Kibernetička sigurnost, hakiranje i zaštita osobnih podataka na internetu

Lišnić, Laura

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Humanities and Social Sciences / Sveučilište Josipa Jurja Strossmayera u Osijeku, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:142:097296

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet Osijek

Dvopredmetni diplomski studij nakladništva i informacijske tehnologije

---

Laura Lišnić

Kibernetička sigurnost, hakiranje i zaštita osobnih podataka na internetu

Diplomski rad

Mentor: prof. dr. sc. Boris Badurina

Osijek, 2024.

Sveučilište J. J. Strossmayera u Osijeku

Filozofski fakultet

Odsjek za informacijske znanosti

Dvopredmetni diplomski studij nakladništva i informacijske tehnologije

---

Laura Lišnić

Kibernetička sigurnost, hakiranje i zaštita osobnih podataka na internetu

Diplomski rad

Društvene znanosti, Informacijske i komunikacijske znanosti

Mentor: prof. dr. sc. Boris Badurina

Osijek, 2024.

Prilog: Izjava o akademskoj čestitosti i o suglasnosti za javno objavljivanje

Obveza je studenta da donju Izjavu vlastoručno potpiše i umetne kao treću stranicu završnog odnosno diplomskog rada.

IZJAVA

Izjavljujem s punom materijalnom i moralnom odgovornošću da sam ovaj rad samostalno napravio te da u njemu nema kopiranih ili prepisanih dijelova teksta tuđih radova, a da nisu označeni kao citati s napisanim izvorom odakle su preneseni.
Svojim vlastoručnim potpisom potvrđujem da sam suglasan da Filozofski fakultet Osijek trajno pohrani i javno objavi ovaj moj rad u internetskoj bazi završnih i diplomskih radova knjižnice Filozofskog fakulteta Osijek, knjižnice Sveučilišta Josipa Jurja Strossmayera u Osijeku i Nacionalne i sveučilišne knjižnice u Zagrebu.

U Osijeku, 10. siječnja 2024.

Laura Lišnić, 0122229022

ime i prezime studenta, JMBAG

Sažetak

Diplomski rad opisuje srž kibernetičke sigurnosti te navodi potencijalne prijetnje koje se mogu zateći u kibernetičkom okruženju (virusi i drugi zlonamjerni softveri). Također se osvrće na OWASP metode i pojam hakiranja te razne načine hakiranja u slučaju neopreznog korištenja interneta i dijeljenja osobnih podataka. Budući da javnost generalno hakere svrstava u lošu skupinu, u radu su predstavljeni i hakeri kojima nije cilj na bilo koji način profitirati na tuđu štetu, tzv. *white-hat* hakeri, ali i oni koji se nalaze na samoj sredini. Neki od napada koji se opisuju u radu su *Man-in-the-middle* (najčešći), *Evil twin*, *Slowloris* i DDoS pri čemu su svi napadi povezani uz mrežno okruženje i važni za zaštitu mrežnih stranica, no *Evil twin* se više temelji na krađi podataka, po kojoj se posebno i ističe. Opisani su i načini kako se zaštititi od navedenih napada te koje se sve mjere trebaju poduzeti kako bi i najmlađi znali prepoznati opasnost, a neki od mjera koje je potrebno poduzeti tiču se korištenja provjerenih internetskih mreža, pogotovo ako se radi o bankovnim transakcijama. U slučaju neopreznog dijeljenja osobnih podataka od strane korisnika isti mogu lako doći u neželjene ruke. U drugom dijelu rada predstavljeni su rezultati istraživanja na 101 ispitaniku koji su željeli istražiti internetske navike studenata te njihova upućenost u potencijalne prijetnje u internetskom okruženju.

Ključne riječi: kibernetička sigurnost, hakiranje, zaštita podataka, internet, OWASP

Sadržaj

1. Uvod

Kibernetička sigurnost danas se usko povezuje s hakerima koji tu sigurnost i narušavaju. Većina ljudi čula je za hakere, ali se velik broj ljudi s hakerima i susreo te snosio posljedice njihovih radnji. Postavlja se pitanje tko su zapravo hakeri te zašto je uopće potrebno biti informiran o njima? Hakerima se smatraju osobe koje vole mijenjati značajke softvera ili elektroničkih sustava, najčešće s ciljem zaobilaženja sigurnosnih sustava. Iste osobe vole istraživati o računalima te učiti kako računalni sustav zapravo funkcionira. Očarani su otkrivanjem novih načina rada računala – vezano i uz mehaničke i uz elektroničke dijelove. Ipak, u zadnje vrijeme hakeri su dobili novo značenje. Smatraju se osobama koje zlonamjerno provaljuju u sustave u svrhu osobne dobiti. Također se nazivaju i *crackers (criminal hackers)*, odnosno kriminalnim hakerima koji provaljuju *(crack)* u sustave sa zlobnim namjerama. Ciljevi koji ih motiviraju su vezani uz osobnu dobit te uključuju slavu, profit ili osvetu, a ono što zapravo čine je izmjena, brisanje i krađa kritičnih informacija što za posljedicu napadnute ljude, žrtve hakiranja, čini nesretnima. Postoji nekoliko kategorija u koje se hakeri mogu svrstati, a najpoznatije su tzv. *white-hat* i *black-hat* hakeri. *White-hat* hakeri predstavljaju dobre hakere koji se ne vole svrstavati u istu košaricu sa zlima *(black-hat)*. Zanimljivo je kako su nazive dobili na temelju *westerna* u kojima su dobri likovi uvijek nosili bijele kaubojske šešire, dok su zlikovci uvijek nosili crne. Osim navedene dvije kategorije, postoji i kategorija *gray-hat* hakera koji se smatraju članovima pomalo od svake kategorije. Međutim, u većini slučajeva ljudi su skloni hakere opisivati isključivo u negativnoj konotaciji, a zanimljivo je kako velik broj zlonamjernih hakera tvrdi kako oni zapravo nikome ne nanose štetu, već ljudima pomažu na nesebičan način. Tvrdnje tog tipa nikako nisu točne te hakeri nanose ogromnu štetu, pri čemu se još nazivaju i elektroničkim lopovima.[1] Kako bi se zaštitili, važno je da ljudi razviju određene kompetencije koje će im pomoći kod zaštite računala i osobnih podataka u svakodnevici, a kako bi to bilo moguće, potrebno je upoznati se s računalom, njegovim dijelovima i načinom na koji računalo i ostali elektronički mediji funkcioniraju. Posebno je važno razvijati potrebne kompetencije još od malih nogu kako djeca i mladi prilikom susretanja s elektroničkim medijima ne bi nehotice podijelili osobne podatke na nesigurnim stranicama koje im te iste podatke žele ukrasti ili koje im žele nametnuti razne viruse koji bi doveli do usporavanja rada računala i elektroničkih medija.

[1] Usp. Beaver, Kevin. Hacking For Dummies. 2nd edition. Indianapolis: Wiley Publishing, Inc., 2007. Str. 9-11.

2. Definiranje kibernetičke sigurnosti

Kibernetička sigurnost široko je korišten pojam koji se opisuje vrlo promjenjivim definicijama koje često znaju biti subjektivne. Činjenica da ne postoji sažeta i široko prihvatljiva definicija otežava tehnološke i znanstvene napretke, pogotovo zato što bi kibernetička sigurnost trebala djelovati usklađeno s drugim disciplinama, a ne se odvajati od njih. Sam pojam „kibernetičke sigurnosti" predmet je mnogih akademskih istraživanja i popularne književnosti koja na temu gleda iz vlastite perspektive što dovodi do raznih subjektivnih i neinformativnih definicija koje su često vezane uz kontekst. Fredrick Chang, bivši direktor istraživanja u NSA (*National Security Agency*) u Sjedinjenim Američkim Državama 2012. godine raspravljao je o temi te naveo problem kako znanost o kibernetičkoj sigurnosti nudi mnoge mogućnosti za daljnje napredovanje, no ipak ljudi moraju neprestano braniti strojeve koje, uz pomoć strojeva, napadaju drugi ljudi. Kako bi se slične radnje spriječile, grupa informatičara, inženjera, psihologa i sociologa pokušala je razviti definiciju koja će obuhvatiti sve potrebne čimbenike i time pomoći u napredovanju tehnologije. Jedan od znanstvenika primijetio je kako oko područja kibernetičke sigurnosti postoji nekoliko isprepletenih diskursa te kako bi najbolje bilo rekonstruirati pojam i podijeliti ga na dvije domene: kibernetičko i sigurnost.[2]

Kibernetičko je prefiks koji označava kibernetički prostor (*cyberspace*) te se odnosi na elektroničke komunikacijske mreže i virtualnu stvarnost, a razvio se iz pojma „kibernetika" koji se odnosio na područje teorije kontrole i komunikacije, bilo to vezanu uz stroj ili uz životinje. Pojam „kibernetički prostor" (*cyberspace*) postao je popularan 1984. kada je izašao roman „Neuromancer" autora Williama Gibsona, a u kojemu autor opisuje svoju viziju trodimenzionalnog prostora koji je ispunjen čistim informacijama koje se kreću od računala do računala gdje su, pritom, ljudi generatori i korisnici informacija. Danas pojam kibernetičkog prostora poznajemo kao okoliš informacija, a *Public Safety Canada* definira ga kao elektronički svijet koji je stvoren međusobno povezanim mrežama informacijske tehnologije i informacija na tim mrežama. *Public Safety Canada* navedeni pojam opisuje kao „globalno dobro" u kojem su ljudi povezani kako bi razmjenjivali ideje, usluge i prijateljstva. Kibernetički prostor ne

[2] Usp. Craigen, Dan; Diakun-Thibault, Nadia; Purse, Randy. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): str. 13-17. URL: http://doi.org/10.22215/timreview/835 (2023-07-02)

smatraju statičnim, već dinamičnim, evoluirajućim i višerazinskim ekosustavom fizičke infrastrukture, softvera, propisa, ideja, inovacija i interakcije pod utjecajem sve veće populacije suradnika koji predstavljaju raspon ljudskih namjera.[3]

Pojam sigurnosti, s druge strane, izrazito je teško definirati u općem smislu te se ne smatra široko prihvaćenim konceptom. Iako postoje konkretniji oblici sigurnosti (fizička svojstva, ljudska svojstva ili svojstva informacijskog sustava – matematiče definicije) pojam preuzima značenje na temelju nečije perspektive i onoga što cijenimo. Središnji opis mogao bi se raspisati kao „slobodan od opasnosti ili prijetnje“.[4]

Nakon razdvajanja pojma kibernetičke sigurnosti u dijelove, odabrano je nekoliko definicija:

- „Kibernetička sigurnost uglavnom se sastoji od obrambenih metoda koje se koriste za otkrivanje i sprječavanje potencijalnih uljeza.“ (Kemmerer, 2003.)
- „Kibernetička sigurnost podrazumijeva zaštitu računalnih mreža i informacija koje one sadrže od prodora i od zlonamjernog oštećenja ili poremećaja.“ (Lewis, 2006.)
- „Kibernetička sigurnost uključuje smanjenje rizika od zlonamjernih napada na softver, računala i mreže. Ovo uključuje alate koji se koriste za otkrivanje provala, zaustavljanje virusa, blokiranje zlonamjernih pristupa, nametanje autentifikacije, omogućivanje šifrirane komunikacije itd.“ (Amoroso, 2006.)
- „Kibernetička sigurnost je skup alata, politika, sigurnosnih koncepata, sigurnosnih mjera zaštite, smjernica, rizika pristupa upravljanju, akcije, obuka, najboljih praksi, osiguranja i tehnologija koje se mogu koristiti za zaštitu kibernetičkog okruženja i organizacije i korisničkih sredstava.“ (ITU, 2009.)
- „Sposobnost zaštite ili obrane korištenja kibernetičkog prostora od kibernetičkih napada.“ (CNSS, 2010.)[5]

Osim prikazanih definicija, navedene su još neke, no prethodnih pet definicija daje jasan uvid u širinu pojma te prikazuje srž koju pojam kibernetičke sigurnosti predstavlja. Iako definicije pomažu, autori Craigen, Diakun-Thibault i Purse u svome ih radu „Defining Cybersecurity. Technology Innovation Management Review“ opisuju holistički neutemeljenima. Definicija treba biti objektivnija te se temeljiti na nečemu poput „sustava za otkrivanje napada“, a ne se

[3] Isto.

[4] Isto.

[5] Isto.

temeljiti na pretpostavki kao što su „namjere hakera“. Ipak, postoji pet dominantnih dijelova od kojih se kibernetička sigurnost sastoji, a to su: tehnološka rješenja; događanja; strategije, procesi i metode; ljudski angažman; referentni objekti (sigurnosti). Navedeni pojmovi odgovorni su za pomoć u pružanju kritičkog konteksta u procesu definiranja pojma. Nasuprot tomu, mogu se uvidjeti i neke razlike, a to su: interdisciplinarni socio-tehnički karakter; biti mreža bez razmjera – u kojoj su mogućnosti mrežni akteri potencijalno slični; visoki stupnjevi promjene, povezanosti i brzine interakcija.[6]

Kada su se sve navedene informacije uzele u obzir, znanstvenici su razvili definiciju koja bi mogla obuhvatiti sve potrebne aspekte, a koja glasi: „Kibernetička sigurnost je organizacija i prikupljanje resursa, procesa i struktura koje se koriste za zaštitu kibernetičkog prostora i sustava omogućenih kibernetičkim prostorom od pojava koji ne usklađuju de iure od de facto vlasništva prava.“[7] Definicija je razdvojena po dijelovima gdje prvi dio opisuje interakciju između ljudi, sustava i između ljudi i sustava, drugi dio opisuje zaštitu od svih prijetnji (namjernih, slučajnih i prirodnih i nepredvidivih), a treći dio opisuje bilo koji događaj ili aktivnost koja ne usklađuje stvarnu (de facto) imovinu prava iz percipiranih (de jure) imovinskih prava, bilo namjerno ili slučajno, poznato ili nepoznato).[8]

[6] Isto.

[7] Isto.

[8] Isto.

3. Prijetnje u kibernetičkoj sigurnosti

Eksponencijalni rast internetskih međupovezanosti doveo je do značajnog porasta incidenata kibernetičkih napada koji su za sobom često ostavljali teške posljedice. Takva vrsta napada često je primarni izbor oružja za izvršavanje zlonamjernih namjera. Kao društvo postali smo uveliko ovisni o računalnim mrežama i rješenjima informacijske tehnologije. Kibernetički napadi također postaju privlačniji. Istraživanja pokazuju kako SAD godišnje potroši 114 bilijuna dolara svake godine kako bi se riješio problema kibernetičkih napada, a kada bi se u cijenu uračunalo i vrijeme koje tvrtke ulože kako bi se oporavile od napada, cifra raste sve do 385 milijardi američkih dolara.[9] U 24 američke zemlje, 69% ih je prijavilo da su bili žrtve kibernetičkog napada tijekom svog života. Čak su provedeni izračuni koji govore da se svake sekunde odvija 14 različitih napada, odnosno više od milijun kibernetičkih napada svaki dan. Postavlja se pitanje zašto su kibernetički napadi toliko česti. Zato što su jeftiniji, praktičniji i manje rizični od fizičkih napada. Zahtijevaju samo računalo i internetsku vezu, a nisu ograničeni geografijom i fizičkom udaljenošću. Kibernetička se sigurnost odnosi na razumijevanje okolnih problema različitih kibernetičkih napada i osmišljavanje obrambenih strategija (protumjera) koje čuvaju povjerljivost, integritet i dostupnost bilo koje digitalne i informacijske tehnologije. Povjerljivost se odnosi na sprječavanje otkrivanja informacija neovlaštenim sustavima ili osobama, integritet se odnosi na sprječavanje bilo kakve izmjene/brisanja na neovlašteni način, a dostupnost se odnosi na osiguravanje sustava odgovornih za isporuku, pohranjivanje i obradu informacija te da navedeni sustavi budu dostupni kada su potrebni i od strane onih kojima su potrebni.[10]

Stručnjaci za kibernetičku sigurnost vjeruju kako je zlonamjerni softver (*malware*) ključan izbor oružja za izvođenje zlonamjerne aktivnosti koja bi narušila napore kibernetičke sigurnosti u kibernetičkom prostoru. Kada se govori o zlonamjernom softveru, misli se na napade koji se učitavaju u sustav bez znanja vlasnika kako bi kompromitirali sustav u korist protivnika, a neki od primjera zlonamjernih softvera uključuju viruse, crve, trojanske konje, *spyware* i izvršne datoteke robota. Uloga je zlonamjernog sustava inficirati sustave na razne načine poput širenja

[9] Usp. Jang-Jaccard, Julian; Nepal, Surya. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80, br. 5 (2014.): str. 973-974.

[10] Isto.

sa zaraženih strojeva, prevare korisnika, navođenja korisnika da posjete web stranice za širenje zlonamjernog softvera koji, također, može sam sebe učitati u USB pogon koji je umetnut u zaraženi uređaj te na taj način zaraziti svaki drugi sustav koji se naknadno priključi na taj uređaj. Većina obrambenih mehanizama koristi vatrozid i antivirusni softver koji mora biti instaliran unutar sustava za prevenciju i detekciju napada. Uz njihovu pomoć, svaki se promet koji dolazi izvana presreće i ispituje kako bi se osigurala sigurnost i kako zlonamjerni softver ne bi uspio prodrijeti u unutrašnjost. S druge strane, zlonamjerni softveri neprestano se razvijaju te često uspijevaju pronaći nedostatke kako bi se provukli u softver i zaobišli obranu, pogotovo ako se radi o novim tehnologijama koje još nisu uspjele pokriti sve propuste. Najveća zabrinutost odražava se na kritičnim infrastrukturama pod kojima se nalaze električne mreže i zdravstveni sustavi, a koji bi kao meta mogli poslužiti za terorizam, sabotažu i informacijski rat. Još jedna zanimljiva činjenica govori kako su društveni mediji (stranice društvenih mreža i blogovi) jako zanimljiva meta napadačima. Budući da ljudi svakodnevno opisuju svoje dnevne i životne događaje te sklapaju nova poznanstva i prijateljstva, napadačima je vrlo lako doći do korisnika koji će kliknuti na poveznicu i na taj način instalirati virus na svoje računalo ili neki drugi uređaj.[11]

3.1. Prijetnje u Facebook okruženju

Zlouporaba podataka potencijalno je štetna za razvoj adolescenata u zadatcima koji uključuju autonomiju, izgradnju identiteta, intimnosti i seksualnosti. Također, mala je vjerojatnost da će djeca sama prijaviti zlostavljanje na internetu iz straha da će im uređaji koji im služe za boravak na internetu biti zaplijenjeni.[12] Značajke kibernetičkog zlostavljanja kao što su širenje glasina, ogovaranje, isključivanje i napadi na ugled odnose se na uobičajene oblike internetskog nasilja, dok se seksualizirano internetsko zlostavljanje i klevetničke stranice odnose na to kako se nečija slika percipira na društvenim mrežama, što utječe na negativne promjere načina na koji se žrtva doživljava. Seksualizirano internetsko zlostavljanje koristi informacije žrtve na štetan način bez prethodnog pristanka te je već naznačeno kako ono utječe na oblikovanje seksualnog identiteta djevojčica. S druge strane, adolescenti muškoga spola bodre se prilikom objavljivanja fotografija bez majice te se u toj razlici može primijetiti kako internet pravi veliku razliku pri

[11] Isto.

[12] Barbovschi, Monica; Velicu, Anca. „“Fraped“ Selves: Hacked, Tagged and Shared Without Permission. The Challenges of Identity Development for Young People on Facebook.“ (2015.)

oblikovanju identiteta djevojčica i dječaka.[13] Osim problema u razvoju identiteta, kibernetičko zlostavljanje može utjecati i na depresiju, nisko samopouzdanje, tjeskobu, suicidalne ideje te psihosomatske probleme poput glavobolje i poremećaja spavanja. *Fraping* je internetski *slang* za pojednica koji napušta svoj Facebook profil prijavljen i bez nadzora, čime svoj profil izlaže riziku zlouporabe druge osobe. Izraz je nastao od kombinacije riječi *Facebook* i *rape* (silovanje), a odnosi se na zlouporabu slike korisnika na način da se stvaraju klevetničke lažne stranice.[14]

Adolescenti su često podložni potrebi za prihvaćanjem od strane vršnjaka te zbog toga velik dio vremena provode na društvenim mrežama uređujući svoje profile, prateći objave koje drugi postavljaju te označavajući objave tzv. lajkovima koji se na Facebooku koristi kao oblik društvene valute. Još neke od radnji kojima se bave su komentiranje objava te označavanje sebe i vršnjaka na fotografijama i videozapisima, a sve samo kako bi bili viđeni i prepoznati među vršnjacima. *Facebook* prijatelji međusobno objavljuju jedni drugima na profilima, označavaju se na objavama i označuju objave s oznakama „sviđa mi se“ na dnevnoj bazi, no kao što postoje i performansi Marine Abramović u kojima publika ima veliku moć pri određivanju ishoda, tako postoji i opasnost publike koja zlorabi moć koju ima na društvenim mrežama. Neki od primjera zlouporabe su hakiranje profila te označavanje i objavljivanje bez dopuštenja.[15] Privatnost je jedna od ključnih potreba pojedinca u internetskom okruženju jer je prilikom objavljivanja velike količine informacija prisutan osjećaj ranjivosti koju pojedinac doživljava. Zanimljivo je kako adolescenti smatraju čudnim sprijateljiti se s roditeljima i drugim odraslim osobama, misleći kako se odrasle osobe time upliću u njihovu privatnost i društveni život, no i dalje imaju veliku potrebu za kontrolom dojma drugih vršnjaka o sebi. Time se mogu uvidjeti potencijalne razlike adolescenata i odraslih u shvaćanju i percepciji pojma privatnosti.[16]

Još jedan od problema internetskog okruženja je lažno predstavljanje putem hakiranja i lažnih računa te javnog sramoćenja i ponižavanja klevetama te prosljeđivanje golišavih slika kao jedan od najtežih oblika internetskog zlostavljanja. Zbog toga bi korisnici trebali imati zaključane profile i namještene postavke privatnosti tako da im samo prijatelji mogu vidjeti profil. Još jedna od mogućnosti je i ograničavanje pristupa za određene korisnike koji su *Facebook* prijatelji, ali su skloni uznemiravanju i zlostavljanju na društvenim mrežama. Na

[13] Isto.

[14] Isto.

[15] Isto.

[16] Isto.

primjer, imaju naviku označavati određene osobe i dijeliti njihove objave bez dozvole. Hakirani profili također mogu predstavljati problem jer se često koriste za slanje nepristojnih poruka ostalim vršnjacima u ime osobe koja je hakirana. Kontrola nad svojim okruženjem nužna je za održavanje samopoštovanja koje je sastavni dio osobnog identiteta i zato je potrebno biti pažljiv prilikom odabira *Facebook* prijatelja ili pratitelja na nekim drugim mrežama te poduzeti sve mjere zaštite profila kako ne bi mogao biti iskorišten u zlonamjerne svrhe.[17]

[17] Isto.

4. Povijest zlonamjernog softvera

U početcima je zlonamjerni softver (*malware*) bio napisan kao eksperiment čija je uloga bila istaknuti sigurnosne ranjivosti ili kako bi širina tehničkih mogućnosti došla do izražaja. Danas se koristi u sasvim drugačije svrhe, gdje mu je primarna misija krađa osjetljivih osobnih, financijskih ili poslovnih podataka za dobrobit drugih. Mete su mu često vlada ili poduzeća te web stranice za prikupljanje čuvanih informacija. Glavne stavke koje softver želi izmijeniti su osobni podatci i brojevi kreditnih kartica. Također, softver je dizajniran u svrhu preuzimanja kontrole nad računalima raznih korisnika koja bi poslužila za iskorištavanje crnog tržišta. Proces bi se odvijao slanjem neželjene e-pošte ili praćenjem ponašanja korisnika prilikom pretraživanja interneta, odnosno prikazivanjem neželjenih reklama. Životni tijek softvera odvija se najčešće u tri koraka: neželjena pošta → krađa identiteta → preuzimanje s interneta. Nekoliko naziva nalazi se iza navedenih radnji.[18]

Spam (neželjena elektronička pošta) – odnosi se na slanje nerelevantnih, neželjenih i neprikladnih poruka tisućama ili čak milijunima primatelja. Ovaj način pokazao se kao vrlo profitabilan ključ na tržištu, a tomu doprinosi činjenica da se neželjena pošta šalje anonimno i bez troškova za pošiljatelja. Zbog toga je *spam* izrazito raširen. Stručnjaci su izračunali kako je 88-92 % ukupnog broja poslanih poruka e-poštom u 2010. godini zapravo bila neželjena pošta.[19]

Phishing (mrežna krađa identiteta) – predstavlja način pokušaja nabavljanja osjetljivih informacija kao što su korisničko ime i lozinka ili podatci koji se tiču kreditne kartice. Način na koji se krađa odvija sastoji se od obmanjivanja korisnika da posjete određenu stranicu, dok se u isto vrijeme predstavljaju kao zakonita agencija ili tvrtka, najčešće banka. Korisnici često nasjednu na trik jer ne provjeravaju URL stranice, a tamo se krije pogreška uz čiju pomoć mogu prepoznati da se radi o prevari. Također upotrebljavaju poddomene kako bi izbjegli korištenje prepoznatljivog IP-a.[20]

Drive-by Downloads – nenamjerno preuzimanje zlonamjernog softvera, to jest način kojim se napadači sve više služe kako bi što brže proširili zlonamjerni softver. Ovaj način narušavanja

[18] Isto. str. 975.

[19] Isto. str. 976.

[20] Isto.

sigurnosti odvija se dok korisnik posjećuje određena web mjesta, dok provjerava e-poštu ili u trenutku kada korisnik klikne na skočni prozor. Najčešće se napad odvija za vrijeme posjećivanja web stranica. Korisnik dobije neželjenu poštu u kojoj se nalaze poveznice (URL adrese) na određenu web stranicu. U trenutku kada korisnik posjeti tu stranicu, softver se krene preuzimati na uređaj bez znanja korisnika.[21]

4.1. Hardware (sklopovlje) i software (programska podrška)

Hardware posjeduje najveću sposobnost manipulacije računalnim sustavom. Ako je ugrožen, napadačima daje ogromnu moć pokretanja zlonamjernih sigurnosnih napada. Jedna od najčešćih vrsta hardverskog iskorištavanja je hardverski trojanski konj. Osim što ima moć umetanja pogrešaka tako da unos bude odbijen i što može umetati međuspremnike čipova u druge međuspremnike kako bi se baterija ispraznila brže zbog manjka energije, u ozbiljnim slučajevima sposoban je spriječiti rad neke funkcije ili resursa. Također ima mogućnost fizički uništiti, onesposobiti ili promijeniti uređaj na način da procesor potpuno zanemari prekid određene periferije.[22]

Do iskorištavanja softvera dolazi onda kada se iskoriste određene značajke njegovog paketa ili sučelja. Najčešće ranjivosti softvera temelje se na iskorištavanju softverskih grešaka u memoriji, validaciji korisničkog unosa te korisničkih privilegija pristupa. Napadačima je krajnji cilj povrijediti sigurnost memorije kako bi izmijenili njezin sadržaj. To se odvija uz pomoć tehnike prelijevanja međuspremnika koje se događa kada program pokuša pohraniti više podataka međuspremnika nego što je namjeravao zadržati. Kako su međuspremnici stvoreni za pohranu određene količine podataka, tako se svaka dodatna informacija može „preliti“ u neki drugi međuspremnik, pritom oštećujući valjane podatke koje međuspremnik sadrži. Budući da ta metoda omogućuje napadačima da izmjenjuju procesni kod, narušena je i provjera valjanosti unosa čija je primarna zadaća osigurati da uneseni podatci slijede određena pravila. Netočna provjera valjanosti vodi prema oštećenju podataka, kao u slučaju SQL injekcije (*SQL injection*) koja spada u jedne od najpoznatijih tehnika koja iskorištava „*bug*“ u softveru web stranice. Napadač upisuje SQL naredbe kako bi izmijenio sadržaj.[23]

[21] Isto.

[22] Isto. str. 977.

[23] Isto. str. 977.-978.

4.2. Pametni telefoni

Pametni su telefoni svakodnevno korišteni medij koji u sebi sadrži razne privatne i poslovne informacije. Sastoje se od nekoliko karakteristika, a prva i najvažnija je upravo mobilnost. Činjenica da su lako prenosivi sama po sebi objašnjava koliko su lake mete za krađu, a druga opasnost je to da mogu lako biti izgubljeni. Zatim imamo snažnu personalizaciju, što se odnosi na to da mobilne uređaje uglavnom ne dijelimo, već ih koristimo zasebno. Snažna povezanost kao sljedeća karakteristika odnosi se na to kako je njihova primarna svrha upravo povezivanje s drugim uređajima kako bi se razmijenili određeni podatci. Konvergencija tehnologije objašnjava kako su brojne funkcionalne značajke već integrirane u uređaje, a odnosi se na igrice, dijeljenje podataka i pretraživanje interneta. Naposlijetku, postoji karakteristika vezana uz ograničene resurse i smanjene mogućnosti te se navode glavna četiri ograničenja, a to su: trajanje baterije, snaga, mala veličina zaslona i male tipke za unos. Sva navedena ograničenja postavljaju izazov u izgradnji sigurnosne mreže. Jedan od načina na koji hakeri mogu doći do osjetljivih podataka je putem prisluškivanja Wi-Fi komunikacije pri čemu može doći do korisničkog imena i lozinke određene osobe.[24]

Ipak, neki od najvećih problema ugrožene kibernetičke sigurnosti tiču se terorizma, sabotaže, informacijskog rata i prirodnih nepogoda (uragan) koje imaju velik utjecaj na oštećenje kritičnih infrastruktura, koje tada postaju laka meta za napadače.[25]

[24] Isto. str. 983.

[25] Isto. str. 984.

5. Računalstvo u oblaku

Jedno od zanimljivijih mjesta za pohranjivanja podataka svih vrsta upravo je oblak (npr. *Dropbox*), a razlog tome je što korisnici za pohranjivanje podataka koriste najčešće Google-ove usluge u oblaku kako bi što lakše mogli pratiti svoja događanja. Prednost je što računalstvu u oblaku pruža jedinstvene karakteristike koje se razlikuju od svih tradicionalnih pristupa. Ključne karakteristike odnose se na: samoposluživanje na zahtjev, sveprisutni mrežni pristup, udruživanje resursa neovisno o lokaciji, brzu elastičnost i odmjerenu uslugu. Sve navedene karakteristike nužne su za transparentno i besprijekorno korištenje oblaka. Također, računalstvu u oblaku služi i za isporuku različitih resursa klijentima na raznim slojevima sustava, pritom koristeći različite resurse. Cijela arhitektura može se podijeliti na nekoliko slojeva: sloj hardvera (s podatkovnim centrima), infrastrukture, platforme i aplikacije.[26]

Sloj hardvera odgovoran je za upravljanje fizičkim resursima u oblaku, a to uključuje fizičke poslužitelje, sklopke, sustave za napajanje i hlađenje te usmjerivače. Sloj se najčešće implementira u podatkovne centre, a neki od tipičnih problema uključuju otpornost na pogreške, upravljanje prometom i resursima za napajanje i hlađenje. Infrastrukturni sloj stvara skup resursa za pohranu dijeljenjem fizičkih resursa, pritom koristeći tehnologije virtualizacije. Sloj platforme izgrađen je na sloju infrastrukture, a sastoji se od operativnih sustava i platformi aplikacija. Svrha mu je smanjiti teret postavljanja aplikacija izravno u spremnike „virtualne mašine“. Zadnji sloj, sloj aplikacije sastoji se od stvarnih aplikacija u oblaku što ga postavlja na sam vrh hijerarhije. Prednost aplikacija u oblaku nad običnim aplikacijama je što mogu postići bolje performanse uz manje troškove.[27]

[26] Isto. str. 981.

[27] Isto str. 981.-982.

6. Kibernetička sigurnost kod mladih

Kanadski centar za digitalnu pismenost opisuje problematiku kibernetičke sigurnosti tinejdžera na način da se adolescenti često služe internetom na sličan način kako i njihovi roditelji te druge odrasle osobe. Međutim, nerijetko se mladi povode za rizičnim ponašanjem te preuzimaju sumnjive aplikacije, piratsku glazbu i filmove. Osim preuzimanja, često su izloženi rizicima vezanim uz društvene mreže kojima se najčešće koriste, a koje sa sobom nose brojne opasnosti poput stvaranja kontakta s lažnim, krivotvorenim profilima kreiranima u svrhu manipulacije drugima. Ono što je mladima potrebno objasniti je kako zaštititi svoje profile koristeći se jakim lozinkama koje neće dijeliti s drugima te ih savjetovati da svoje uređaje uvijek zaključavaju PIN kodovima (ili na neki drugi način). Također, valjalo bi ih uputiti na to da nikada ne objavljuju svoje puno ime, cijeli datum rođenja ili druge osjetljive informacije koje bi se kasnije mogle upotrijebiti na lažnim profilima. Mladima bi trebalo objasniti koje su sve opasnosti piratskog preuzimanja glazbe, filmova i aplikacija te ih upozoriti kako se na taj način mogu preuzeti i razni virusi, odnosno brojni zlonamjerni softveri te bi sadržaj uvijek trebali preuzimati s legitimnih, službenih stranica, odnosno službenih trgovina za preuzimanje aplikacija. Prilikom kupovine preko interneta, mladi bi trebali biti upozoreni da uvijek provjeravaju ponude koje dobivaju kako bi spriječili potencijalnu mogućnost krađe podataka ili prevare dobavljača koji se često služe *eBay* i *Amazon* platformama. Osim navedenoga, bilo bi poželjno uputiti ih da za vrijeme kupnje koriste način privatnog pregledavanja i da nikada ne dopuštaju web stranicama da pohranjuju podatke o njihovim karticama te da uvijek istraže stranice na kojima kupuju i ostavljaju svoje osobne podatke. Istraživanje je vrlo bitno kako se ne bi dogodilo da na proizvodu piše jedna cijena, ali su izostavljeni podatci o porezu, dostavi i slično. Zbog toga je važno uvijek detaljno provjeriti košaricu prije nego se krene s konačnim plaćanjem. Konačno, vrlo je važno čuvati svu e-poštu i račune ukoliko dođe do nekih problema, a to se može učiniti na jednostavan način tako da korisnici naprave snimku zaslona.

6.1. Nužnost obrazovanja o kibernetičkoj sigurnosti u školama

Mnogi korisnici društvene mreže koriste kao platforme za izražavanje vlastitih mišljenja, osjećaja ili kako bi izazivali rasprave te postali poznati na internetu. Velik broj korisnika želi biti prvi na internetu koji će podijeliti određeni problem ili misao, no često zanemaruju jesu li prezentirane informacije autentične ili ne. Korištenje interneta i znanje o kibernetičkoj

sigurnosti ne bi trebalo biti ograničeno samo na odrasle ljude, već i na djecu koja uvelike koriste društvene mreže i internet. Internet se danas koristi za sve te ima ogroman potencijal za učenje, no prečesto korištenje interneta može dovesti do niza štetnih ishoda kao što su tzv. *cyber* ovisnost, ovisnost o igricama i kockanju, pornografija te izloženost osobnim informacijama.[28] Kibernetički kriminal koji se vrši nad djecom i maloljetnicima velik je problem s kojima se roditelji često ne suočavaju na pravi način zbog toga što ne shvaćaju da je njihovo dijete žrtva takve vrste kriminala. Jedan od razloga zašto je tako je upravo to što roditelji često nisu svjesni što njihovo dijete radi u kibernetičkom okruženju. Djeca mogu biti maltretirana putem komentara i vrijeđanja, mogu biti uznemirivani ili zastrašivani te seksualno iskorištavani. Statistike Kraljevske malezijske policije pokazuju da gotovo 80% slučajeva silovanja koji su u razdoblju od dvije godine (2018.-2020.) prijavljeni u cijeloj zemlji, uključuju prijateljstva u virtualnom svijetu, a navodi se da je većina žrtava mlađa od 18 godina. Seksualno zlostavljanje se pogoršava upravo zbog toga što je na internetu sve više seksualnih predatora koji tražeći žrtve koriste lažne identitete.[29]

Ipak, nema sumnje da su djeca i mladi prilično vješti u korištenju interneta i tehnologije, no svakako ih treba uputiti na potencijalne rizike koje korištenje istih donosi sa sobom, pogotovo zato što im djeca danas imaju sve raniji pristup. Nastavnici bi trebali biti ti koji će ih uputiti na kibernetičku sigurnost i koji će promicati odgovorno ponašanje na internetu. Škola bi trebala provoditi nastavu kritičkog digitalnog opismenjavanja učenika, ali isto tako i informirati roditelje o dječjem korištenju interneta kod kuće. Još jedan od problema interneta koji često zahvaća adolescente je ovisnost o računalnim igrama. Navedena ovisnost ima vrlo loš utjecaj na mlade jer noći koje provode na internetu mogu dovesti do zdravstvenih problema. Ipak, neki od izazova s kojima se škole suočavaju prilikom provedbi obrazovanja o kibernetičkoj sigurnosti uključuju nedostatak stručnosti, financija i resursa što je velik problem upravo zbog brzine tehnoloških promjena koje donose nove rizike. Neka od mogućih rješenja mogli bi biti simpoziji o kibernetičkoj sigurnosti ili više dostupnih baza podataka za čije korištenje je potrebno upoznati učenike s načinima pretraživanja uz korištenje ključnih riječi ili slično.[30] Ankete provedene u sklopu istraživanja o važnosti obrazovanja o kibernetičkoj sigurnosti u

[28] Usp. N. A. A., Rahman; I. H., Sairi; N. A. M., Zizi; F., Khalid. The importance of Cybersecurity Education in School. (2020.): str. 378-382. URL: https://www.semanticscholar.org/paper/The-Importance-of-Cybersecurity-Education-in-School-Rahman-Sairi/86ffd5ed7c2dd7a53fa9797250b8270556faef3e?p2df (2023-12-13)

[29] Isto.

[30] Isto.

školama donose rezultate iz kojih je vidljivo kako odrasli nisu spremni trošiti novac i vrijeme na seminare i programe o kibernetičkog sigurnosti, stoga je ključno da škole postanu centri znanja za kibernetičke probleme u zajednicama. Crtani filmovi također bi mogli biti jedan od alata koji se koriste za promoviranje obrazovanja o kibernetičkoj sigurnosti u školama, isto kao i razni programi podizanja svijesti o sigurnosti. Jedan od dobrih primjera promicanja obrazovanja o kibernetičkoj sigurnosti je i ljetni kamp za učenike i nastavnike pod nazivom *GenCyber*, a koji je namijenjen za američke osnovne škole. Kako ovakva inicijativa može promicati svijest o kibernetičkoj sigurnosti i spremnost školske zajednice na suočavanje s istom, nužno je da svaka škola provodi barem sličnu inicijativu. Aktivno učenje o problemu potiče bolje razumijevanje tako da bi se učitelji i roditelji trebali udružiti u obrazovanju učenika i prevladati ovaj problem. Također, mediji poput televizije i radija mogli bi puno toga postići u obrazovanju djece o kibernetičkoj sigurnosti jer su takve vrste učenja interaktivne i djeci zanimljive i razumljive.[31]

6.2. Obrazovanje o kibernetičkoj sigurnosti na sveučilištima

Kako bi se izgradili pouzdani sustavi, neophodna je obrazovna radna snaga. Jedan od problema kibernetičke sigurnosti na fakultetima je taj što mnogi ignoriraju nastavno osoblje koje predaje o kibernetičkoj sigurnosti, a uzrok tome je neuključenost nastavnog osoblja u rasprave o stvaranju kurikuluma. Nedostatak autoriteta za obrazovanje na fakultetskoj razini uvelike utječe na obrazovanje o kibernetičkoj sigurnosti izvan same institucije.[32]

Još jedna od prepreka u stvaranju kurikuluma je to što istraživačka sveučilišta ne pridaju veliku vrijednost pedagogiji. Zato istraživači kibernetičke sigurnosti nisu potaknuti pisati udžbenike ili anketne članke iako taj način aktivnosti dovodi do otkrivanja novih kategorizacija i ideja. Ipak, čak i kada bi nastava bila temeljena na udžbenicima vrhunskih istraživača, neizvjesno je što bi trebalo podučavati buduće programere softvera. Jedna strana misli kako bi takvi kolegiji mogli potaknuti kontradiktorno razmišljanje, ali drugi vjeruju da bi se kolegiji tog tipa trebali temeljiti na načelima i apstrakcijama koje unose disciplinu u izgradnju sigurnosnih sustava. Kultura je ono što koči razvoj nastavnog plana i programa kibernetičke sigurnosti te bi trebalo poduzeti značajne promjene kako bi nastavnici mogli poduzeti određene mjere i uvesti

[31] Isto.

[32] Usp. B. Schneider, Fred. Cybersecurity Education in Universities. (2013.): str. 3-4. URL: https://ieeexplore.ieee.org/abstract/document/6573305 (2023-12-13)

kvalitetne kolegije koji se mogu baviti problematikom kibernetičke sigurnosti na svim razinama, pogotovo zato što istraživanja Nacionalne inicijative za karijere i studije kibernetičke sigurnosti SAD-a pokazuje rastući interes za obrazovanjem na tom polju.[33]

[33] Isto.

7. Podjela kibernetičke sigurnosti i razmjer prijetnji

Multinacionalni pružatelj kibernetičke sigurnosti i antivirusnih usluga, Kaspersky Lab, kibernetičku sigurnost smatra praksom obrane računala, poslužitelja, mobilnih uređaja, elektroničkih sustava, mreža i podataka od zlonamjernih napada, odnosno sigurnosti informacijske tehnologije, vrlo je jasno kako je definicija široko primjenjiva i djeljiva u kategorije. Prva kategorija je mrežna sigurnost koja osigurava računalne mreže od uljeza. Zatim postoji kategorija koja podrazumijeva sigurnost aplikacija koja se najprije usmjerava na zaštitu softvera i uređaja, a uspjeh ove kategorije počinje još u fazi projektiranja programa i uređaja, a ne nakon njihove implementacije. Sljedeća je informacijska sigurnost koja štiti privatnost podataka i tijekom pohrane i tijekom prijenosa. Operativna sigurnost temelji se na procesima za zaštitu imovine podataka, a uključuje dopuštenja koja korisnici imaju za vrijeme pristupanja mreži i postupke koji određuju gdje se podatci i na koji način mogu pohranjivati ili dijeliti. Oporavak od katastrofe i kontinuitet poslovanja kategorija je koja definira način na koji određena organizacija reagira na kibernetičku sigurnost ili neki drugi događaj koji može uzrokovati gubitak podataka. Cilj je da organizacija reagira na način koji će ju što brže i efikasnije vratiti na radni kapacitet koji je bio ustaljen prije incidenta, a kontinuitet poslovanja predstavlja plan kojim se organizacija služi u procesu oporavljanja bez potencijalno potrebnih resursa. Zadnja kategorija odnosi se na edukaciju krajnjih korisnika pri čemu se ljudi smatraju najnepredvidljivijim faktorom procesa zato što sustave mogu slučajno zaraziti virusima. Stoga je bitno podučiti ih da brišu sve sumnjive podatke elektroničke pošte kao i da ne koriste USB pogone za koje nisu sigurni što mogu prenijeti na računalo.[34]

Prijetnje s kojima se kibernetička sigurnost sve češće mora nositi dijele se u tri skupine. Prva je kibernetički kriminal koji se odnosi na pojedince ili skupine koje ciljaju sustave zbog financijske dobiti ili samo zbog poremećaja određenog sustava. Druga prijetnja pod nazivom *cyber-attack* (kibernetički napad) odnosi se na prikupljanje informacija koje je najčešće motivirano politikom te političkim informacijama i događajima. Treća skupina prijetnji naziva

[34] Usp. What is Cyber Security? URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (2023-07-02)

se kibernetički terorizam (*cyberterrorism*) te joj je cilj potkopati elektroničke sustave što bi za posljedicu rezultiralo panikom ili strahom.[35]

Osim već spomenutnoga *malware* zloćudnog softvera, virusa, *trojanaca* i ostalih štetnih softvera koji napadaju uređaje, otkriveni su neki novi napadači. *Dridex malware* jedan je od novijih zloćudnih softvera koji je imao veliku ulogu u globalnom napadu 2019. godine, a ministarstvo pravosuđa SAD-a optužilo je vođu jedne kibernetičke kriminalne skupine za napad zloćudnim softverom koji je imao snažan utjecaj na javnost, vladu, poslovanje i čitavu infrastrukturu širom svijeta. *Dridex* zapravo pripada u skupinu financijskih trojanaca s cijelim spektrom mogućnosti, a koristi se još od 2014. Djeluje na temelju tzv. *phishing*-a elektroničke pošte te je namijenjen za krađu zaporki, bankovnih i osobnih podataka koji se kasnije koriste u lažnim transakcijama. Istraživanja pokazuju kako je odgovoran za stotine milijuna dolara vrijedne financijske gubitke. Kao obrambena zaštita od zloćudnog softvera, javnosti se savjetuje da uključe antivirusne programe, redovno ih ažuriraju te sve datoteke sigurnosno kopiraju. Nadalje, jedna od čestih kibernetičkih prevara je romantična prevara, a odvija se putem stranica za upoznavanje te ostalih aplikacija za dopisivanje. Na taj način se iskorištavaju ljudi koji su u potrazi za partnerima, a koje se navodi na dijeljenje osobnih podataka. Još jedan od novijih zlonamjernih softvera je *Emotet malware* koji se smatra sofisticiranim *trojancem* koji ima sposobnost krađe podataka i učitavanja drugog zlonamjernog sustava odmah zatim. *Emotet* značajno napreduje baš zbog nedovoljno jakih lozinki kojima se korisnici koriste.[36]

7.1. Kako se zaštititi od kibernetičkih napada

Kako je pojedinac često slučajno odgovoran za učitavanje zlonamjernog softvera na neki od svojih uređaja, tako je važno da se pojedinac od zlonamjernih softvera zna i zaštititi. Jedan od načina je korištenje sigurnosnih softvera koji imaju mogućnost zaštite informacija u prijenosu te zaštite od gubitka ili krađe informacija. Elektronički sigurnosni protokoli namijenjeni su za otkrivanje napada u stvarnom vremenu te se za pomoć koriste razne analize za praćenje ponašanja programa i koda za obranu od zlonamjernih softvera koji mijenjaju svoj oblik pri svakom izvođenju (tzv. polimorfni i metamorfni zlonamjerni softveri). Zlonamjerni softveri izdvajaju se u posebne, izdvojene virtualne mjehuriće gdje se zatim proučava njihovo ponašanje. Zaključno, na kraju se sve svodi na nekoliko koraka kojih se korisnici moraju

[35] Isto.

[36] Isto.

pridržavati kako bi se osigurali od napada zlonamjernih softvera. Bitno je redovno ažurirati softver i operativni sustav kako bi se mogli služiti novitetima zaštite. Potrebno je koristiti antivirusne softvere kako bi se na vrijeme otkrila i uklonila prijetnja. Neophodno je koristiti jake lozinke koje nisu lake za pogoditi te ne otvarati privitke sumnjive elektroničke pošte. Korisnici ne bi trebali otvarati poveznice u elektroničkim porukama koje su stigle od nepoznatih korisnika te bi uvijek trebali izbjegavati korištenje nesigurnih WiFi mreža na javnim mjestima jer su takve mreže idealno područje za napade čovjeka u sredini (*man-in-the-middle attack*).[37]

[37] Isto.

8. Što je hakiranje?

Hakiranje se odnosi na sve aktivnosti koje nastoje ugroziti digitalne uređaje poput računala, pametnih telefona, tableta ili čak cijele mreže. Već je spomenuto kako hakiranje nije uvijek zlonamjerno, međutim, većina referenci koja se danas koristi uz hakiranje karakterizira tu radnju kao nezakonitu aktivnost kibernetičkih kriminalaca koji su motivirani financijskom dobiti, prosvjedom, prikupljanjem informacija, odnosno špijuniranjem ili hakeri izvršavaju napade samo zbog zabave koju im taj izazov donosi. Velik broj ljudi misli kako se pojam hakera odnosi na samoukog tinejdžera ili vještog programera koji je upoznat s načinima modificiranja softvera na načine koji nisu primarna svrha njegova zanimanja.[38] Hrvatska enciklopedija hakera definira tako da je on: „osoba dobro upućena u računala, računalne mreže ili programiranje, no time se bavi na svoju ruku, kadšto i prelazeći granicu dopuštenoga (neovlašteno pristupanje računalnim sustavima, probijanje zaštita programa od kopiranja i sl.)“[39], dok računalnu sigurnost definira i opisuje kao: „skup mjera i postupaka kojima se osiguravaju podatci pohranjeni u računalima, često dostupni i preko računalne mreže. U današnje doba, kada se najveći dio podataka pohranjuje u računalima, kadšto i samo u tom obliku, te kada se velik dio poslovanja, komunikacije i sl. odvija u računalnom okruženju, gubitak ili zloporaba podataka može prouzročiti velike štete. Stoga je računalna sigurnost osobito važna, a obuhvaća zaštitu podataka od gubitka ili oštećenja, kao i od neovlaštena pristupa njima.“[40] Zbog toga je važno razumjeti motive kojima se hakeri vode pri izvršavanju kibernetičkog kriminala, a koji često uključuju novac, moć i ego.

Hakiranje obično predstavlja stvaranje zlonamjernog oglašavanja vođeno zlonamjernim softverom koji ne zahtijeva interakciju s korisnicima, no često se koristi i psihologija koja pomaže u prevari nad korisnicima tako što ih navodi da kliknu na zlonamjernu poveznicu ili da ostave svoje osobne podatke. Taj način zavaravanja naziva se društveni inženjering, a osim njega postoje još i tzv. *botneti*, otmice preglednika, napadi uskraćivanjem usluge (DDoS),

[38] Usp. Hacking definition: What is hacking? URL: https://www.malwarebytes.com/hacker (2023-07-18)

[39] Haker. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=68094 (2023-07-18)

[40] Računalna sigurnost. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=68380 (2023-07-18)

trojanci, virusi, crvi i slično. Zbog brojnih mogućnosti hakiranje se razvilo iz dječjeg nestašluka u rastući posao koji je vrijedan milijarde dolara u kriminalnoj infrastrukturi koja se svakodnevno razvija i prodaje alate za hakiranje čak i onima koji nemaju dovoljno razvijene vještine za obavljanje tog posla samostalno. Postoje glavna četiri razloga zbog kojih se hakeri mogu okušati u kibernetičkom kriminalu, a oni uključuju financijsku dobit koja se temelji na krađi brojeva kreditnih kartica ili prevarama bankovnih sustava, zatim ugled koji se stječe među ostalim hakerima, korporativna špijunaža gdje hakeri jedne tvrtke žele ukrasti informacije konkurencije kako bi na tržištu mogli biti u prednosti te destabilizacija infrastrukture protivnika koja se često odnosi na hakiranje nacionalnih podataka, a koja rezultira pomutnjom u čitavoj zemlji. Još jedna kategorija koja postoji obuhvaća politički ili društveno motivirane hakere kojima je cilj usmjeriti pozornost javnosti na problem tako što objavljuju vrlo osjetljive informacije.[41]

Kada govorimo o etičkom hakiranju, razlikujemo već spomenute bijele i crne šešire te sive šešire kao spoj prethodna dva. Hakeri s crnim šeširima osobe su s istančanim razumijevanjem računalnih sustava i softvera, no cilj im je potkopati tehnologiju kako bi ukrali nešto vrijedno ili poremetili sustav iz bilo kojeg drugog razloga (krađa, ugled, korporativna špijunaža ili hakiranje države). Nasuprot njima imamo bijele hakere kojima je cilj poboljšati sigurnosne sustave tako da pronađu ranjive dijelove i poboljšaju ih prije nego dođe do kibernetičkog zločina. Između navedenih hakera s bijelim i crnim šeširima nalaze se hakeri sa sivim šeširima koji provaljuju u sustave bez dopuštenja, ali svoje pronalaske zatim prijavljuju vlasniku napadnute mreže ili sustava te nude popravak nedostatka u zamjenu za novčanu naknadu. Kako bi se obranili od bilo kakvih hakera, važno je osigurati svoju mrežu na kvalitetan način te izbjegavati preuzimanja aplikacija koje se ne nalaze na provjerenim platformama poput Google Play-a ili Amazon Appstore-a. Također, ukoliko aplikacije imaju niske recenzije i malen broj preuzimanja, najbolje ih je izbjegavati. Softvere koji se bave sprječavanjem napada potrebno je redovno ažurirati i nikada ne ostavljati osjetljive podatke u elektroničkim porukama te uvijek paziti da se ne ulazi na sumnjive poveznice koje stižu s nepoznatim elektroničkim porukama. Važno je educirati korisnike sustava kako bi znali prepoznati neželjenu elektroničku poštu i kako bi znali postaviti jake zaporke, uz implementaciju višefaktorske provjere autentičnosti. I naravno, potrebno je redovno ažurirati softvere.[42] Kako bi se korisnici što bolje mogli zaštititi, potrebno ih je podučiti koji su to sve načini na koji hakeri mogu provaliti u

[41] Usp. Hacking definition: What is hacking? URL: https://www.malwarebytes.com/hacker (2023-07-18)

[42] Isto.

sustave i doći do njihovih podataka, a u tome može pomoći OWASP organizacija koja ima popis najčešćih sigurnosnih rizika s kojima se web aplikacije mogu susresti, a koji uvelike pomažu programerima i testerima pri stvaranju sigurnih aplikacija.

9. Što je OWASP i koji su najčešći sigurnosni rizici web aplikacija?

OWASP je *Open Web Application Security Project*, odnosno Otvoreni projekt web aplikacija za sigurnost te neprofitna organizacija koja je usmjerena na sigurnost softvera. Projekti organizacije su brojni, a također uključuju mnoštvo programa i alata koji pomažu pri razvoju softvera otvorenoga koda. Istraživanja su pokazala da se kod skeniranja 130000 aplikacija čak 68% aplikacija susrelo sa sigurnosnim propustima koji su prikazani kao najčešći po OWASP popisima. Testiranje na temelju OWASP nedostataka ključno je za razvoj sigurnih aplikacija, stoga su stručnjaci organizacija napravili upute koje se sastoje od nekoliko jednostavnih koraka: ugraditi sigurnosni sustav na početku razvojnog procesa, više puta testirati kod koristeći se sigurnosnim standardima (poželjno uz automatizaciju testova) te identificirati poznate nedostatke u kodu treće strane kako bi programeri bili sigurni da se kod ne služi nesigurnim ovisnostima (*dependencies*).[43] U nastavku su prikazani neki od sigurnosnih rizika web aplikacija, koji uključuju tzv. *Injection*, *Broken Authentication*, *Sensitive Data Exposure*, *Broken Access Control* i slično.

Injection (Injekcija) je nedostatak koji se događa kada zlonamjerni haker iskoristi nesiguran kod za ubrizgavanje (*inject*) vlastitog koda u neki program. Program ne može odrediti kod umetnut na ovaj način i zato se hakeri mogu služiti ovim principom kako bi pristupili sigurnim i povjerljivim podatcima. Neki od primjera ovog načina hakiranja su SQL injekcije, injekcije naredbi i slično, a mogu se otkriti testiranjem sigurnosti aplikacije, nakon čega dolazi do raznih tehnika ispravljanja gdje je potrebno ukloniti određene znakove iz korisničkog unosa ili je potrebno napisati parametrizirane SQL upite. Sljedeći nedostatak naziva se Neispravna autentifikacija (*Broken Authentication*) koja predstavlja neispravno provedenu provjeru autentičnosti koja dovodi do visokih sigurnosnih rizika jer hakeri tako mogu preuzeti identitet drugih osoba. Kako bi se zaštitili od ove vrste napada, korisnici bi trebali prakticirati višefaktorsku autentifikaciju. Zatim postoji rizik od izlaganja osjetljivih podataka (*Sensitive Data Exposure*) gdje se API-ji koji omogućuju povezivanje aplikacija s uslugama treće strane poput npr. Google karata, što iznimno štedi vrijeme programera, mogu osloniti na metode koje nisu previše sigurne za prijenos podataka, što dovodi do toga da hakeri mogu doći do podataka o korisničkim pristupnim podacima ili drugih osjetljivih informacija. Rješenje bi bila enkripcija

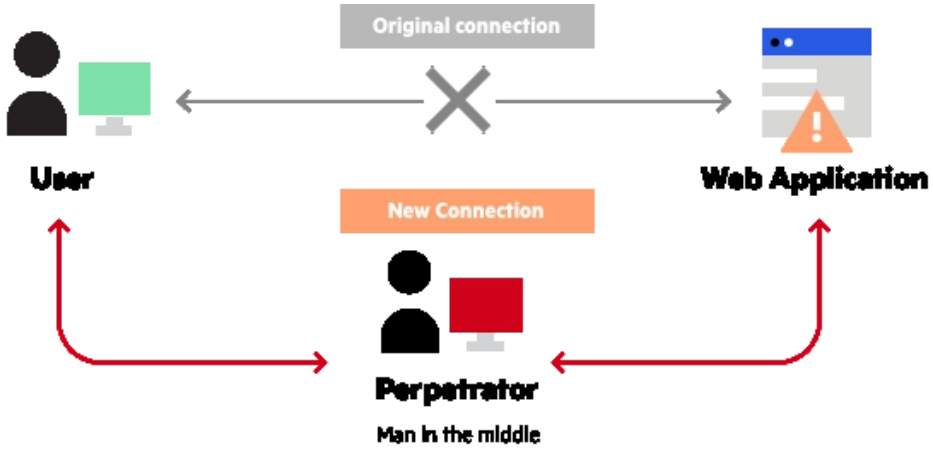
[43] Usp. OWASP Top 10 Vulnerabilities. URL: https://www.veracode.com/security/owasp-top-10 (2023-07-19)

podataka ili onemogućavanje predmemoriranja odgovora. XML vanjski entiteti (*XML External Entities*) predstavljaju rizik koji se pojavljuje kad napadači prenose zlonamjeran XML sadržaj zbog nesigurnog koda, a može se spriječiti onemogućavanjem obrade vanjskih XML entiteta. *Broken Access Control* ili pokvarena kontrola pristupa podrazumijeva neispravno implementiranu autentifikaciju i ograničenje pristupa koji hakerima omogućuju pristup osjetljivim informacijama. Ovaj se način hakiranja može otkriti testiranjem prodora (*penetration testing*), no potrebno je i ojačati kontrolu pristupa te zaključavati administrativne račune uz korištenje višefaktorske autentifikacije. Sigurnosna pogrešna konfiguracija (Security *Misconfiguration*) je kao i prethodni nedostatak kontrole pristupa vrlo velik problem koji se može riješiti dinamičkim testiranjem koje otkriva je li sigurnost u aplikaciji pogrešno konfigurirana. *Cross-Site Scripting* (Skriptiranje na različitim mjestima) odnosi se na zlonamjerno iskorištavanje API-ja i manipulaciju DOM-a (*Document Object Model*) u svrhu dohvaćanja podataka ili slanja naredbi određenoj aplikaciji, a hakerima također omogućava i pregled povijesti pretraživanja, otimanje korisničkih računa, širenje virusa, daljinsko kontroliranje preglednika i još mnogo toga. Rizik se smanjuje kodiranjem podataka i redovnom provjerom valjanosti unosa. *Insecure Deserialization* (Nesigurna deserijalizacija), to jest dohvaćanje podataka i objekata koji su zapisani na diskovima ili spremljeni na neki drugi način, koristi se za daljinsko izvršavanje koda koje omogućuje daljnje zlonamjerne napade na sustav, a napisan je u JSON ili XML formatima. Služi za promjenu ponašanja aplikacije ili za uskraćivanje usluge (DoS), a rizik od takvih napada može se smanjiti testiranjem prodora ili korištenjem sigurnosnih alata aplikacije. Još jedan od načina da se navedeni rizik spriječi je neprihvaćanje serijaliziranih objekata iz sumnjivih izvora, kao i nekorištenje metoda koje dopuštaju isključivo primitivne tipove podataka. *Using Components with Known Vulnerabilities* (Korištenje komponenti s poznatim ranjivostima) rizik je koji govori o tome kako napadači, bez obzira na sigurnost koda, mogu iskoristiti API-je, ovisnosti i ostale komponente ako i one nisu sigurne. Analiza softvera sposobna je locirati i neutralizirati nesigurnosti s kojima se aplikacija susreće te je navedenu analizu potrebnu provesti prije nego aplikacija bude objavljena. Naposlijetku, imamo nedovoljno bilježenje i praćenje (*Insufficient Logging and Monitoring*) koji opisuje neuspjeh bilježenja pogrešaka i napada te lošu praksu nadzora, a hakeri često na nedostatak nadzora i računaju, budući da je on popraćen i sporijim vremenom sankcioniranja problema. Ovaj se rizik može spriječiti tako da se svi neuspjesi prijave kako bi programeri imali uvid u potencijalno sumnjive aktivnosti, a još jedan od načina

sankcioniranja navedenog rizika bilo bi testiranje prodora (penetracijsko testiranje). Naravno, bitno je i uspostaviti praksu redovnog i učinkovitog praćenja.[44]

9.1. Čovjek u sredini (*Man in the middle attack*)

MITM napad odnosi se na napade u kojima je haker pozicioniran u interakciji između korisnika i aplikacije koju korisnik koristi. Cilj hakera je prisluškivanje ili predstavljanje kao jedna od dvije navedene strane interakcije, a krajnji željeni ishod odnosi se na krađu osobnih podataka poput pristupnih podataka, podataka o računu ili brojeva kreditnih kartica. Aplikacije koje su često napadnute na ovaj način su financijske aplikacije, web trgovine i slično, a napad može rezultirati krađom identiteta, neodobrenim plaćanjem proizvoda ili nedozvoljenim mijenjanjem zaporke. Slikovito bi se napad mogao objasniti poštarom koji otvara nečiji bankovni izvod, zapisuje podatke o računu te ponovno zatvara omotnicu i dostavlja je na adresu određene osobe.[45]



Slika 1. Prikaz MITM napada[46]

Kako bi se napad uspješno izvršio, potrebno je proći kroz dvije različite faze, a to su presretanje i dešifriranje. Presreće se promet korisnika putem mreže napadača, a to se najčešće odvija uz pomoć pasivnih napada koji su načinjeni od besplatnih i zlonamjernih Wi-Fi javnih mreža. Takve mreže uglavnom budu nazvane po lokaciji na kojoj se nalaze te nisu zaštićene zaporkama, a kada se korisnik spoji na takvu mrežu, napadač može vidjeti svu internetsku

[44] Isto.

[45] Man in the middle (MITM) attack. URL: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (2023-07-27)

[46] Isto.

razmjenu podataka koja se odvija na uređaju. Nakon što napadač uspješno presretne mrežu, potrebno je dešifrirati dvosmjerni promet koji se odvija na uređaju, no bez prethodnog upozorenja korisnika. Napadač tada šalje lažne certifikate koje korisnik potvrđuje i zatim dobiva krivotvorene autentifikacijske podatke kojima se može služiti u daljnjem hakiranju. Kako bi se zaštitili od MITM napada, korisnici bi trebali izbjegavati Wi-Fi mreže koje nisu zaštićene zaporkama, isto kao i web mjesta na kojima preglednik javlja kako mrežno mjesto nije zaštićeno. Potrebno je i izbjegavati javne mreže općenito, ukoliko se radi o provođenju određenih transakcija te se uvijek odjavljivati s aplikacija koje se u tom trenutku ne koriste.[47]

9.2. *Evil twin* napad

Već je spomenuto kako bi korisnici zbog sigurnosti trebali izbjegavati javne Wi-Fi adrese, no njihovo korištenje ipak je vrlo uobičajeno ukoliko se korisnici nalaze izvan svojih domova, a nemaju vlastitu mrežu. Zli napad blizanaca još je jedna od prijetnji s kojima se korisnici mogu susresti, a događa se kada hakeri postave lažnu Wi-Fi mrežu i čekaju da se korisnici umjesto na legitimnu, spoje na nju. Nakon spajanja, svi podatci koje korisnik dijeli putem mreže prolaze poslužiteljem kojim upravlja haker. Haker stvara zlog blizanca s pametnim telefonom ili drugim uređajem koji ima pristup na internet i jedan od lako dostupnih softvera. Napad se odvija u nekoliko koraka. Prvi korak je traženje pravog mjesta, a odnosi se na to da hakeri uglavnom traže mjesta s besplatnom Wi-Fi mrežom na koju se spaja velik broj ljudi (kafići, knjižnice i slično). Drugi korak odnosi se na postavljanje Wi-Fi pristupne točke pri čemu mogu koristiti bilo koji uređaj. Haker bilježi identifikator skupa usluga (SSID – *Service Set Identifier*) prave mreže te postavlja novi račun s istim SSID-om. Problem je u tome što uređaji koji se povežu na mrežu napadača ne mogu razlikovati pravu mrežu od lažne. Zatim slijedi poticanje korisnika da se povežu na *evil twin* Wi-Fi mrežu. Kako bi uspjeli u tome, hakeri se fizički približavaju korisnicima žrtvama kako bi stvorili jači signal nego što to nudi prava mreža. Korisnici će se prije spojiti na jaču vezu nego na slabiju, a neki uređaji će se prisilno spojiti automatski. Četvrti korak je postavljanje lažnog zarobljeničkog portala. Kako bi se prijavili na velik broj javnih Wi-Fi mreža, korisnici moraju ostaviti svoje podatke koji se šalju generičkoj stranici za prijavu. Hakeri u tom slučaju postavljaju kopije tih stranica te ostaje samo da čekaju na korisnike koji ne sumnjaju u tu mrežu, a kada dobiju pristupne podatke korisnika mogu se prijaviti na mrežu i kontrolirati je. Zadnji korak tiče se krađe podataka. Svaki korisnik koji se prijavi povezuje se

[47] Isto.

na mrežu preko hakera što odražava primjer napada čovjeka u sredini (MITM) i koji hakerima omogućuje praćenje svih online aktivnosti napadnutih korisnika. U slučaju bilo koje prijave na bilo koji račun, hakeri imaju uvid u pristupne podatke i zbog toga je vrlo opasno koristiti iste pristupne podatke za više različitih računa. Također, ova vrsta napada uglavnom ne ostavlja nikakve znakove za sobom te korisnici često primijete da se napad dogodio tek nakon što se određene radnje izvedu u njihovo ime. Kako bi izbjegli ovu vrstu napada, korisnici trebaju izbjegavati nezaštićene Wi-Fi mreže ili barem izbjegavati pristupne točke koje su označene kao nesigurne, ako se baš moraju spojiti na javnu mrežu. Trebali bi koristiti vlastitu pristupnu točku koja se spaja na pouzdane mreže, no potrebno je na vlastitu pristupnu točku postaviti lozinku kako bi ostala privatna. Također, trebali bi provjeravati obavijesti upozorenja, umjesto da iste ignoriraju te onemogućiti automatsko povezivanje. Trebali bi i izbjegavati prijavu na privatne račune dok su spojeni na javnu Wi-Fi mrežu te primjenjivati višefaktorsku provjeru autentičnosti (npr. lozinka + kod poslan na pametni telefon koji se treba unijeti za nastavak). Potrebno je i držati se HTTPS stranica, umjesto HTTP, jer slovo S označava sigurno, a HTTPS stranice koriste *end-to-end* enkripciju koja hakerima sprječava uvid u ponašanje korisnika na mreži. Za kraj, potrebno je i koristiti VPN (*Virtual Private Network*) virtualnu privatnu mrežu koja šifrira podatke prije nego što ih pošalje na mrežu i na taj način štiti korisnike od napada.[48]

9.3. Napad uskraćivanjem usluge (*Denial-of-service* (DoS) *attack*)

DoS napad je napad u kojem haker želi određeno računalo ili neki drugi uređaj učiniti nedostupnim za svoje uobičajene korisnike te želi prekinuti normalno funkcioniranje određenoga uređaja. Ova vrsta napada funkcionira preplavljivanjem uređaja raznim zahtjevima sve dok god se normalni promet ne može obraditi, a to rezultira uskraćivanjem usluge korisnicima. Napad je karakterističan po tome što se za njegovo pokretanje koristi samo jedno računalo. Također postoji i distribuirani napad uskraćivanjem usluge DDoS, a on je vrsta DoS napada koja dolazi iz raznih distribuiranih izvora, poput DDoS napada *botnet* mreže. (*Botnet* se odnosi na skupinu računala koja su zaražena zlonamjernim softverom, a koja su došla pod kontrolu hakera.[49]) Cilj DoS napada je prezasićenje kapaciteta određenog uređaja, što vodi uskraćivanju usluge za sve dodatne zahtjeve, no DoS napadi najčešće se svrstavaju u dvije skupine. Prva skupina su napadi prekoračenja međuspremnika (*Buffer overflow attacks*), a

[48] Usp. Evil twin attacks and how to prevent them. URL: https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks (2023-07-27)

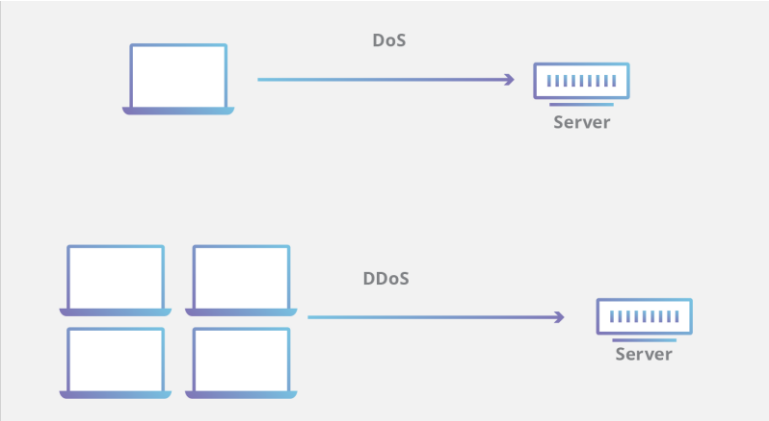
[49] Usp. What is a Botnet? URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (2023-07-28)

odnose se na prekoračenje međuspremnika memorije koje uzrokuje potrošnju svog raspoloživog prostora na tvrdom disku ili memoriji uređaja. Ovaj način napada odgovoran je za usporeni rad uređaja, pad sustava ili sličnim ponašanjem poslužitelja koji utječu na uskraćivanje usluge. Druga skupina su napadi poplava (*Flood attacks*), a oni zasićuju poslužitelj velikom količinom paketa kako bi prezasitili cijeli kapacitet poslužitelja pri čemu hakeri moraju imati veću raspoloživu propusnost od ciljanog uređaja kako bi napad bio uspješan.[50]

U povijesti DoS napada, može se primijetiti kako su napadi uglavnom iskorištavali sigurnosne propuste koji su prisutni u dizajnu određene mreže, softvera ili hardvera. Ipak, takvi napadi su postali sve rjeđi upravo zbog DDoS napada koji imaju puno veću sposobnost ometanja, a vrlo ih je lako stvoriti zbog dostupnih alata. Također, velik broj DoS napada može se pretvoriti u DDoS napade. Neki od češćih napada su *Smurf attack* (slanje lažnih paketa koje rezultira plavljenjem određene IP adrese), *Ping flood* (preplavljivanje uređaja s više ICMP (*ping*) paketa nego što je računalo može odgovoriti, a dovodi do uskraćivanja usluge – također se koristi i kao DDoS napad) i *Ping of Death* (povezan s *Ping flood*, uključuje slanje pogrešnog paketa na računalo, što rezultira padom sustava) napad. Neke od naznaka da se odvija DoS napad su neuobičajeno spora izvedba mreže (dugo vrijeme učitavanja datoteka ili mrežnih stranica), nemogućnost učitavanja određene mrežne stranice ili iznenadni gubitak povezivanja između uređaja na istoj mreži. Također, bitna razlika između DDoS i DoS napada je broj veza koje se koriste u napadu. Neki od DoS niskih i sporih napada poput *Slowloris* napada crpe svoju snagu u minimalnim zahtjevima koji su potrebni kako bi napad bio učinkovit. DoS koristi jednu vezu, a DDoS koristi višebrojne izvore prometa napada koji se često pojavljuju u obliku *botnet*-a.[51]

[50] Usp. What is a denial-of-service (DoS) attack? URL: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ (2023-07-28)

[51] Isto.



Slika 2. Razlika između DoS i DDoS napada[52]

9.4. Distribuirani napad uskraćivanja usluge (*Distributed denial-of-service (*DDoS*) attack*)

DDoS napad predstavlja pokušaj prekida normalnog prometa određenoga poslužitelja, usluge ili mreže, a temelji se na preplavljivanju uređaja ili njegove okolne infrastrukture poplavom internetskog prometa. Napadi su učinkoviti uz pomoć korištenja više kompromitiranih računalnih sustava koji predstavljaju izvor prometa napada. Uređaji koji se iskorištavaju su računala i drugi umreženi resursi poput IoT (*Internet of Things*) uređaja. Metaforički, DDoS napad predstavlja neočekivanu prometnu gužvu koja začepljuje autocestu, pritom sprječavajući redovni promet da dođe do krajnjeg odredišta. Ova vrsta napada izvodi se s mrežama računala koje su povezane s internetom, a te se mreže sastoje od računala i drugih uređaja koji su zaraženi zlonamjernim softverom, što hakerima omogućuje da ih daljinski kontroliraju. Navedeni pojedinačni uređaji nazivaju se *botovi*, a skupina *botova* naziva se *botnet*. Nakon što se *botnet* uspostavi, haker usmjerava napad slanjem daljinskih uputa svakom pojedinačnom *botu*. Kad napadnuta mreža dođe u doticaj s *botnetom*, svaki *bot* šalje zahtjeve na određenu IP adresu, što može uzrokovati preopterećenje poslužitelja ili mreže, a kao posljedica to dovodi do uskraćivanja usluge normalnom prometu. Odvajanje normalnog prometa od napadačkog može biti vrlo teško, budući da je svaki *bot* legitiman internetski uređaj. Jedan od najočitijih znakova za prepoznavanje napada je iznenadna sporost ili nedostupnost određene mrežne stranice ili usluge. Ipak, alati za analizu prometa mogu pomoći kako bi korisnici bili sigurni da se radi o napadu. Neki od znakova su: sumnjive količine prometa koje potječu s jedne IP adrese ili IP raspona, poplava prometa korisnika koji dijele jedan profil

[52] Isto.

ponašanja (vrsta uređaja, geolokacija, verzija mrežnog preglednika), neobjašnjivi porast zahtjeva prema jednoj stranici ili krajnjoj točki, čudni obrasci prometa (svakih deset minuta ili svaki neparni sat u danu) i slično. DDoS napadi dijele se u tri kategorije: napadi aplikacijskog sloja (*Application layer attacks*), napadi na protokol (*Protocol attacks*) i volumetrijski napadi (*Volumetric attacks*). Prvoj vrsti napada cilj je iscrpiti ciljne resurse za stvaranje uskraćivanja usluge, a jedan od primjera je *HTTP flood* koji je sličan stalnom pritiskivanju tipke za osvježavanje mrežnog preglednika na više računala u isto vrijeme, velik broj HTTP zahtjeva preplavljuje poslužitelj i tako dolazi do uskraćivanja usluge. Cilj druge vrste napada je uzrokovati prekid usluge prekomjernom potrošnjom resursa poslužitelja ili mrežne opreme poput vatrozida te ju učiniti nedostupnom. Treća vrsta napada pokušava stvoriti zagušenje trošenjem cijele dostupne propusnosti između ciljanog uređaja i interneta. Napadnutom uređaju šalju se velike količine podataka, a za to se koristi neki od oblika pojačanja za stvaranje masovnog prometa, poput zahtjeva s *botneta*. Kako bi se napad ublažio ili spriječio, potrebno je stvoriti crnu rutu i prema njoj usmjeriti sav normalan promet, no to nije idealno rješenje jer na taj način mreža postaje nedostupna, što je krajnji cilj hakera. Još jedno rješenje je ograničavanje broja zahtjeva koje poslužitelj može prihvatiti u određenom vremenskom roku. Također, moguće je i raspršiti promet napada preko mreže distribuiranih poslužitelja do točke u kojoj mreža apsorbira promet (*Anycast network diffusion*). Ovaj pristup širi utjecaj distribuiranog napadačkog prometa do točke u kojoj postaje upravljiv i gdje se sve ometajuće sposobnosti raspršuju.[53]

9.5. *Slowloris* DDoS napad

Slowloris je napad uskraćivanja usluge koji omogućuje hakerima da preplave određeni poslužitelj otvaranjem i održavanjem mnogih istovremenih HTTP veza između hakera i određenog uređaja. Predstavlja napad aplikacijskog sloja koji djeluje korištenjem djelomičnih HTTP zahtjeva koji otvara veze s ciljanim mrežnim poslužiteljem i onda te veze drži otvorenima koliko god dugo je to moguće. Ne spada pod kategoriju napada, već je *Slowloris* alat za napad koji je dizajniran da jednom uređaju omogući rušenje poslužitelja bez korištenja velike propusnosti. Za razliku od DDoS napada koji troši propusnost, ova vrsta napada koristi minimalnu količinu propusnosti te joj je cilj iskoristiti resurse poslužitelja sa zahtjevima koji su

[53] Usp. What is a DDoS attack? URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (2023-07-28)

sporiji od normalnih, no koji oponašaju normalni promet. Svaka veza poslužitelja pokušat će se održavati dok čeka da se završi spori zahtjev, no kad se prekorači najveći mogući broj veza poslužitelja, na svaku narednu vezu neće biti odgovoreno te će doći do uskraćivanja usluge. *Slowloris* napad odvija se u četiri koraka. Napadač prvo otvara višestruke veze s određenim poslužiteljem slanjem višestrukih djelomičnih HTTP zahtjeva. Ciljani poslužitelj tada otvara vezu za svaki dolazni zahtjev, s namjerom zatvaranja nakon njezina dovršenja. Kako ne bi došlo do isteka vremena, haker povremeno šalje djelomična zaglavlja zahtjeva uređaju kako bi održao zahtjev. Ciljani poslužitelj ne može otpustiti niti jednu od otvorenih djelomičnih veza dok čeka dovršenje zahtjeva, a nakon što sve dostupne veze budu u upotrebi, poslužitelj neće moći odgovoriti na dodatne zahtjeve koji se upućuju iz normalnog prometa te tada dolazi do uskraćivanja usluge. Kako bi se napad ublažio, potrebno je povećati dostupnost poslužitelja jer će povećanje maksimalnog broja klijenata povećati i broj veza koje haker mora napraviti prije preopterećivanja poslužitelja. Potrebno je i ograničiti brzinu dolaznih zahtjeva te ograničiti maksimalan broj veza koje jedna IP adresa smije ostvariti. Osim toga, potrebno je i ograničiti brzinu prijenosa i maksimalno vrijeme koje je korisniku dopušteno da ostane povezan.[54]

[54] Usp. Slowloris DDoS attack. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (2023-07-28)

10. Kako ostati siguran na internetu?

Savjeti oko toga kako ostati siguran na internetu imaju dovoljno prostora za napredak. Od ljudi se traži previše toga, a ciljevi zahtjeva često su nerealni, dugotrajni ili nisu vrijedni truda. Kako bi se sigurnosna zaštita korisnika na internetu poboljšala potrebno je saznati koje prakse ljudi koriste te koje će preporuke koje im se nude donijeti najveću korist. Istraživački rad kojim su se bavili Iulia Ion, Rob Reeder i Sunny Consolvo donosi prikaz usporedbe sigurnosnih praksi nestručnjaka i stručnjaka za sigurnost koji se bave računalnom sigurnosti najmanje pet godina.[55]

Istraživanje pokazuje kako stručnjaci najčešće izvješćuju instaliranje ažuriranja softvera, korištenje dvofaktorske provjere autentičnosti i korištenje upravitelja lozinki za sigurnost na mreži, a nestručnjaci navode kako koriste antivirusne softvere, posjećuju samo poznate web stranice te učestalo mijenjaju lozinke. U već navedenom istraživačkom radu, istraživači su ispitali stručnjake koje bi savjete dali korisnicima koji nisu previše upućeni u tehnologiju. Odgovori su najčešće bili: održavanje sustava i softvera ažurnima, korištenje jedinstvenih lozinki, korištenje jakih lozinki, korištenje dvofaktorske autentifikacije, korištenje antivirusnih softvera i upravitelja lozinki. Ipak, nestručni sudionici istraživanja smatrali su učinkovitim korištenje antivirusnog softvera, korištenje jakih zaporki i njihove često mijenjanje te posjećivanje isključivo pouzdanih mrežnih stranica. Nadalje, stručnjaci su se izjasnili kako ne preporučuju otvaranje poveznica ili e-pošte od nepoznatih ljudi, no ipak su izvijestili da to čine puno češće nego nestručna populacija istraživanja. Također, izjasnili su se kako ne smatraju posjećivanje isključivo provjerenih stranica vrlo bitnim.[56]

Potvrđeno je kako nestručna populacija istraživanja najčešće ne ažurira sigurnosne sustave jer su isti često povezani s drugim nepoželjnim značajkama ili su imali poteškoća s procjenom vrijednosti ažuriranja, a nekad su bili i zbunjeni zašto su ažuriranja uopće potrebna. Problem stvaranja lozinki istraživači su primijetili prilikom obuke korisnika gdje su ih učili kako sastaviti neprobojnu lozinku i na taj način zaštititi profile. Kasnije su otkrili kako su korisnici koristili nepotpune ili netočne oblike lozinki te nisu bili uvjereni da im je korištenje upravitelja lozinki donijelo značajne sigurnosne prednosti i oklijevali su prepustiti kontrolu svojih lozinki

[55] Ion, I.; Reeder, R. W.; Consolvo, S. „„…no one can hack my mind“: Comparing Expert and Non-Expert Security Practices.“ *Symposium On Usable Privacy and Security.* (2015.): str. 327-328.

[56] Isto.

na softver. Još jedna od poduzetih radnji prilikom istraživanja bila je svjesnost koja je uključivala posjećivanje samo poznatih mrežnih stranica, provjeravanje HTTPS indikatora i e-pošte, a sve u svrhu zaštite od *phising-a*, zlonamjernog softvera i napada čovjeka u sredini. Istraživanje je pokazalo kako su korisnici imali poteškoća s razlikovanjem stranica za krađu identiteta.[57]

Istraživanje se provodilo na 231 ispitaniku koji se vodio kao stručnjak u ovome području i na 294 ispitanika koji nisu bili stručnjaci. Na pitanje što rade kako bi ostali sigurni na internetu, stručnjaci su najčešće odgovarali tako da instaliraju ažuriranje softvera (35%), dok je samo 2% nestručnjaka spomenulo da ima istu praksu. 2% stručnjaka reklo je i kako koristi automatsko ažuriranje, što niti jedan nestručnjak nije spomenuo. Kao razlog loše prakse instaliranja ažuriranja kod nestručne populacije ispostavilo se da je nedostatak svijesti o tome koliko su ažuriranja učinkovita. Ipak, čak su i neki stručnjaci izrazili zabrinutost prilikom automatskog ažuriranja jer bi se taj način mogao iskoristiti za ažuriranje zlonamjernog sadržaja. Korištenje antivirusnog softvera našlo se među najučestalijim praksama zaštite računala od zlonamjernih softvera, a njihovo korištenje među prve tri stavke zaštite navelo je 42% nestručnjaka i 7% stručnjaka. Kada su ih pitali koriste li antivirusni softver na osobnim računalima, 85% nestručnjaka odgovorilo je pozitivno, dok je samo 63% stručnjaka potvrdilo da čini isto. Korištenje vatrozida, često u kombinaciji s antivirusnim softverom, potvrdilo je 17% nestručnjaka i 3% stručnjaka. Prilikom odgovaranja na upit o korištenju jedinstvenih zaporki, potvrdno je odgovorilo 25% stručnjaka i 15% nestručnjaka, no nisu svi potvrdili i korištenje jakih lozinki, kao ni korištenje upravitelja lozinkama gdje je samo 12% stručnjaka i 3% nestručnjaka odgovorilo potvrdno. Neki stručnjaci naveli su kako zapisivanje lozinki smatraju zamjenom za korištenje upravitelja lozinki, pogotovo zbog toga što zlonamjerni softver ne može pročitati podatke s papira. 38% nestručnjaka i 20% stručnjaka izjasnilo se da su zapisali barem neke od svojih lozinki. Oni koji su bili protiv toga izrazili su zabrinutost za to koliko će papir sigurno biti pohranjen. S druge strane, samo 4% stručnjaka i 15% nestručnjaka izjavilo je kako se ne sjeća niti jedne svoje lozinke te su neki naveli i kako ih često moraju ponovno uspostavljati jer ih zaborave. Velika razlika u sigurnosnim potezima kojima se ispitanici služe bila je kod učestalog mijenjanja lozinki gdje se potvrdno izjasnilo 21% nestručnjaka i samo 2% stručnjaka. Istraživači su im kasnije objasnili kako napadači koji znaju staru lozinku vrlo lako mogu pogoditi novu ako na njih primijene jednostavne transformacije. Primjenu dvofaktorske

[57] Isto, str. 328.

autentifikacije potvrdilo je 89% stručnjaka i 62% nestručnjaka, no neki stručnjaci smatraju kako je takav način zaštite još uvijek težak za neke korisnike ili nije široko dostupan. Posjećivanje samo provjerenih i poznatih mrežnih stranica potvrdilo je 21% nestručnjaka i 4% stručnjaka, no 4% nestručnjaka izjavilo je kako osobne podatke daju samo provjerenim mrežnim mjestima i samo 3% nestručnjaka izjavilo je kako kupuju samo na pouzdanim mrežnim mjestima. Stručnjaci nisu spominjali takve prakse. Samo 10% stručnjaka i 4% nestručnjaka reklo je kako provjeravaju HTTPS mrežnog mjesta na kojemu se nalaze, no 2% nestručnjaka i 3% stručnjaka reklo je kako ne daju osobne podatke i podatke o kreditnim karticama osim ako je veza preko HTTPS-a. Ipak, iako je većina ispitanika (60%) potvrdila kako je način pregledavanja HTTPS-a odlična i efikasna praksa, samo se 50% ispitanika izjasnilo kako bi mogli slijediti tu praksu. Samo 6% nestručnjaka i jedan stručnjak izjasnili su se da je praksa brisanja ili ograničavanja kolačića jedna od najčešćih praksi s kojima se služe za zaštitu od zlonamjernih softvera, a 54% stručnjaka ocijenilo je tu praksu lošom, dok je samo 21% ocijenio navedenu praksu dobrom praksom prilikom zaštite od napada zlonamjernog softvera. Još jedna od praksi zaštite bilo je ne otvarati e-poštu i poveznice od nepoznatih pošiljatelja te se preko 80% ispitanika složilo kako je to dobra praksa. Ipak, 38% stručnjaka i 12% nestručnjaka izjasnili su se kako otvaraju poveznice nepoznatih pošiljatelja. Time je moguće naslutiti kako stručnjaci najviše slijede savjete poput instalacije ažuriranja i korištenja upravitelja lozinkama, dok ostale savjete više slijede nestručnjaci. Zanimljiva izjava koju je rekao jedan od nestručnjaka je kako nitko ne može hakirati njegov um i zato će radije pamtiti lozinke, nego ih povjeriti upravitelju zaporki.[58]

Kako se u zadnjih nekoliko godina povećao broj ljudi koji rade od kuće, tako su došle i nove prijetnje, odnosno rizici od *phising* napada kroz koje zaposlenici mogu biti prevareni na način da otkriju svoje informacije poput pristupnih podataka za prijavu u sustav. Još jedan od problema je i što je u Velikoj Britaniji provedeno istraživanje koje je pokazalo da čak 51% zaposlenih dijeli lozinke s ostalim kolegama u manjoj ili većoj mjeri.[59] Višefaktorska provjera autentičnosti pruža dodatan sloj sigurnosti za poslovne mreže, no uvijek postoji rizik od krađe identiteta ili napada čovjeka u sredini. Višefaktorska autentifikacija može se provoditi putem nezaboravnih riječi ili jednokratnih SMS lozinki, no unos odgovora i šifri često je sklon greškama te oduzima vrijeme zaposlenima, stoga zaposlenici smatraju kako im taj način zaštite predstavlja prepreku za obavljanje posla i smanjuje njihovu produktivnost. *Cloud* okruženje

[58] Isto, str. 330-338.

[59] Sarginson, Nic. Why is phising still successful?: Securing your remote workforce against new phising attacks. // Computer Fraud & Security 2020(9): str. 9-12.

zbog toga bi moglo biti najbolja opcija budući da podržava rad na daljinu bez ugrožavanja suradnje.[60]

[60] Isto.

11. Istraživanje o zaštiti osobnih podataka među populacijom studenata te koliko su upoznati s načinima hakiranja ili kibernetičkom sigurnošću

Cilj i svrha istraživanja koji će biti predstavljeni u ovom diplomskom radu bili su otkriti koliko su studenti upoznati s pojmom hakiranja te koliko su oprezni pri dijeljenju svojih osobnih podataka na društvenim mrežama ili ostalim mrežnim mjestima poput mrežnih trgovina. Anketni upitnik koji je proveden u svrhu ovog istraživanja bavio se s nekoliko glavnih pitanja:

1. Jesu li studenti upoznati s opasnostima davanja osobnih informacija na internetu?
2. Smatraju li studenti da znaju kako zaštititi svoje osobne podatke na računima mrežnih stranica?
3. Jesu li studenti svjesni kolika je učestalost krađe podataka koja se događa zbog nemarnog korištenja interneta i dijeljenja svojih podataka na stranicama koje nisu provjerene?
4. Jesu li studenti upoznati s metodama zaštite mrežnih stranica te OWASP organizacijom (Otvoreni projekt web aplikacija za sigurnost)?

Upitnik je kreiran putem *Google* obrasca 7. travnja 2023. godine te je u istom mjesecu i proveden tako što je postavljen u razne Facebook grupe za studente gdje su mu studenti mogli pristupiti i ispuniti ga online.

11.1. Uzorak ispitanika

Prema narednim tablicama, moguće je proučiti dobnu skupinu, spol i godinu studija ispitanika te utvrditi koji je to udio ispitanika kada se izrazi u postotcima. Broj ispitanika koji su sudjelovali u ovome istraživanju iznosi 101.

Tablica 1. *Prikaz osnovnih podataka ispitanika (Dobna skupina)*

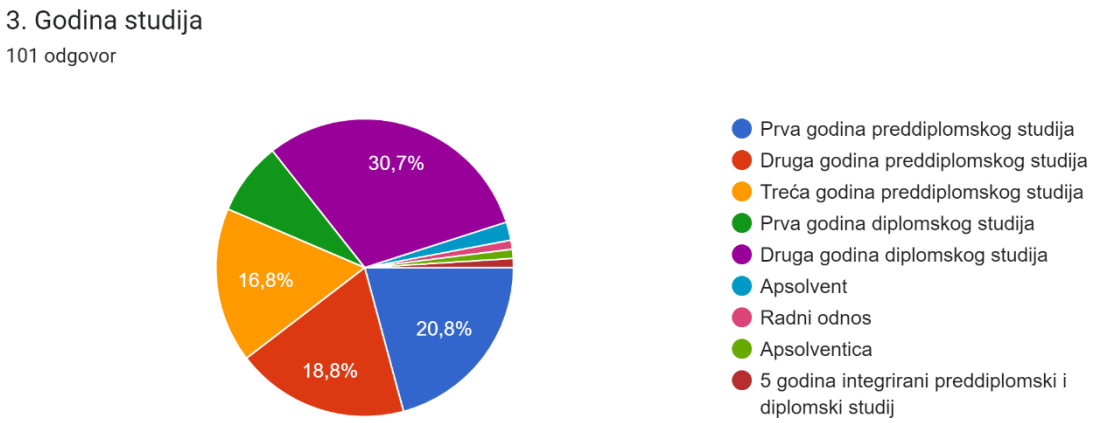
Dobna skupina	Broj ispitanika	Udio ispitanika u postotcima
18-20	27	26,7%
21-23	37	36,6%
24-25	35	34,7%
26-30	2	2%
Ukupno	101	100

Sljedeća tablica prikazuje iznos ispitanika gledajući po njihovom spolu te su iznosi postavljeni i prema brojevima i prema postotcima. Podatci navedeni pod „Ostalo“ odnose se na ispitanike koji se nisu željeli izjasniti.

Tablica 2. *Prikaz osnovnih podataka ispitanika (Spol)*

Spol	Broj ispitanika	Udio ispitanika u postotcima
Muški	17	16,8%
Ženski	80	79,2%
Ostalo	4	4%

Nakon što smo utvrdili osnovne podatke o spolu i dobi ispitanika ovog istraživanja, možemo prijeći na utvrđivanje godine studija i studijskog smjera na koji su ispitanici upisani. Naime, najveći broj ispitanika trenutno pohađa drugu godinu diplomskog studija (30,7%), zatim slijedi prva godina preddiplomskog studija (20,8%), što provedeno istraživanje čini vrlo šarolikim, sudeći po razlici u godinama ispitanika. Nakon njih slijede druga godina preddiplomskog studija (18,8%) i treća godina preddiplomskog studija (16,8%). Najmanji broj ispitanika trenutno pohađa prvu godinu diplomskog studija (7,9%), zatim slijede apsolventi (3%) i ostali (2%). Ispitanici su najčešće studenti Filozofskog fakulteta u Osijeku te studiraju informatologiju, nakladništvo ili informacijske tehnologije na odsjeku za informacijske znanosti. Među ostalim smjerovima našli su se i: psihologija, socijalni rad, biologija, engleski jezik, geografija, pedagogija, poslovna informatika, matematika, računarstvo, marketing, učiteljski studij, kultura u kombinaciji s medijima i menadžmentom, dizajn vizualnih komunikacija, dizajn interakcija, kemija, kineziologija, hortikultura, digitalni marketing, arhitektura, rani i predškolski odgoj i obrazovanje, fizioterapija, kroatistika, šumarstvo, hrvatski jezik, njemački jezik i književnost, povijest umjetnosti, medicinsko-laboratorijska dijagnostika, likovna kultura, sestrinstvo, poduzetništvo, pravo, specijalna zootehnika, logopedija, menadžment marketinga, talijanistika i ruski jezik te brojni drugi smjerovi koji uvelike olakšavaju uvid u problematiku ovog istraživanja, budući da je koncept sadržaja koji studenti slušaju drugačiji na različitim smjerovima.



Graf 1. *Prikaz osnovnih podataka ispitanika (Godina studija)*

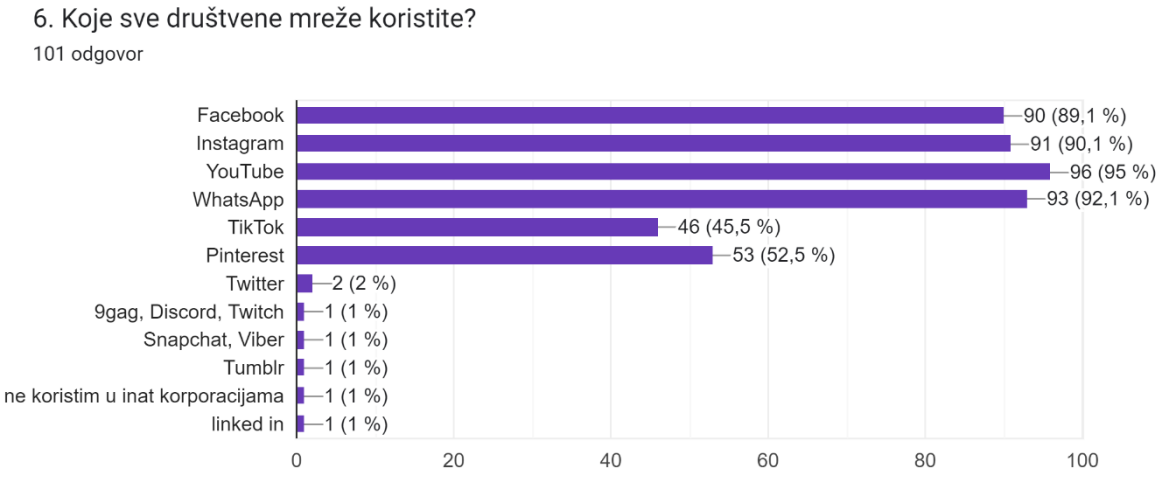
11.2. Ispitanici kao korisnici na internetu

Sljedeće pitanje na koje su ispitanici trebali dati odgovor glasilo je: „Koristite li društvene mreže?“ Na grafičkom je prikazu jasno vidljiv odgovor.

Graf 2. *Prikaz podataka o korištenju društvenih mreža*

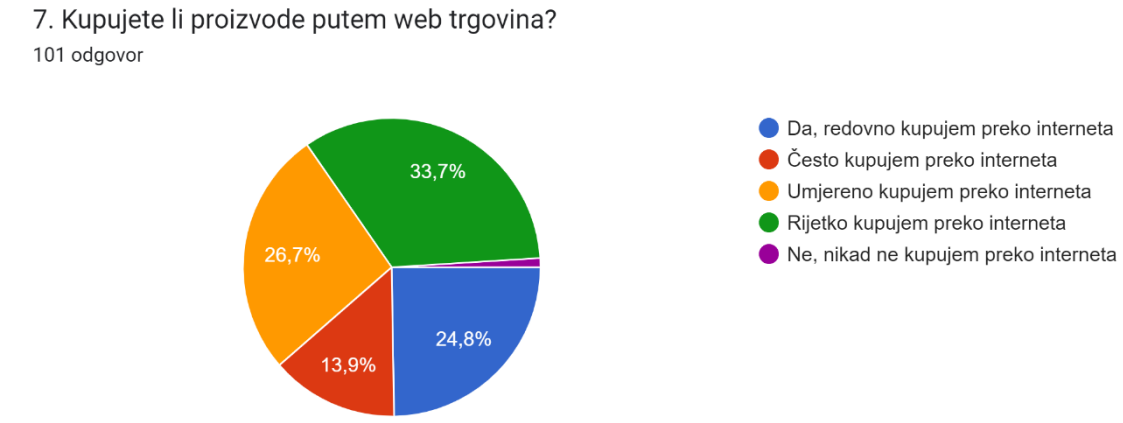
Odmah nakon tog pitanja, ispitanici su trebali označiti i/ili navesti kojim društvenim mrežama se koriste, gdje su se među prva četiri mjesta našli YouTube, WhatsApp, Instagram i Facebook. Zanimljivo je kako se na zadnjem mjestu našao LinkedIn (uz još nekoliko društvenih mreža

poput Tumblr-a, Snapchat-a i Viber-a) koji se smatra jednom od najvećih poslovnih mreža, sudeći prema podatcima iz rujna 2022., koje je objavio sam LinkedIn.[61]



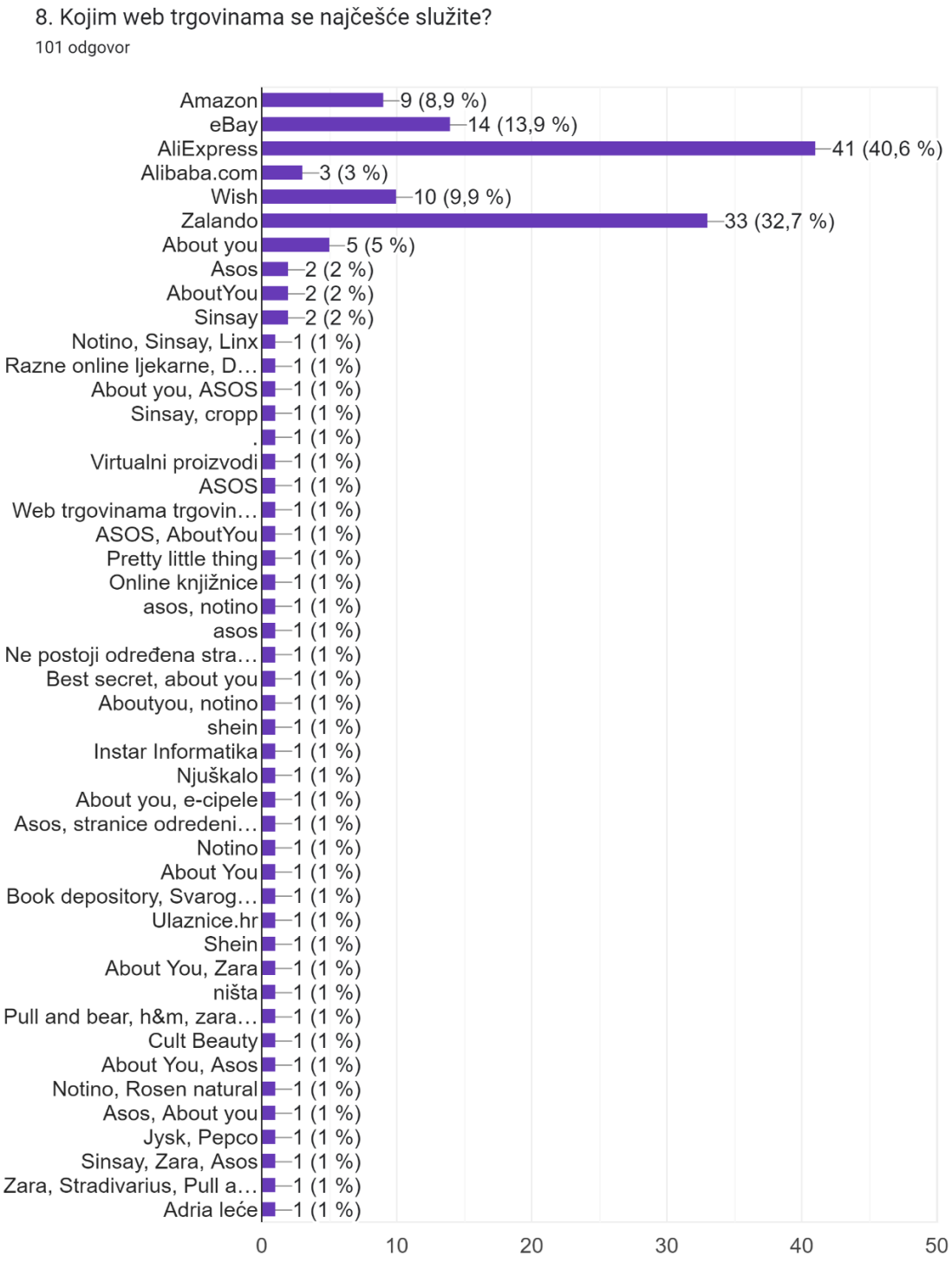
Graf 3. *Prikaz najkorištenijih društvenih mreža*

Osim društvenih mreža na kojima ispitanici provode svoje vrijeme, važno je proučiti kupuju li korisnici proizvode i/ili usluge preko interneta te koje su web trgovine kojima se ispitanici najčešće služe. Sljedeća dva grafa daju jasan prikaz odgovora na postavljena pitanja.



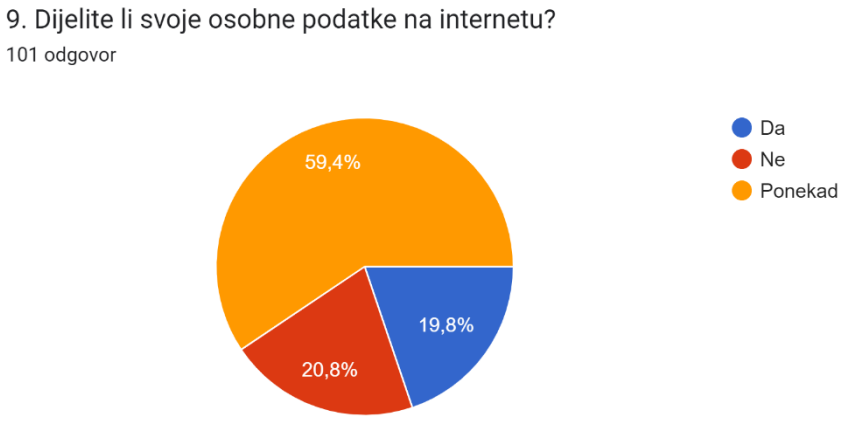
Graf 4. *Prikaz korištenja web trgovina*

[61] Usp. Top 6 Most Popular Social Media Platforms in 2022. URL: https://www.linkedin.com/pulse/top-6-most-popular-social-media-platforms-2022-louise-savoie/ (2023-05-31)

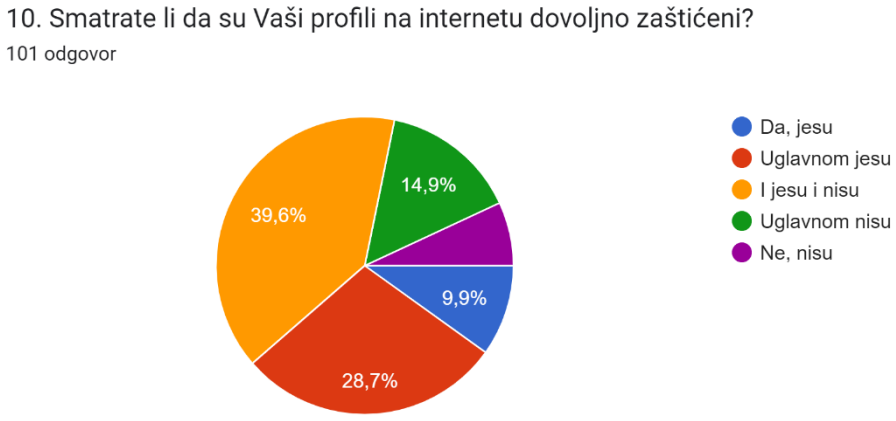


Graf 5. *Prikaz najkorištenijih web trgovina*

Budući da se rijetko može pronaći mrežno mjesto ili aplikacija koja ne uzima osobne podatke svojih korisnika, ispitanici su odgovarali na pitanje o tome dijele li svoje osobne podatke na internetu ili ne. Najveći broj ispitanika izabrao je opciju „Ponekad“, dok su odgovori „Da“ i „Ne“ podjednako raspodijeljeni (*Graf 6.*). Naravno, budući da postoji mogućnost da brojni ispitanici ne mogu utvrditi jesu li dovoljno zaštićeni na internetu ili ne ili možda ne znaju odgovor na to pitanje (*Graf 7.*), može se pretpostaviti da bi se određen postotak onih ispitanika koji su odgovorili s „Ne“, ipak mogao premjestiti u odgovor „Da“.



Graf 6. *Prikaz koliko ispitanici dijele svoje podatke na internetu*



Graf 7. *Prikaz koliko ispitanici smatraju da su njihovi profili na internetu zaštićeni*

Iako veći broj korisnika smatra kako zna zaštititi profile na način da im nitko drugi ne može pristupiti (*Graf 8.*), svakako i dalje velik broj ispitanika smatra kako ne zna zaštititi profile na taj način i tu dolazi do svih problema vezanih uz krađu podataka i hakiranje profila.

Graf 8. *Prikaz znaju li ispitanici zaštititi svoje profile*

Graf 9. *Prikaz jesu li ispitanici ikada ostavili svoje podatke na neprovjerenim stranicama*

Graf 10. *Prikaz jesu li ispitanicima profili ikada bili hakirani*

Kada se usporede odgovori na zadnja tri pitanja, lako se može doći do zaključka kako postoji razlog zašto određeni profili budu hakirani. Iako većina ispitanika smatra kako zna zaštititi svoje profile tako da im nitko drugi ne može pristupiti, gotovo 30% ispitanika priznaje kako su ipak nekada ostavljali svoje podatke na stranicama koje nisu provjerene. Određeni broj ispitanika nije snosio posljedice za neprimjereno ponašanje na internetu, no čak 20% korisnika ipak je bilo hakirano, stoga se može zaključiti da na internetu treba biti vrlo oprezan i ostavljati svoje podatke samo u nužnim situacijama, samo na provjerenim i sigurnim stranicama, aplikacijama i platformama.

Neki od korisnika koji su bili hakirani iznijeli su svoje načine na koje su riješili problem. Jedni su prijavili lažne profile, drugi su mijenjali lozinke uz dodatne autentifikacije, treći su obrisali profile uz pomoć mail-a ili ih na taj način vratili. Neki su se obratili za pomoć čak i korisničkoj podršci ili administratorima stranice. Ipak, nekoliko ispitanika priznalo je kako na kraju nisu uspjeli vratiti izgubljene podatke. Nakon što su se prisjetili svojih primjera, ispitanici su upitani koliki postotak ljudi godišnje bude hakiran te su se brojevi u odgovorima kretali sve od 0,1% pa do 90%, a cilj pitanja bio je potaknuti ispitanike na razmišljanje kako bi shvatili ozbiljnost problema i poduzeli mjere zaštite kako im profili ne bi bili napadnuti. Osim prikupljanja podataka, cilj je istraživanja bio korisnike potaknuti na poduzimanje svih mjera zaštite kako im profili i osobni podatci ne bi bili napadnuti od strane hakera. Prema podatcima iz veljače 2023. godine, prosječno 111,7 milijuna Amerikanaca svake godine bude hakirano[62], dok Amerikanci

[62] Usp. 30 IMPORTANT CYBERSECURITY STATISTICS [2023]: DATA, TRENDS AND MORE. URL: https://www.zippia.com/advice/cybersecurity-statistics/ (2023-05-31)

svake godina izgube 15 bilijuna dolara upravo zbog krađe identiteta.[63] Statistike pokazuju da na globalnoj razini prosječno 30,000 mrežnih stranica bude hakirano svaki dan, od čega je 43% napada ciljano na mala poduzeća.[64]

11.3. Koliko su ispitanici upoznati s vrstama hakiranja i organizacijama koje preveniraju napade

Sljedeću skup pitanja sastojao se od toga jesu li ispitanici čuli za OWASP – Otvoreni projekt web aplikacija za sigurnost (*Open Worldwide Application Security Project*) te jesu li upoznati s nekim od najčešćih vrsta hakerskih napada poput *Man-in-the-middle*, *Evil twin* i *Slowloris* napada. Za OWASP zajednicu čulo je samo 5 ispitanika (5%), za *Man-in-the-middle* napad čulo je 14 ispitanika (13,9%), s *Evil twin* napadom upoznato je 13 ispitanika (12,9%), dok se sa *Slowloris* napadom upoznalo samo 6 ispitanika (5,9%).

Zadnje pitanje bilo je pitanje dugog odgovora, a navodilo je korisnike da predlože neke ideje na koje načine bi riješili današnji problem krađe podataka. Ovo su neki od najzanimljivijih odgovora:

1. „Teško da postoji savršeno rješenje, ali mislim da je većinski dovoljno mijenjati lozinke, paziti koje podatke ostavljamo na kojim stranicama, provjeriti „*cookies*“ i na što pristajemo kada prihvaćamo uvjete korištenja... Također, smatram kako je potrebno više informirati generalnu javnost o opasnostima hakiranja i načinima na koje se mogu zaštititi od takvih napada i što učiniti ako se situacija pogorša.“
2. Da osobi postane najnormalnija stvar koristiti pretplatu za postojeće servise koji blokiraju aktivnosti tog tipa dok su na mreži.
3. Odbit vladi i političarima pristup podacima i smanjit postotak "analitičara" koji se bave proučavanjem uzoraka ponašanja osobe na internetu, smatram ih hakerima. Maknuti kolačiće sa portala i društvenih mreža jer mi ništa apsolutno ne znače personalizirani oglasi niti želim pristajati na njih.
4. Zakonska zaštita osobnih podataka i edukacija korisnika interneta i društvenih mreža.

[63] Usp. How many accounts get hacked a day: 17 more hacking Stats. URL: https://www.vpnhelpers.com/hacking-statistics/ (2023-05-31)

[64] Usp. How Many Cyber Attacks Per Day: The Latest Stats and Impacts in 2023. URL: https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/ (2023-12-11)

5. Stvaranjem jakih zaporki, što manjim dijeljenjem osobnih podataka i provjeravanjem iskustva drugih ljudi o određenoj stranici prije nego podijelimo osobne podatke.
6. Sto manje osobnih informacija dijeliti online, informirati se kako zaštititi svoj profil i ne ulaziti na sumnjive stranice
7. Prvo da pročitamo šta piše i istražimo, a ne da odmah damo informacije
8. Podučiti ljude o *scamovima* sa neta. Maknuti starije ljude sa *sketchy* stranica
9. legitimnije korištenje interneta, poznavanje vještina o zaštiti podataka, razvoj digitalnih kompetencija
10. Mislim da bi trebalo danas mnogo više raditi na osvještavanju djece i roditelja o krađi identiteta i podataka na internetu kroz razne skupove, radionice i predavanja. Osim toga smatram da konkretan problem krađe podataka se može riješiti prijavljivanjem istog policijskoj upravi koja ima adekvatna rješenja i stručnjake za takve situacije.
11. Trenutno nikako, ali kada dođu kvantna računala u široku primjenu, koristiti ih za enkripciju podataka.
12. Kroz edukaciju korisnika o zaštiti njihove privatnosti i sigurnosti na internetu

12. Zaključak

Hakiranje kao pojava nije ništa novo, već se događa svakodnevno i najčešće u negativne svrhe kao što su zarada, stjecanje moći i krađa osobnih podataka kojima se napadači kasnije mogu služiti kako bi nanijeli materijalnu ili emocionalnu štetu osobi koju kibernetički napadaju. Ipak, nasuprot hakerima koji imaju zloćudne namjere (tzv. *black-hat*), postoje i dobroćudni hakeri (*white-hat*) te hakeri koji se nalaze na granici između navedenih (*gray-hat*). Kako se tehnologija iz dana u dan razvija velikom brzinom, jasno je kako se i tehnologije za hakiranje razvijaju jednako tako te postoji sve veći broj raznih virusa i ostalih zloćudnih softvera koji se često razvijaju brže nego što ih je moguće zaustaviti. Problem je što zloćudni softveri djeluju neko vrijeme prije nego ih se otkrije, a kada ih se pokuša zaustaviti ili spriječiti, oni već djeluju na nekoj drugoj razini. Zbog toga je vrlo važno naučiti korisnike kako da se zaštite od potencijalnih prijetnji. Najprije im je potrebno objasniti da nikada ne ostavljaju svoje osobne ili bankovne podatke na stranicama za koje nisu u potpunosti sigurni da su legitimne. Osim toga, važno je napomenuti i kako nikada ne bi trebali koristiti iste pristupne podatke (lozinku) na različitim stranicama. Važno je imati drukčiju lozinku jer ako haker dođe do jedne lozinke, a ta lozinka se koristi i na nekim drugim računima, lako će ukrasti informacije sa svih računa. Stoga, ako se ipak dogodi da je jedan račun hakiran, korisnici se trebaju pobrinuti da nema straha da će još neki od računa isto biti hakiran. Kako postoje zloćudni softveri, jasno je da ih se nekako mora umetnuti u mrežu korisnika žrtve te se ta radnja najčešće događa putem Wi-Fi mreža na koje su korisnici spojeni. Vrlo je važno izbjegavati javne i nezaštićene mreže jer su one odlična podloga za kibernetičke napade. Ipak, ako se korisnici nalaze u situaciji da nemaju izbora i moraju koristiti javne i nezaštićene mreže, važno je upoznati se sa signalima koji odaju da mreža nije legitimna, isto kao i izbjegavati bilo kakve bankovne transakcije na tim mrežama jer hakeri samo čekaju da netko nasjedne na njihov trik. Nadalje, važno se upoznati s vrstama hakiranja, među kojima su neke od najčešćih *man-in-the-middle*, *evil twin*, *slowloris* i DDoS. Kako bi izbjegli bilo koji od napada, važno je shvatiti kako svaki od njih pojedinačno funkcionira, kako ga se može primijetiti te kako ga zaustaviti. Istraživanje koje je na 101 ispitaniku provedeno u svrhu ovog rada pokazalo je da je gotovo 21% ispitanika barem jednom u životu bilo hakirano na društvenoj mreži ili mrežnoj trgovini, a postotak onih koji su čuli za navedene vrste napada iznosi manje od 15%. Budući da velik broj maloljetnih osoba i djece koristi internet i ulazi na svakakve stranice koje im se pojavljuju u šarenim i primamljivim bojama, a možda nisu sigurne,

svijest o ovome problemu trebala bi se proširiti od najmlađih pa sve do najstarijih. Posljedice hakiranja mogu biti kobne za napadnute korisnike te je mjere opreza potrebno provesti još danas.

13. Literatura

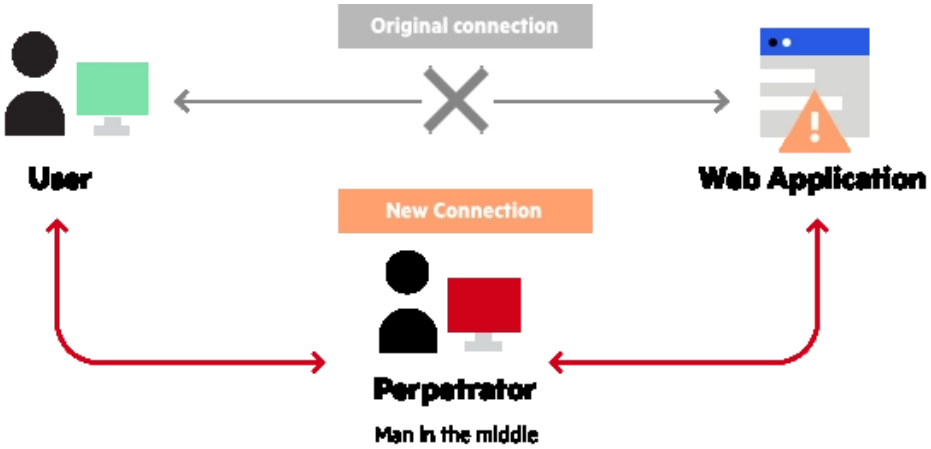
1. Barbovschi, Monica; Velicu, Anca. „“Fraped“ Selves: Hacked, Tagged and Shared Without Permission. The Challenges of Identity Development for Young People on Facebook.“ (2015.)
2. Beaver, Kevin. Hacking For Dummies. 2nd edition. Indianapolis: Wiley Publishing, Inc., 2007. Str. 9-11.
3. B. Schneider, Fred. Cybersecurity Education in Universities. (2013.): str. 3-4. URL: https://ieeexplore.ieee.org/abstract/document/6573305 (2023-12-13)
4. Craigen, Dan; Diakun-Thibault, Nadia; Purse, Randy. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): str. 13-17. URL: http://doi.org/10.22215/timreview/835 (2023-07-02)
5. Cyber Security: Special Issues for Teens. URL: https://mediasmarts.ca/cyber-security/cyber-security-special-issues-teens (2023-07-02)
6. Evil twin attacks and how to prevent them. URL: https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks (2023-07-27)
7. Hacking definition: What is hacking? URL: https://www.malwarebytes.com/hacker (2023-07-18)
8. Haker. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=68094 (2023-07-18)
9. How many accounts get hacked a day: 17 more hacking Stats. URL: https://www.vpnhelpers.com/hacking-statistics/ (2023-05-31)
10. How Many Cyber Attacks Per Day: The Latest Stats and Impacts in 2023. URL: https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day/ (2023-12-11)
11. Ion, I.; Reeder, R. W.; Consolvo, S. „„„…no one can hack my mind“: Comparing Expert and Non-Expert Security Practices.“ *Symposium On Usable Privacy and Security.* (2015.)
12. Jang-Jaccard, Julian; Nepal, Surya. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80, br. 5 (2014.): str. 973-974.
13. Man in the middle (MITM) attack. URL: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (2023-07-27)

14. N. A. A., Rahman; I. H., Sairi; N. A. M., Zizi; F., Khalid. The importance of Cybersecurity Education in School. (2020.): str. 378-382. URL: https://www.semanticscholar.org/paper/The-Importance-of-Cybersecurity-Education-in-School-Rahman-Sairi/86ffd5ed7c2dd7a53fa9797250b8270556faef3e?p2df (2023-12-13)
15. OWASP Top 10 Vulnerabilities. URL: https://www.veracode.com/security/owasp-top-10 (2023-07-19)
16. Računalna sigurnost. *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2021. URL: http://www.enciklopedija.hr/Natuknica.aspx?ID=68380 (2023-07-18)
17. Sarginson, Nic. Why is phising still successful?: Securing your remote workforce against new phising attacks. // Computer Fraud & Security 2020(9): str. 9-12.
18. Slowloris DDoS attack. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/ (2023-07-28)
19. Top 6 Most Popular Social Media Platforms in 2022. URL: https://www.linkedin.com/pulse/top-6-most-popular-social-media-platforms-2022-louise-savoie/ (2023-05-31)
20. What is a Botnet? URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (2023-07-28)
21. What is a DDoS attack? URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (2023-07-28)
22. What is a denial-of-service (DoS) attack? URL: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ (2023-07-28)
23. What is Cyber Security? URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (2023-07-02)
24. 30 IMPORTANT CYBERSECURITY STATISTICS [2023]: DATA, TRENDS AND MORE. URL: https://www.zippia.com/advice/cybersecurity-statistics/ (2023-05-31)

14. Prilozi

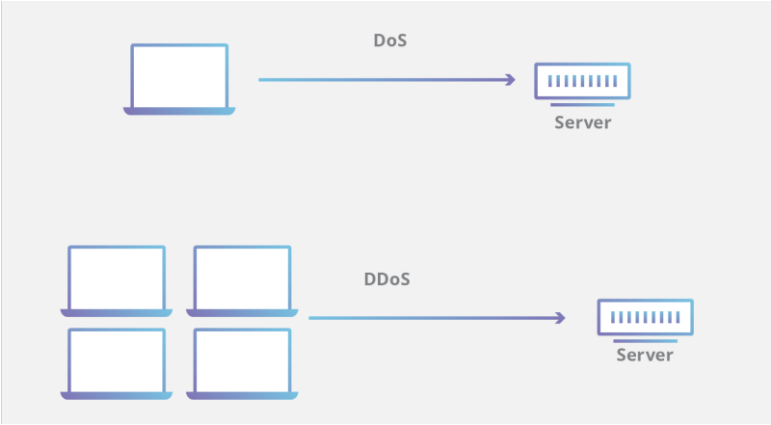
Prilog 1. Prikaz MITM napada

Man in the middle (MITM) attack. URL: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (2023-07-27)



Prilog 2. Razlika između DoS i DDoS napada

What is a denial-of-service (DoS) attack? URL: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ (2023-07-28)



Prilog 3. Pitanja s anketnog upitnika kojeg su ispunjavali ispitanici

Pozdrav svima!

U nastavku se nalazi kratak anketni upitnik koji Vam neće oduzeti puno vremena.

Cilj upitnika je utvrditi:

1. Jesu li studenti upoznati s opasnostima davanja osobnih informacija na internetu?
2. Znaju li studenti zaštititi svoje osobne podatke na računima mrežnih stranica?
3. Jesu li studenti svjesni kolika je učestalost krađe podataka koja se događa zbog nemarnog korištenja interneta i dijeljenja svojih podataka na stranicama koje nisu provjerene?
4. Jesu li studenti upoznati s metodama zaštite mrežnih stranica te OWASP organizacijom (Otvoreni projekt web aplikacija za sigurnost)?

Unaprijed se zahvaljujem na sudjelovanju u ovom istraživanju!

Laura Lišnić,
studentica druge godine diplomskog dvopredmetnog studija nakladništva i informacijskih tehnologija na Filozofskom fakultetu u Osijeku

1. Spol
   - Muško
   - Žensko
   - Ne želim se izjasniti

2. Dob
   - 18-20
   - 21-22
   - 23-25
   - 26-30
   - 30+

3. Godina studija
   - Prva godina preddiplomskog studija
   - Druga godina preddiplomskog studija
   - Treća godina preddiplomskog studija
   - Prva godina diplomskog studija
   - Druga godina diplomskog studija
   - Ostalo_____

4. Studijski smjer?

   _____

5. Koristite li društvene mreže?
- Da
- Ne

6. Koje sve društvene mreže koristite?
- Facebook
- Instagram
- YouTube
- WhatsApp
- TikTok
- Pinterest
- Ostalo_____

7. Kupujete li proizvode putem web trgovina?
- Da, redovno kupujem preko interneta
- Često kupujem preko interneta
- Umjereno kupujem preko interneta
- Rijetko kupujem preko interneta
- Ne, nikad ne kupujem preko interneta

8. Kojim web trgovinama se najčešće služite?
- Amazon
- eBay
- AliExpress
- Alibaba.com
- Wish
- Zalando
- Ostalo_____

9. Dijelite li svoje osobne podatke na internetu?

- Da
- Ne
- Ponekad

10. Smatrate li da su Vaši profili na internetu dovoljno zaštićeni?
- Da, jesu
- Uglavnom jesu
- I jesu i nisu
- Uglavnom nisu
- Ne, nisu

11. Smatrate li da znate zaštititi profile tako da im nitko ne može pristupiti bez Vaše dozvole?
- Da
- Ne

12. Jeste li ikada ostavili svoje podatke na stranicama koje nisu provjerene?
- Da
- Ne

13. Je li Vaš profil na društvenoj mreži / web trgovini ikada bio hakiran?
- Da
- Ne

14. Ako ste bili hakirani, na koji način ste riješili problem? Npr. kako ste i jeste li povratili izgubljene podatke?

_____

15. Što mislite, koliki postotak ljudi godišnje bude hakirano?

_____

16. Jeste li čuli za OWASP organizaciju?
- Da
- Ne

17. Jeste li upoznati s karakteristikama „Man-in-the-middle“ napada?

- Da
- Ne

18. Jeste li upoznati s „Evil twin“ napadom?

- Da
- Ne

19. Jeste li upoznati sa „Slowloris“ napadom?

- Da
- Ne

20. Imate li prijedlog na koji način biste riješili današnji problem krađe podataka?

_____