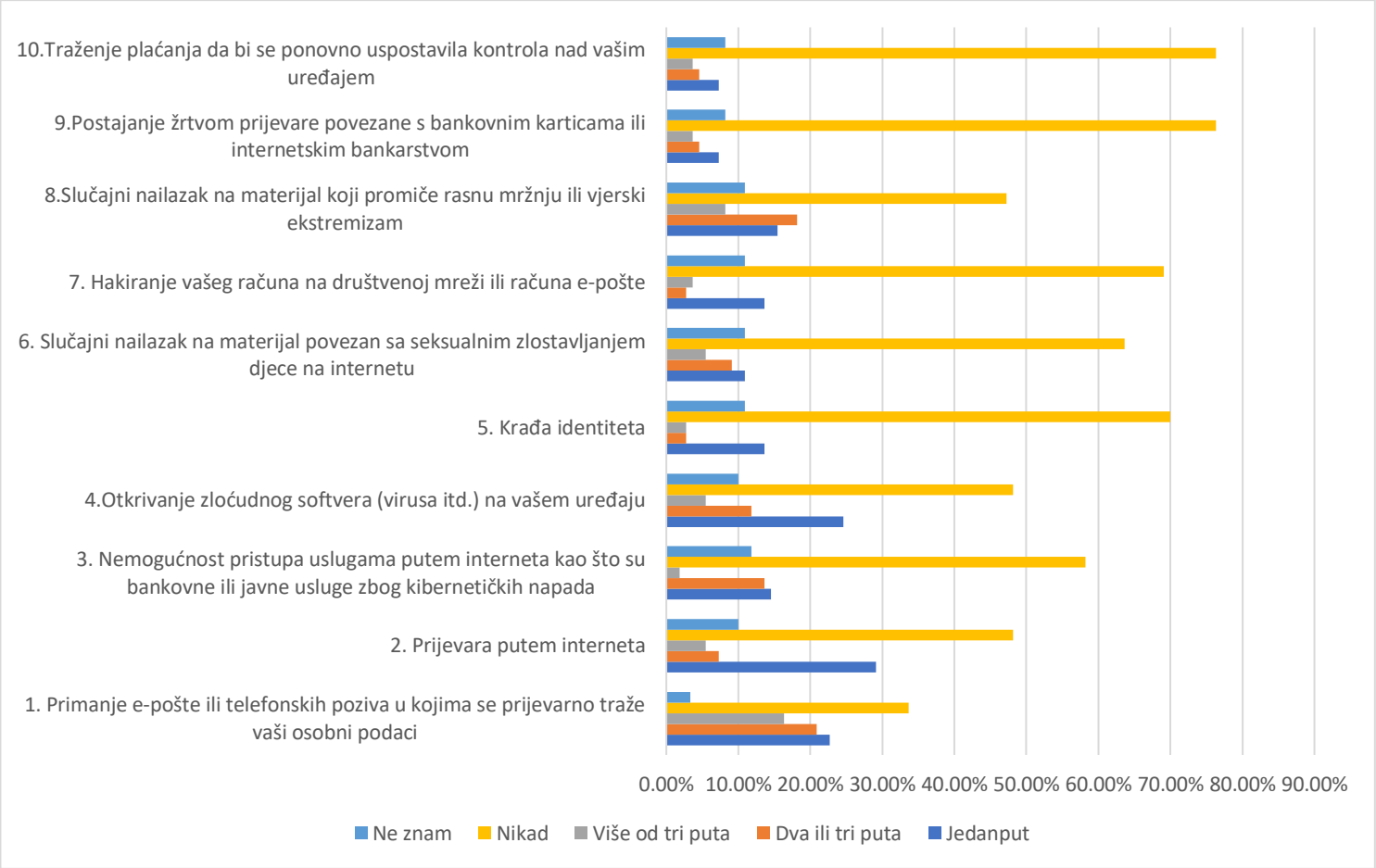


Slika 7: Prikaz zabrinutosti korisnika za sigurnost

Izvor: Istraživanje autora

Slika 7 prikazuje kako su ispitanici svjesni rizika na internetu, te kako prilagođavaju svoje ponašanje na internetu sa svrhom osobne zaštite. Najveći broj ispitanika, njih 47,3% posjećuje samo mrežne stranice koje poznaju i kojima vjeruju, što pokazuje da ispitanici imaju visok stupanj opreza i povjerenja u povjerljive izvore. Također, veći dio ispitanika, njih 42,7% izbjegava davanje osobnih informacija na mrežnim mjestima, što također ukazuje na

zabrinutost ispitanika za privatnost i sigurnost osobnih podataka. S druge strane, najmanji broj ispitanika, njih 4,5% nije promijenio svoje ponašanje na internetu jer nisu zabrinuti. Ovaj dio ispitanika je u manjini što ukazuje da nisu svjesni rizika na internetu, i da je ipak veći dio ispitanika svjestan rizika i poduzima radnje u svrhu zaštite osobnih podataka.



Slika 8: Prikaz učestalosti osobnih iskustava u zadnje tri godine

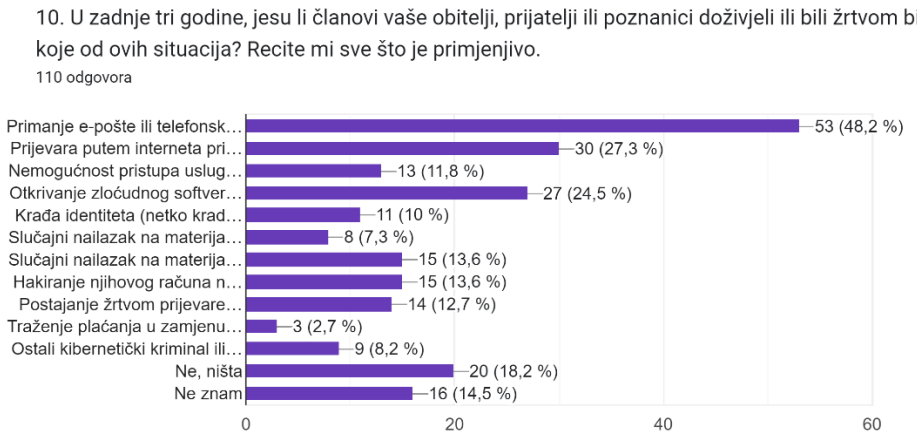
Izvor: Istraživanje autora

Slika 8 prikazuje odgovore na pitanja o učestalosti osobnih iskustava u zadnje tri godine. U posljednje tri godine 33,64% ispitanika nikad nije primilo e-poštu ili telefonski poziv u kojemu se prijevarom traže osobni podaci, dok je 22,73% ispitanika jedanput primilo e-poštu ili telefonski poziv u kojemu se prijevarom traže osobni podaci. U posljednje tri godine 48,18% ispitanika nikad nije doživjelo prijevaru putem interneta, dok je 29,09% ispitanika doživjelo jedanput prijevaru putem interneta. U posljednje tri godine 58,18% ispitanika nikad nije moglo ne pristupiti uslugama putem interneta (bankovne, javne) zbog kibernetičkih napada, dok se 14,55% ispitanika susrelo jedanput sa navedeno situacijom. Također, u posljednje tri godine 48,18% ispitanika nikad nije otkrilo nekakvu vrstu zloćudnog softvera na uređaju, dok je 24,55% ispitanika jedanput otkrilo nekakvu vrstu zloćudnog softvera.

Čak 70 % ispitanika se nije nikad susrelo sa krađom identiteta, dok se 13,64% ispitanika susrelo jedanput sa krađom identiteta. Ispitanici se nikad nisu susreli sa slučajnim nailaskom na materijal povezan sa seksualnim zlostavljanjem djece, točnije 63,64% ispitanika, dok se 13,64% ispitanika susrelo jedanput. U posljednje tri godine 69,09% ispitanika se nikad nije susrelo sa hakiranjem računa na društvenim mrežama, dok se 13,64% jedanput susrelo sa hakiranjem računa na društvenim mrežama.42,27% ispitanika se nikad nije susrelo sa slučajnim nailaskom na materijal koji promiče rasnu mržnju ili vjerski ekstremizam, dok se 18,18% ispitanika susrelo dva ili tri puta sa materijalom koji promiče rasnu u mržnju ili vjerski ekstremizam. Većina ispitanika njih 73,36% nikad nije postalo žrtvom prijevare koja je povezana s bankovnim karticama ili internet bankarstvom, dok se 7,27% ispitanika susrelo jedanput sa situacijom u kojoj su bili žrtva prijevare bankovnim karticama. Naposljetku, većina ispitanika, njih 76,36 se nikad nije susrela da netko traži novac u zamjenu za vraćanje kontrole nad njihovim uređajem, dok se 4,55% ispitanika jedanput susrelo sa navedenom tvrdnjom.

Tvrdnje koje su ponuđene kao odgovor u slici 10 su sljedeće:

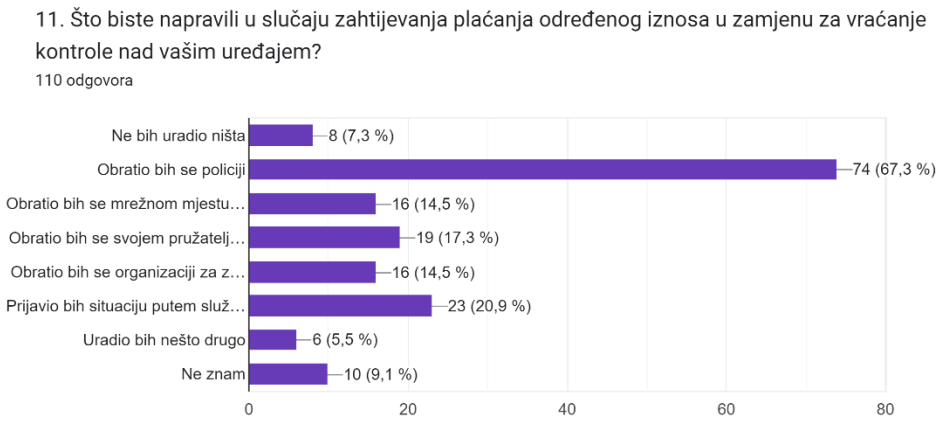
A. Primanje e-pošte ili telefonskih poziva u kojima se prijevarno traže njihovi osobni podaci (uključujući pristup njihovom računalu, korisnička imena i zaporke, informacije o bankovnim poslovima ili plaćanju)
B. Prijevara putem interneta pri kojoj kupljena roba nije isporučena, ili je krivotvorena, ili ne odgovara onome što je navedeno pri oglašavanju
C. Nemogućnost pristupa uslugama putem interneta kao što su bankovne ili javne usluge zbog kibernetičkih napada
D. Otkrivanje zlođudnog softvera (virusi itd. na njihovom uređaju)
E. Krađa identiteta (netko krade njihove osobne podatke i predstavlja se kao oni)
F. Slučajni nailazak na materijal povezan sa seksualnim zlostavljanjem djece na internetu
G. Slučajni nailazak na materijal koji promiče rasnu mržnju ili vjerski ekstremizam
H. Hakiranje njihovog računa na društvenim mrežama ili računa e- pošte
I. Postajanje žrtvom prijevare povezane s bankovnim karticama ili internetskim bankarstvom
J. Traženje plaćanja u zamjenu za ponovnu uspostavu kontrole nad njihovim uređajem
K. Ostali kibernetički kriminal ili drugo protuzakonito ponašanje na internetu (kibernetički napadi, zlostavljanje ili maltretiranje putem interneta)
L. Ne, ništa



Slika 9: Iskustva s internetskim sigurnosnim prijetnjama kod obitelji i prijatelja u posljednje tri godine

Izvor: Istraživanje autora

Prema rezultatima istraživanja najveći broj ispitanika, njih 48,2% je naveo da su njihove obitelji, poznanici ili prijatelji bili metom lažnih e-pošti ili telefonskih poziva u kojima se prijevarno traže njihovi osobni podaci, što nam ukazuje da su *phishing* napadi uvelike prisutni. S druge strane, najmanji broj ispitanika, njih 2,7% je naveo kako su njihove obitelji, poznanici ili prijatelji bili žrtvom napada u kojima napadači traže plaćanje za ponovnu uspostavu kontrole nad uređajem.

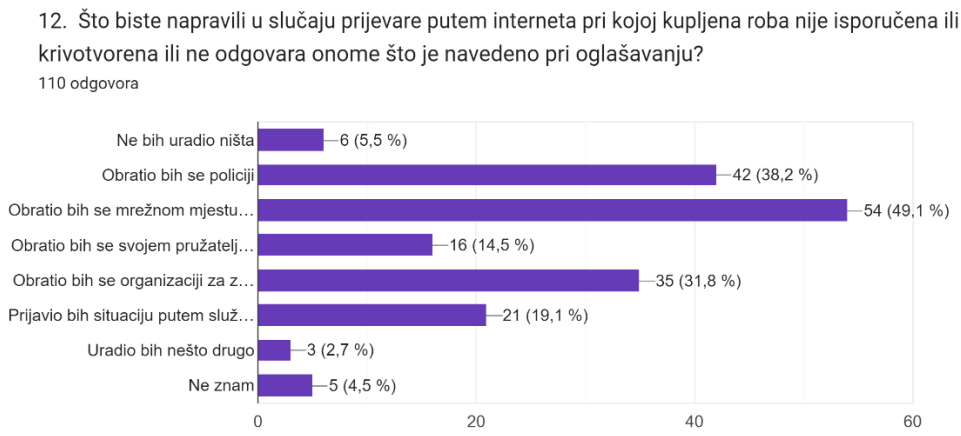


Slika 10: Iskustva s plaćanjem za povrat kontrole nad uređajem

Izvor: Istraživanje autora

Pitanja od 11 do 20 u anketi bila su koncipirana tako da su ispitanicima predstavljene određeni scenariji, a oni su morali odgovoriti što bi učinili u tim situacijama. Ponuđeni odgovori na ta pitanja su bili identični.

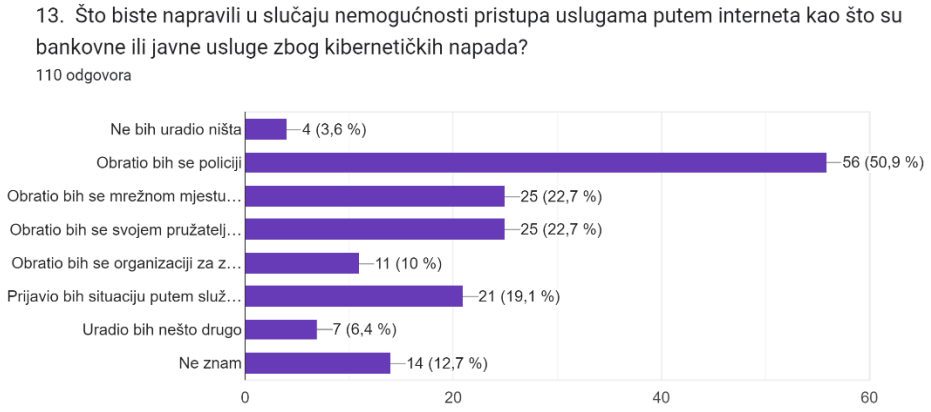
Prema istraživanju najveći broj ispitanika, njih 67,3% da se nađe u situaciji da netko zahtijeva plaćanje u zamjenu za vraćanje kontrole nad njihovim uređajem bi se obratio policiji, dok bi najmanji broj ispitanika, njih 5,5% uradilo nešto drugo po vlastitom nahođenju. Iz navedenoga može se zaključiti kako najveći postotak ispitanika ima najviše povjerenja u policiju, dok je je manji dio ispitanika sklon rješavanju ovakvih problema na drugačiji način.



Slika 11: Reakcije na internetsku prijevaru u kupovini: preferencije i postupci ispitanika

Izvor: Istraživanje autora

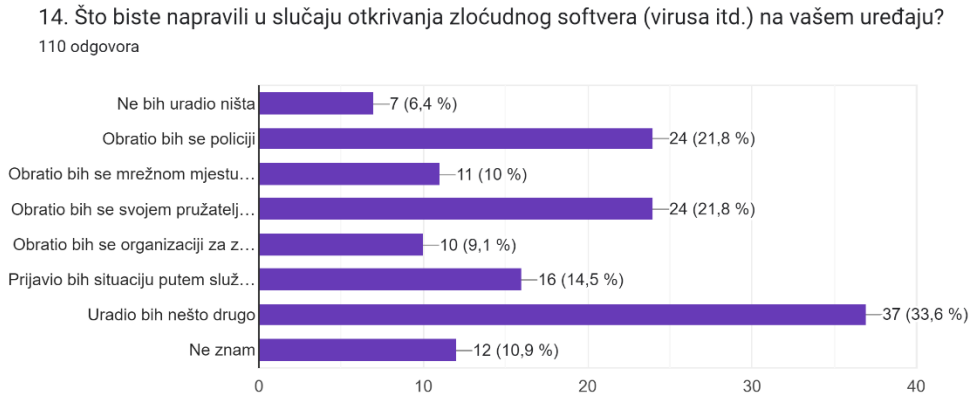
Najviše ispitanika, odnosno 49,1 % bi u situaciji internetske prijevare u kojoj kupljena roba nije isporučena ili je krivotvorena ili ne odgovara onome što je navedeno pri oglašavanju bi kontaktiralo prodavača ili mrežno mjesto, dok bi najmanji broj ispitanika, njih 2,7% uradilo nešto drugo. Iz prethodnoga možemo zaključiti kako je veći dio ispitanika osviješten kako reagirati u ovakvim situacijama, te bi većina ispravno postupila.



Slika 12: Reakcije na kibernetički napad: postupci korisnika u nemogućnosti pristupa internetskim uslugama

Izvor: Istraživanje autora

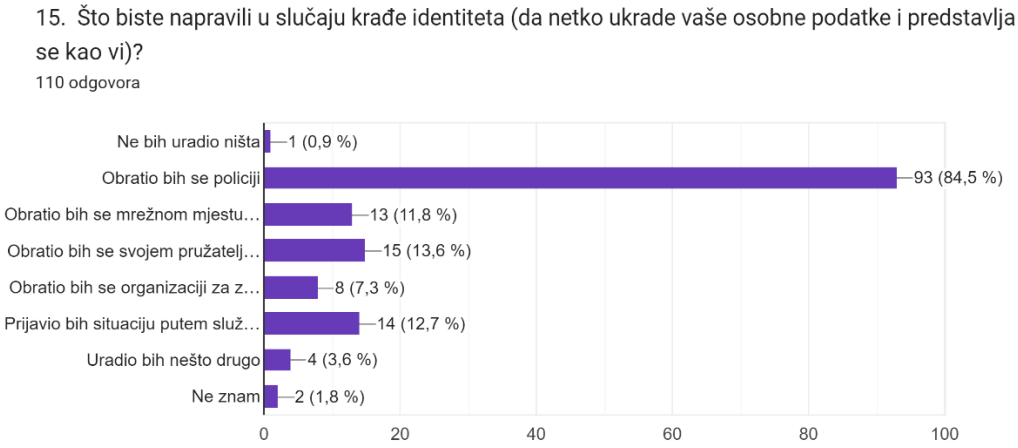
Na slici 13. može se vidjeti kako bi se 50,9% ispitanika u situaciji nemogućnosti pristupa uslugama kao što su javne usluge ili bankovne usluge obratila policiji, dok bi najmanji broj ispitanika učinilo nešto drugo, njih 6,4%. Iz prethodnoga, može se zaključiti kako većina ispitanika najviše povjerenja ima u policiju kao i u prethodnim pitanjima ovog tipa.



Slika 13: Reakcija na otkrivanje zloćudnih softvera

Izvor: Istraživanje autora

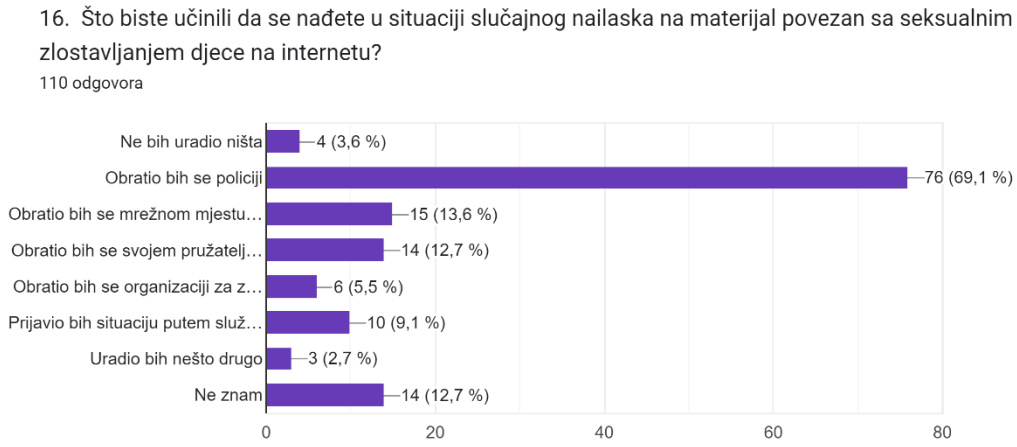
Iz slike 14 zaključujemo kako niti jedan od ponuđenih odgovora nisu odgovarali specifičnoj situaciji pa bi najveći broj ispitanika, njih 33,6% uradilo nešto drugo, dok najmanji broj ispitanika, njih 6,4% ne bi uradilo ništa.



Slika 14: Reakcija na krađu identiteta

Izvor: Istraživanje autora

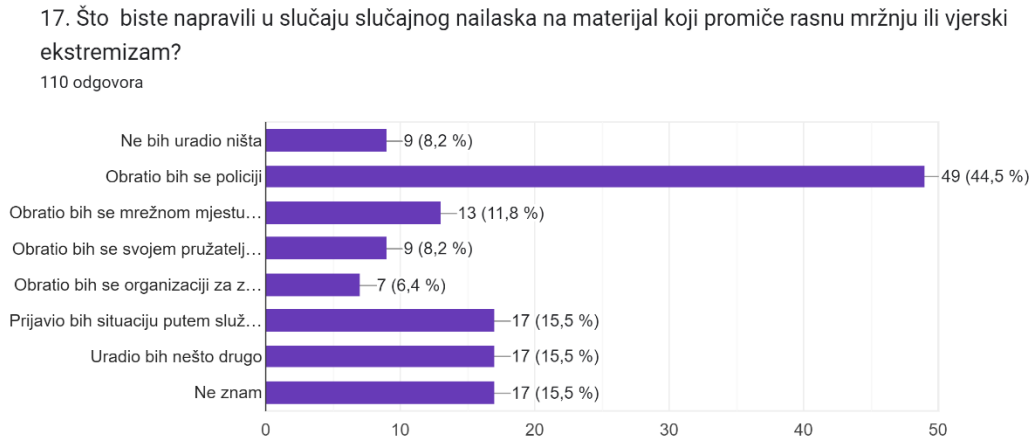
U situaciji kada bi se ispitanicima dogodila krađa identiteta (da netko ukrade njihove podatke i lažno se predstavlja), najveći dio ispitanika bi se obratio policiji, 84,5%. S druge strane, najmanji broj ispitanika ne bi uradilo ništa, njih 0,9%.



Slika 15: Reakcije na slučajni nalazak materijala o dječjem seksualnom zlostavljanju na internetu

Izvor: Istraživanje autora

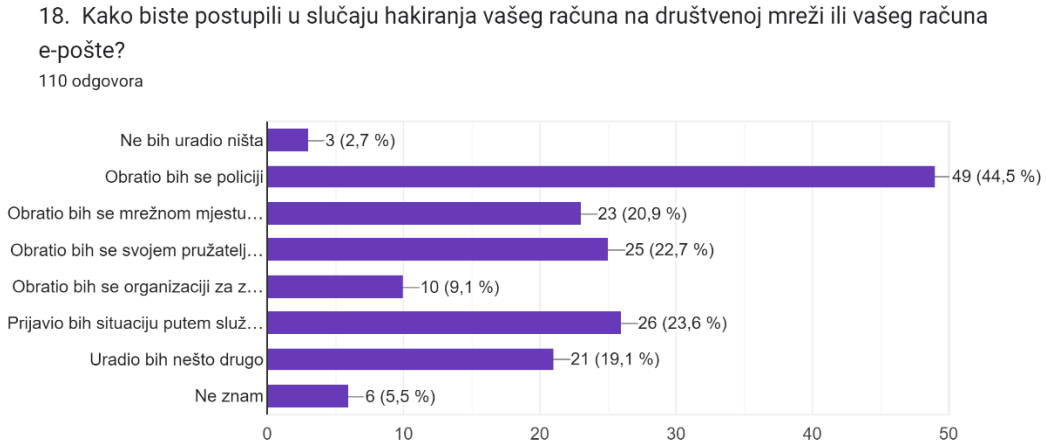
U situaciji slučajnog nailaska na materijal o dječjem seksualnom zlostavljanju većina ispitanika bi se obratila policiji, njih 69,1%. Dok bi najmanji dio ispitanika, njih 2,9% uradilo nešto drugo. U ovakvim ozbiljnim situacijama najispravnije je obratiti se policiji, tako da se može zaključiti kako bi većina ispitanika postupila ispravno.



Slika 16: Reakcije na slučajni nalazak materijala koji promiče rasnu mržnju ili vjerski ekstremizam

Izvor: Istraživanje autora

U situaciji slučajnog nailaska na materijal koji promiče rasnu mržnju ili vjerski ekstremizam 44,5% ispitanika bi se obratilo policiji, dok bi se najmanji dio ispitanika, njih 6,4% obratilo organizaciji za zaštitu potrošača. Dakako, može se zaključiti kako je potrebna edukacija o pojedinim vrstama kibernetičkog kriminala kako bi ispitanici znali kontaktirati ispravne službe za pomoć.

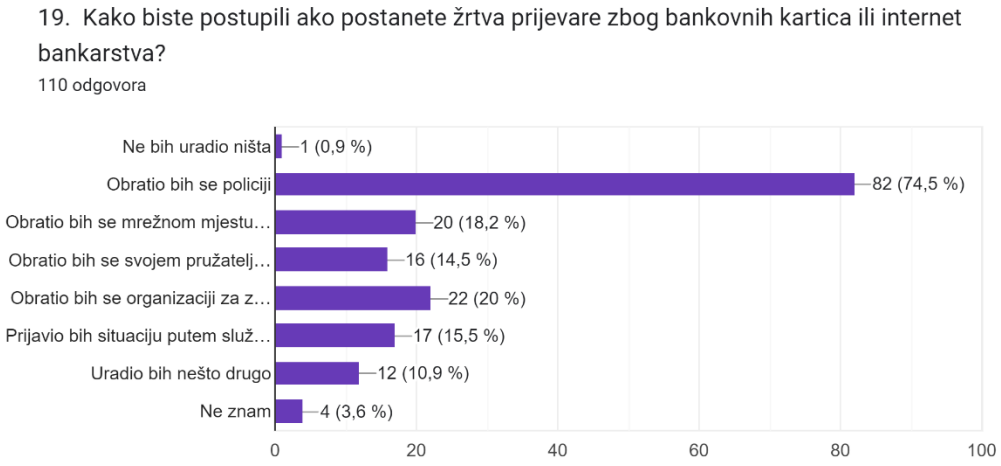


Slika 17: Reakcije na situaciju hakiranja računa

Izvor: Istraživanje autora

Ukoliko bi se ispitanici pronašli u situaciji hakiranja njihova računa na društvenim mrežama ili računima e-pošte , najveći dio bi se obratio policiji, njih 44,5. S druge strane, najmanji dio

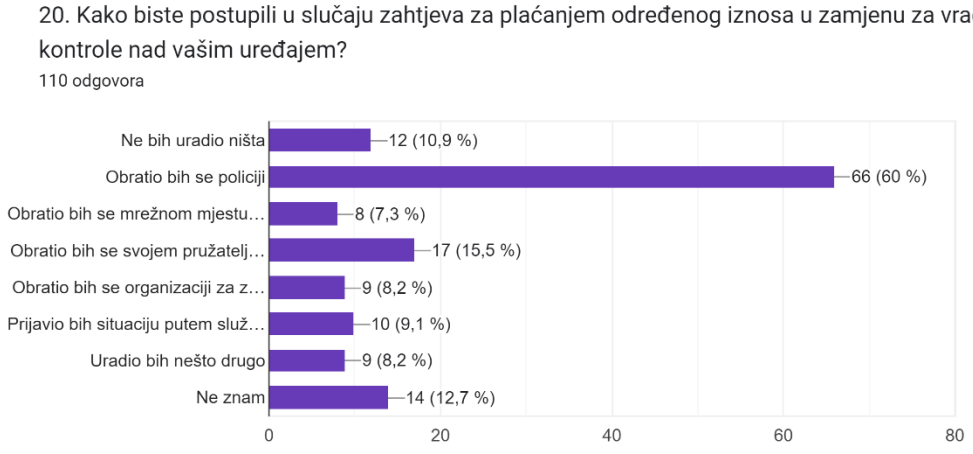
ispitanika 2,7% ne bi uradilo ništa. Može se zaključiti kao i do sada najveći dio ispitanika vjeruje policiji, dok samo mali dio ipak ništa ne bi uradio u ovoj situaciji.



Slika 18: Reakcije na prijevaru s bankovnim karticama i Internet bankarstvom

Izvor: Istraživanje autora

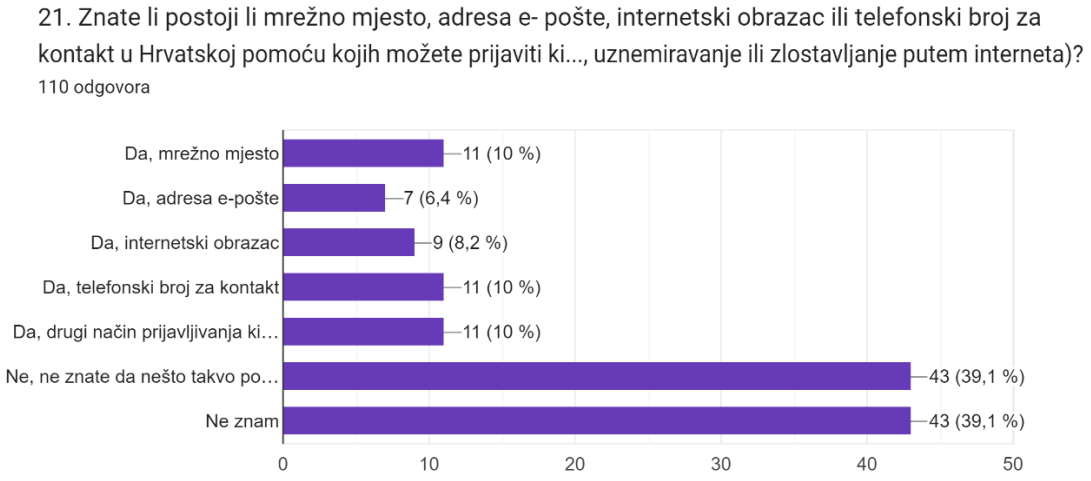
U situaciji internetske prijevare u obliku bankovnih kartica ili internetskog bankarstva, najveći dio ispitanika bi se obratio policiji, njih 74,5%. Najmanji dio ispitanika ne bi uradio ništa, njih 0,9%. U ovoj situaciji naravno treba obavijestiti i svoju banku pa se može zaključiti kako ispitanici nisu najbolje informirani koga točno trebaju kontaktirati u ovoj situaciji.



Slika 19: Reakcije na zahtjev za otkupninu za povrat kontrole nad uređajem

Izvor: Istraživanje autora

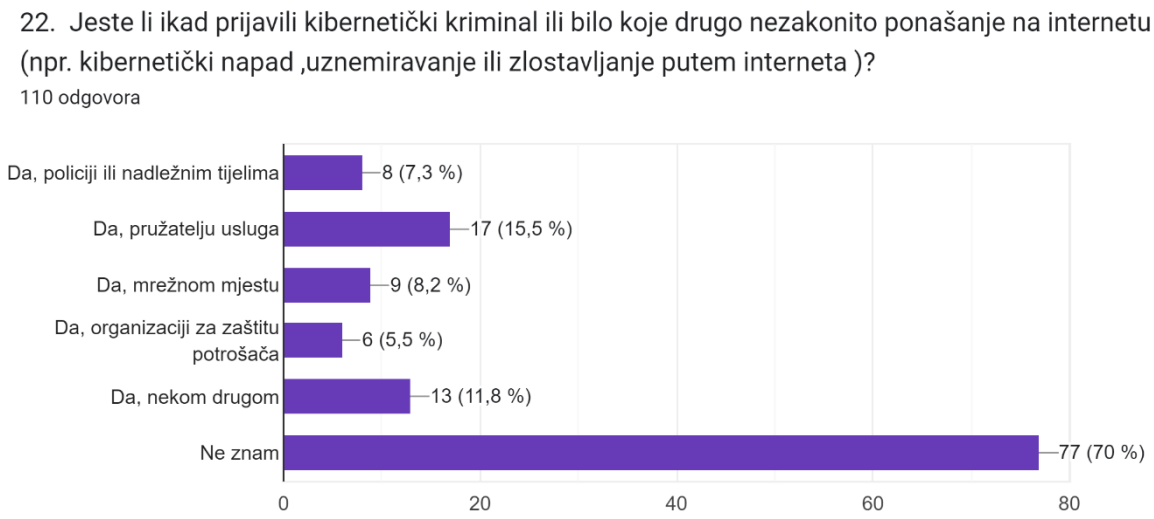
Na posljednjem primjeru u ovome nizu pitanja može se zaključiti kako bi se najveći dio ispitanika, njih 60% u slučaju da netko zahtjeva novac u zamjenu za kontrolu nad njihovim uređajem obratio policiji. Najmanji dio ispitanika, njih 7,3% obratilo bi se mrežnom mjestu ili prodavaču.



Slika 20: Metode prijave kibernetičkog kriminala i nezakonitog ponašanja na internetu u Hrvatskoj

Izvor: Istraživanje autora

Najviše ispitanika, odnosno 39,1% ne zna da postoji mrežno mjesto, adresa-pošte, internetski obrazac ili telefonski broj za kontakt u Hrvatskoj gdje se mogu prijaviti razna uznemiravanja putem interneta. Dok najmanji dio ispitanika, njih 6,4% zna da postoji takva adresa e-pošte. Iz rezultata može se zaključiti kako je potrebno uložiti u edukaciju građana Hrvatske o tome komu i na koji način se mogu obratiti ukoliko se susretnu sa kibernetičkim kriminalom.



Slika 21: Iskustva s prijavom kibernetičkog kriminala i nezakonitog ponašanja na internetu

Izvor: Istraživanje autora

Najveći dio ispitanika, njih 70% je odgovorilo da ne zna odgovor na pitanje jesu li ikada prijavili kibernetički kriminal ili bilo koje drugo nezakonito ponašanje na internetu, dok je najmanji dio ispitanika njih 5,5% prijavilo kibernetički kriminal ili neko drugo nezakonito ponašanje na internetu organizaciji za zaštitu potrošača.

6.3 Istraživačka ograničenja i preporuke

Rezultati ovog istraživanja jasno prikazuju informiranost ispitanika o sigurnosti na internetu, no ipak treba obratiti pozornost na ograničenja provedenog istraživanja. Prvo ograničenje odnosi se na veličinu uzorka. Ispitano je ukupno 110 ispitanika u Republici Hrvatskoj što nije dovoljno velik uzorak za donošenje konkretnih zaključaka. No, unatoč ograničenju za potrebe rada zbog kojeg je provedena anketa moguće je donijeti indikativne zaključke, dok bi za cjelovit prikaz bilo potrebno napraviti anketu na većem i reprezentativnom uzorku.

Još jedno od ograničenja može biti Likertova skala. U Likertovoj skali jedan od ponuđenih odgovora je bio Ne znam, a taj odgovor nije mjerljiv i ispitanici koji su u tim pitanjima označili odgovor Ne znam morali su se izuzeti iz računanja prosječne ocjene. Osim toga, bez obzira na to što je anketa bila anonimna ne smije se zaboraviti da je moguća pristranost ispitanika u davanju odgovora.

Anketa koja je provedena u svrhu ovog rada temelji se na prethodnom istraživanju koje je proveo Eurobarometar 2019. godine na temu Računalne sigurnosti i što Europljani Europljani

misle o tome (European Commission, Directorate-General for Communication, 2020), a navedeno istraživanje je opširno i zahtjeva koncentraciju zbog većih ponuđenih odgovora zbog čega je bilo teško doći do većeg broja ispitanika.

Ukoliko se gleda demografska raznolikost poželjno je za buduća istraživanja pronaći jednak broj ispitanika iz svih dobnih skupina. Sama tema istraživanja je kompleksna i ne priča se dovoljno o njoj zbog čega ispitanici mogu biti nedovoljno educirani.

Preporuka je svakako proširiti veličinu uzorka kako bi se dobili reprezentativniji podaci. Osim toga, bilo bi poželjno na razne načine educirati građane RH o temi sigurnosti na internetu. Kontinuirano praćenje trendova te korištenje rezultata istraživanja u praksi također je jedna od preporuka ovog istraživanja.

7. Rasprava

Kao što je u metodologiji spomenuto istraživanje koje je provedeno za potrebe ovog diplomskog rada oslanja se na istraživanje koje je proveo Euro barometar (European Commission, Directorate-General for Communication, 2020). Ukoliko uspoređujemo istraživanje koje je provedeno za Euro barometar i istraživanje koje je provedeno za potrebe ovog rada može se primijetiti kako su na većinu pitanja ispitanici odgovarali isto, uz odstupanja na samo nekoliko pitanja. Naravno važno je za napomenuti kako je u istraživanju od Euro barometra sudjelovalo 1016 ispitanika iz Republike Hrvatske, dok je u ispitivanju za potrebe diplomskog rada sudjelovalo 110 ispitanika.

Na pitanje o stajalištima različitih aspekata kibernetičkog kriminala ispitanici u istraživanju koje je provedeno za diplomski rad, uglavnom su se slagali sa tvrdnjama, dok su se u izvornom ispitanici u potpunosti slagali sa tvrdnjama. Osim toga, kod pitanja o promjeni korisničkih zaporki ispitanici istraživanja provedenog za ovaj rad najčešće su mijenjali lozinke na društvenim mrežama, dok u izvornom istraživan ju nisu uopće mijenjali. S obzirom na razmak od 2019. kad je provedeno izvorno istraživanje pa sve do 2024., može se primijetiti kako su ispitanici u istraživanju postali osviješteniji o rizicima kibernetičkih napada i važnosti mijenjanja korisničkih zaporki. Također, pitanja od 11 do 20 su bila strukturirana na način da su ispitanicima postavljene određene situacije a oni su morali odgovoriti što bi učinili u toj situaciji, u većini odgovora ispitanici bi se obratili policiji što je ispravno, ali u nekim situacijama je ipak potrebno kontaktirati specijalizirane službe iz čega se može zaključiti kako ispitanici nisu dovoljno informirani te educirani te su upravo to stavke na kojima je potrebno raditi s ciljem smanjenja stope kibernetičkih napada.

Nadalje, može se zaključiti kako je u istraživanju sudjelovalo više ispitanika ženskog spola (59,1%) negoli muškog spola (40,9%). Također ovo istraživanje je obuhvatilo sve dobne skupine pri čemu ima najviše ispitanika u dobi od 18 do 25 godina što bi značilo na veću prisutnost mlade populacije.

Potrebno je naglasiti kako je razina informiranosti ispitanika o kibernetičkom kriminalu oscilirajuća iz razloga što podjednak dio ispitanika (40%) smatra da nije naročito informiran i da je prilično informiran. Iz dobivenih rezultata vidljivo je kako je potrebno educirati građane Hrvatske o rizicima kibernetičkog kriminala i njegovim napadima.

Osim toga, jedna od glavnih stavki koje su zabrinjavale ispitanike jest sigurnost prilikom korištenja internetskih usluga kao što su internetsko bankarstvo ili internetska kupovina.

Ispitanici su tu izrazili veći stupanj zabrinutosti (52,7%), kao i kod online plaćanja (43,6%). Može se donijeti zaključak kako su ispitanici u velikoj razini zabrinuti za sigurnost i privatnost svojih podataka prilikom korištenja interneta.

Iz istraživanja se također može zaključiti kako gotovo polovica ispitanika (48,18%) nikada nije doživjela prijevaru putem interneta u kojemu roba ili usluge koje su kupili nisu bili isporučeni ili su bili krivotvoreni, dok s druge strane zabrinutost za ovakvu vrstu prijevare je visoka, prosječna ocjena jest 3,45.

Naposljetku, većina ispitanika nije svjesna da postoje određene internetske stranice i kontakti na koje se mogu obratiti ukoliko se susretnu sa nekom vrstom kibernetičkog napada, iz čega je se zaključuje kako je osim na edukaciji korisnika potrebno raditi i na promociji institucija koje se bave kibernetičkim kriminalom.

Zaključno, kibernetički kriminal je složen i rastući izazov današnjeg modernog svijeta. Kibernetički kriminal zahtjeva edukaciju, zaštitu osobnih podataka te općenito podizanje svijesti kako bi se njegova stopa smanjila. Rezultati istraživanja pokazuju kako je potrebno ulaganje u obrazovanje svih građana Republike Hrvatske o temi kibernetičkog kriminala, osim toga potrebno je kontinuirano unaprjeđenje sigurnosnih mjera na računalnim sustavima kako bi se smanjila stopa napada, ali i zaštitili osobni podaci.

8. Zaključak

Sveukupan zaključak ovog rada bi bio da je pojavom i razvojem marketinškog informacijskog sustava te njegovog napretka i razvoja kroz povijest razvio i računalni kriminal. Ugrubo rečeno, marketinški informacijski sustav je zadužen da informacija dođe do ovlaštenih osoba. Definiramo ga kao sustav ljudi, opreme i organizacije koji prikuplja, analizira i distribuira informacije donositeljima marketinških odluka. Računalni kriminal kao pojam pojavio se već 1887. godine pojavom električnog tabulatora, a definiramo ga kao niz ilegalnih radnji i prekršaja koje se odvijaju putem računala ili nekog drugog oblika informacijskih sustava. Može se zaključiti kako je razumijevanje dva ključna pojma potrebni za razumjeti četiri koraka koja poduzimaju počinitelji kako bi neovlašteno stekli pristup nekog računalnog sustava. Jako je važno razumjeti svaki počiniteljev korak kako bi se educirali i stekli saznanja s ciljem sprečavanja računalnog kriminala. Moderna tehnologija sa sobom je osim mnogobrojnih prednosti donijela i velike rizike. Prvi napadačev korak su metode poput socijalnog inženjeringa, maskiranja, *spoofinga*, ispitivanja ili pogađanja, prisluškivanja, prerušavanja, druženja te kompromitiranja. U ovoj početnoj fazi napada može se zaključiti kako je važno identificirati računalni kriminal kako bi se spriječilo proširenje osnovnih metoda napada sa još preciznijim metodama. Napadači u pretposljednjem koraku manipuliraju podacima, koriste se napadima uskraćivanja usluga te koriste maliciozne programe. U posljednjem koraku uništavaju dokaze o svojim ilegalnim radnjama počinjenim na računalnom sustavu. Ono što se zaključuje temeljem teorijskog pregleda literature jest kako je važno razumijevanje metoda koje napadači koriste kako bi se na ispravan način mogla osigurati sigurnost i zaštita računalnog sustava. Osim toga, važno je konstanto usavršavanje i educiranje o vrsti, metodama i tehnikama napada jer se sa razvojem tehnologije razvijaju i metode napada te se pojavljuju nove koje nisu još dovoljno istražene. Iz primarnog istraživanja pokazuje se kako ispitanici nisu dovoljno informirani o rizicima računalnog kriminala i njegovim napadima, te se na tom području svakako treba educirati s ciljem smanjenja stope računalnog kriminala. U konačnici, informacije su u današnjici ključan resurs, a razvojem moderne tehnologije koja je donijela mnogobrojne prednosti razvio se i računalni kriminal. Zaštita i suzbijanje računalnog kriminala zahtijeva edukaciju o istome te postavljanje preventivnih sustava na računala. Čuvanje podataka od napadača je ključna stavka u cijelom procesu zaštite i suzbijanja te je iz tog razloga potrebno konstantno poboljšanje operativnih sustava te educiranje korisnika kako bi se smanjio računalni kriminal i podaci ostali zaštićeni.

LITERATURA

1. Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga* , 10(38), 113-132. *National Academy of Internal Affairs.*
2. Bača, M. (2004). Uvod u računalnu sigurnost. Zagreb: Narodne novine d.d.
3. Biloš, A. (2022). *Marketing informacijski sustavi.* [Online] Ekonomski fakultet u Osijeku. Dostupno na: https://moodle.srce.hr/2022-2023/pluginfile.php/7965801/mod_resource/content/1/mis2022-23-02-mis.pdf [Pristupljeno: 10. lipanj 2024]
4. Centar informacijskih sigurnosti (2011). *Nadzor rada sustava* Dostupno na: https://www.cis.hr/sigurnosni-alati/nadzor-rada-sustava.html [Pristupljeno: 10. lipnja 2024]
5. Cynet - Cybersecurity Platform (2020). *What Is Cobalt Strike and How Does It Work?* Dostupno na: https://www.cynet.com/network-attacks/cobalt-strike-white-hat-hacker-powerhouse-in-the-wrong-hands/ [Pristupljeno: 18. lipnja 2024]
6. Čutura, M. (2018). Marketing dionika: Prema boljem razumijevanju društvene odgovornosti marketinga. *Ekonomska misao i praksa*, 27(1), 141-156.
7. Dragičević, D. (1999). *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb: Informator
8. Easttom, C., Taylor, J., and Hurley, H. (2011). *Computer crime, investigation, and the law.*Boston, MA, USA: Course Technology.
9. Erbschloe, M. (2005). *Trojans, Worms and Spyware.*Burlingron, MA, SAD: Linacre House, fordan Hill, Oxford, UK.
10. European Commission, Directorate-General for Communication. (2020). Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime) [Data set]. http://data.europa.eu/88u/dataset/S2249_92_2_499_ENG
11. Gašić, D. (2022). Top Cyber Attacks In 2022. [Online] *Purplesec* Dostupno na: https://purplesec.us/security-insights/top-cyber-attacks-2022/ [Pristupljeno 13. srpnja 2024]
12. Gordon, S and Ford, R. (2006). On the Definition and Classification of Cyberrime. *Journal in Computer Virology,* 2(1); 13-20.
13. Harmon, R. (2003). Marketing information Systems. *Encyclopedia of Information,* 3, pp. 137-151. [Online] Portland State University. Dostupno na:

https://www.studocu.com/row/document/university-of-zimbabwe/marketing-communications-1/2003-marketing-information-systems-harmon/15704738 [Pristupljeno: 7. lipanj 2024].

14. Harmon, R. (2002). Marketing Information Systems. Encyclopedia of information systems, 3, 137-151.
15. Holm, H. (2014). A Large- Scale Study of the Time Required to Compromise a Computer System. *IEEE Transactions on Dependable and Secure Computing,* 11(1), 2-15.
16. Hrvatska enciklopedija, mrežno izdanje (2024). Dostupno: https://www.enciklopedija.hr/clanak/informacijski-sustav [Pristupljeno: 10.lipanj 2024]
17. Hudak, P. (2018). *Marketinški informacijski sustav u poduzeću Oprema d.d.* [Online] Sveučilište Jurja Dobrile u Puli Fakultet ekonomije i turizma „Dr. Mijo Mirković". Dostupno:https://repozitorij.unipu.hr/islandora/object/unipu%3A2620/datastream/PDF/view [Pristupljeno: 7.lipanj 2024]
18. Jakobsson, M. and Ramzan, Z. (2008). *Crimeware.* Boston, MA: Addison-Wesley
19. Jaiswal, M. (2017). Computer Viruses: Principles of Exertion, Occurrence and Awareness. *International Journal of Creative Research Thoughts,* 5(4), 648-651.
20. Kabay, M.E. (2008). Glossary of Computer Crime Terms. Norwich University.
21. Kamiš, A., Kukolj, S., Penjišević, A. i Sančanin,B. (2023). Defense in depth strategija zaštite protiv socijal inžinjeringa i phishing napada. *II. scientific meeting "balkan on Jahorina 2023" "development perspectives of the western balkans in the xxi century.*
22. Karabašić, L. (2017). *Kompjuterski ekonomski kriminal.* Sarajevo.
23. Khosrow-Pour, M. (2017). *Handbook of Research on Technology Adoption, Social Policy, and Global Integration.* Hershey PA, USA: IGI Global
24. Kondos G.,F., (1988). *Basic Considerations in Investigating and Proving Computer-Related Federal Crimes.* [Online] Washington,D.C.: U.S.Department of Justice. Dostupno na: https://www.ojp.gov/ncjrs/virtual-library/abstracts/basic-considerations-investigating-and-proving-computer-related [Pristupljeno 14.lipnja 2024]
25. Kotler P., Keller K. L. i Martinović M. (2014). *Upravljanje marketingom*. Zagreb: MATE d.o.o.
26. Lačić, L. (2016). *Marketinški informacijski sustavi.* Dostupno na: https://prezi.com/vogld49yb4hl/marketinski-informacijski-sustavi-mis/ [Pristupljeno: 13. lipanj 2024]

27. Laudon, K. C., & Laudon, J. P. (2004). Management information systems: Managing the digital firm. Pearson Educación
28. Matejkowski, D. (2023). Online identity theft detecton and prevention methods. [Online] *Advances in Web Development Journal*, 1(1), 10-11.
29. McGuire, M. and Dowling, S. (2013). *Cyber crime: A review of evidence*. Research Report 75, Chapter 1.
30. Milnsbridge, *4 Real World Consequences of Cyber Crime.* Dostupno na: https://www.milnsbridge.com.au/4-real-world-consequences-of-cyber-crime/ [Pristupljeno: 12. lipanj 2024]
31. Mishra, A., Alzoubi, Y. I., Gill, A. Q., and Anwar, M. J. (2022). Cybersecurity Enterpries Policies: A Comaprative Study. *Advances in Security and Reliability for Wireless Body Area Networks,* 22(2), 538.
32. Montesanp,J., J. (2019). The anti-forensics tactics, techniques, and procedures (ttps) cybercriminals use to hide electronic evidence of crimes. A Capstone Project Submitted to the Faculty of . Utica Collage.
33. Muncaster, P. (2022). *10 common security mistakes and how to avoid them.* Dostupno na: https://www.welivesecurity.com/2022/11/09/10-common-digital-security-mistakes-how-avoid/ [Pristupljeno: 12. lipanj 2024]
34. Phillips, K., C.Davidson, J., R.Farr, R., Burkhardt, C., Caneppele,S. and P.Aiken, M. (2022). Conceptualizing Cybercrime: Definitons, typologies and taxonomies.*Forensic Sciences,* 2(2), 379-398.
35. Ramakić, A., Bundalo, Z. (2013). Softversko-hardverska zaštita podataka u računarskim sistemima. Univerzitet u Bihaću; Univerzitet u Banjoj Luci.
36. Raićević, V., Matijašević- Obradović,J. i Ignjatijević, S. (2014) *Upotreba malicioznih programa kao pretnja na elektronskom poslovanju.* 3rd International Scientific Conference on „Power of Communication 2014“, Panevropski Univerzitet „Aperion“, Banja Luka.
37. Ružić, D. (2007). *Marketing u turističkom ugostiteljstvu*. Osijek: Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku
38. Ružić, D., Biloš, A. i Turkalj D. (2014). *E-marketing*. Osijek: Sveučilište Josipa Jurja Strossmayera, Ekonomski fakultet u Osijeku
39. Sabelli, M. (2022). *Security Serious Game* Dostupno na: https://webthesis.biblio.polito.it/25519/ [Pristupljeno: 21.lipnja 2024]

40. Salahdine, F., Kaabouch, N. (2019). Social Engineering Attacks: A Survey. . *School of Electrical Engineering and Computer Science, University of North Dakota*, 11(4), 89.
41. Samociuk, D. (2023). Antivirus Evasion Methods in Modern Operating Systems. *Institute of Informatics, Silesian Univesity of technology,* 13(8), 44-110.
42. Shah, D. Shah, V., Shah, H. and Kanani, P. (2017). Survey on Computer Worms. *International Journal on Recent and Innovation Trends in Computing and Communication*, 5(8),184-194.
43. Šimundić,S. i Franjić,S. (2009). *Računalni kriminalitet*. Split: Sveučilište u Splitu, Pravni fakultet
44. Šnicek,D. i Vrbanec, T. (2010). *Distribuirani napad uskraćivanjem usluga.* 354-358.
45. Sinha,K.,P. (2012). Distributed Operating Systems. New Delhi: PHI Learning.
46. Stouffer, C. (2023). Spyware: What it is and how to protect yourself. [Online] *Norton.* Dostupno na: https://us.norton.com/blog/malware/spyware [Pristupljeno: 15.srpnja 2024]
47. Sveučilište Minnesota Libraries Publishing. (2016). *Exploring Business*.
48. Težak, Đ. (2010). *Internet- POSLIJE ODUŠEVLJENJA*. Zagreb: Hrvatska Sveučilišna Naklada d.o.o.
49. Thomas, D. and Loader, B. (2000). *Cybercrime.* London: Routledge.
50. Vitolić, I. (2020). *Sigurnost MIS-a i računalni kriminal.* Osijek: Ekonomski fakultet u Osijeku. Dostupno na: https://repozitorij.efos.hr/islandora/object/efos:3589 [Pristupljeno: 5. lipnja 2024]
51. Varga, M. (2011). Zaštita elektroničkih podataka. *Technical Journal*, 5(1), 61-73. Tehnička škola Čakovec.
52. Vrbanus, S. (2023). 20 najčešćih lozinki hrvatskih korisnika u 2023. [Online] Bug.hr. Dostupno na: https://www.bug.hr/sigurnost/top-20-najcescih-lozinki-hrvatskih-korisnika-u-2023-manje-smo-neoprezni-nego-36597 [Pristupljeno 11. srpnja 2024]

POPIS SLIKA, GRAFIKONA I TABLICA

Popis slika:

Popis grafikona:

Popis tablica: