Online prijetnje i tehnike sprječavanja hakerskih napada

Zorkić, Valentino

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Preddiplomski sveučilišni studij

Valentino Zorkić

Online prijetnje i tehnike sprječavanja hakerskih napada

Online threats and hacking prevention techniques

Završni rad

Opatija, 2023.

SVEUČILIŠTE U RIJECI
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU, OPATIJA

Preddiplomski sveučilišni studij
Poslovna ekonomija u turizmu i ugostiteljstvu
Studijski smjer: Menadžment u turizmu

Online prijetnje i tehnike sprječavanja hakerskih napada

Završni rad

Kolegij: Sigurnost informacijskih sustava
Mentor: izv.prof.dr.sc. Ljubica Pilepić Stifanich

Student: Valentino Zorkić
Matični broj: 24808PO19

Opatija, Lipanj 2023.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Valentino Zorkić	**24808**
(ime i prezime studenta)	(matični broj studenta)

Online prijetnje i tehnike sprječavanja hakerskih napada

(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor završnog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, 2023.

Valentino Zorkić

Potpis studenta

Sažetak

Online prijetnje svakodnevnica su modernog svijeta. Internetom kola veliki broj informacija i korisnika. Upravo zbog toga nerijetko su podatci korisnika meta hakera. Cyber kultura podrazumijeva društvene uvjete koji su nastali kao rezultanta široke upotrebe računalnih mreža u cilju komuniciranja, zabave ili poslovanja. Prilikom vršenja napada hakeri se koriste različitim alatima i neprestano smišljaju nove tehnike kako bi došlo do informacija koje mogu dalje unovčiti. Smatra se kako su motivi hakera primarno bili znatiželja ili dostupno slobodno vrijeme, no u današnje vrijeme hakere motivira novčana zarada od podataka koje pribave hakiranjem. Osim navedenog, kako bi haker izvršio napad on prolazi kroz nekoliko postupovnih faza, a to su faza pripreme, ilegalna faza te faza izvršenja. Kao odgovor na sve češće napade hakera postoje brojne tehnike kojima se žele spriječiti hakerski napadi i otkloniti prijetnja. Dakle, kroz analizu online prijetnji te načina za njihovo sprječavanje žele se prikazati ispravni načini postupanja na internetu u cilju zaštite uređaja i informacija koji se nalaze na njima.

Ključne riječi: hakeri, napadi, sigurnost

SADRŽAJ

1. Uvod

Čovjek u svojoj svakodnevnici korištenja Internetom izložen je svakojakim prijetnjama i napadima od strane hakera. Naime, online prijetnje i napadi smatraju se ozbiljnim problemom u recentno vrijeme. Takva vrsta napada može rezultirati vrlo ozbiljnim posljedicama za pojedince ali i za društvo. Primjeri njihovog razmjera može varirati od napada na pojedine osobe i njihove informacije do nestanka električne energije, kvarova razne opreme te povređivanja nacionalnih sigurnosnih tajni. Dakle, može doći do poremećaja unutar telefonskih i računalnih mreža ili do potpunih paraliza pojedinih sistema, što posljedično dovodi do nedostupnosti podataka.

Danas se svakodnevno počinje nekoliko zločina potpomognutih internetom poznatih kao kibernetički kriminal u različitim oblicima kao što su lažna elektronička pošta, pornografija, krađa identiteta, hakiranje, internetsko uznemiravanje, spam, lažiranje bankomata, piratstvo i krađa identiteta. Stoga, potrebno je razraditi efektivne tehnike kako bi se spriječili napadi od strane hakera. Eksponencijalni porast ovog kriminala u društvu postao je snažan problem koji se ne smije zanemariti. Utjecaj ove vrste kriminala može se osjetiti na živote, gospodarstvo i međunarodni ugled nacije.

1.1. Predmet rada

Predmet rada su online prijetnje te tehnike za njihovog sprječavanje kao i fokus na sigurnost u području interneta.

1.2. Svrha i cilj rada

Svrha rada jest navest postojeće online prijetnje te sve postupke koji se danas primjenjuju za njihovo sprječavanje.

Cilj rada jest da se kroz opisivanje online prijetnji i postupanja njihovog sprječavanja prikaže obrazac za ispravan način postupanja na internetu u cilju zaštite vlastitog uređaja i informacija koji su na njemu pohranjeni.

1.3. Znanstvene metode

Prilikom sastavljanja ovog završnog rada korištene su razne znanstvene metode, a među kojima su metoda deskripcije, metoda analize i sinteze, povijesna metoda te metoda komparacije.

1.4. Struktura rada

Rad će primarno započeti s opisivanjem online prijetnji. Cyber kultura i etika hakera sljedeće je poglavlje rada. Zatim će rad pomnije opisati sigurnost na internetu. Unutar ovog poglavlja primarno će se definirati kibernetika i informacija sigurnost. Potom će se opisati razvoj kibernetičke sigurnosti. Kibernetički kriminal posljednje je poglavlje ovog dijela rada. Sljedeće poglavlje opisati će hakerske napade te tehnike sprječavanja hakerskih napada. Rad završava zaključnim spoznajama.

2. Online prijetnje

Internetske prijetnje izlažu ljude i računalne sustave ozljedama na internetu. U navedenu kategoriju spada širok raspon opasnosti, uključujući dobro poznate prijetnje poput krađe identiteta i računalnih virusa. Međutim, drugi oblici prijetnji, poput izvanmrežne krađe podataka, također se mogu smatrati dijelom ove skupine.

Online prijetnje nisu ograničene na online aktivnosti, već u konačnici uključuju internet u pojedinog fazi za nanošenje štete. Iako nisu sve online prijetnje stvorene namjerno, mnoge su namijenjene ili mogu imati potencijal da uzrokuju sljedeće (Kaspersky, 2023):

- Access acquisition (akvizicija pristupa) – neovlašteni ili neželjeni ulazak u privatno računalo i/ili mrežne usluge,
- Access denied (pristup odbijen) – sprječavanje ulaska u računalo i/ili mrežne usluge,
- izlaganje privatnih podataka bez dopuštenja, kao što su fotografije, podatci o računima i osjetljive informacije povezane s državom ili
- neovlašteno ili neželjeno korištenje računalnih i/ili mrežnih usluga.

Posljednjih godina, spektar prijetnji na webu je doživio značajan porast. Tehnologije poput pametnih uređaja i brzih mobilnih mreža omogućile su uvijek povezan vektor zlonamjernog softvera, prijevara i drugih komplikacija. Također, usvajanje weba u područjima poput komunikacije i produktivnosti putem Interneta stvari (IoT – Internet of Things) nadmašilo je svijest korisnika o sigurnosti.

Obzirom na činjenicu kako se nastavljamo sve više oslanjati na web za svakodnevni život, on će nastaviti eksponencijalno rasti kao atraktivna opcija napada za zlonamjerne stranke. Pogodnost i nedostatak opreza prilikom korištenju weba smatra se osnovnim problemom koji i dalje predstavlja nove rizike za privatnost i sigurnost. Dok su mete obično računalne, ljudske žrtve u konačnici doživljavaju trajne učinke online prijetnji.

Kada se pojavi prijetnja s weba, određene se okolnosti pojedine okolnosti se trebaju poklopiti kako bi se ono smatralo prijetnjom u sigurnosnom smislu. Naime, postoji nekoliko osnovnih komponenti svake web prijetnje, a koji su (Kaspersky, 2023):

- motivi prijetnje koji daju agentu prijetnje razlog ili cilj za nanošenje štete jer neke prijetnje ne djeluju namjerno ili djeluju autonomno i stoga mogu biti bez motiva,
- prijetnje su bilo što ili bilo tko tko može negativno utjecati te koji koristi Internet kao smjer prijetnje ili samu metu,
- ranjivosti koje uključuju sve slabosti u ljudskom ponašanju, tehnološke sustave ili druge resurse koji mogu dovesti do štetnog iskorištavanja ili incidenta te
- ishodi prijetnje koji se smatraju negativnim rezultatima kada prijetnja djeluje protiv jedne ili više ranjivosti.

Tzv. agenti prijetnji u pravilu su ljudi sa zlim namjerama. Osim navedenog, agenti također mogu biti bilo što čime se manipulira kako bi se djelovalo u korist izvornog agenta prijetnje. Međutim, neki agenti prijetnje, poput destruktivnih prirodnih događaja, djeluju u cijelosti bez ljudske intervencije.

Slijedom navedenog, vrste agenata prijetnji podrazumijevaju (Kaspersky, 2023):

- neljudski agenti: primjeri uključuju zlonamjerni kod (virusi, zlonamjerni softver, crvi), prirodne katastrofe (vremenske, geološke), komunalne kvarove (električni, telekomunikacijski), tehnološki kvar (hardver, softver) i fizičke opasnosti (toplina, voda, udarac);
- namjerni ljudski agenti: na temelju zlonamjerne namjere, a mogu biti unutarnji (zaposlenici, izvođači, obitelj, prijatelji, poznanici) i vanjski (profesionalni i amaterski hakeri, akteri i agencije iz nacionalne države, konkurentske korporacije);
- slučajni ljudski agenti: na temelju ljudske pogreške, a slično namjernim prijetnjama, ova vrsta može uključivati unutarnje i vanjske agente te
- ljudski agenti koji su bazirani na nemaru i na temelju nemarnog ponašanja ili sigurnosnih propusta (ova kategorija također može uključivati unutarnje i vanjske agente).

Pored toga, ranjivosti mogu biti točke slabosti gdje se netko ili nešto može manipulirati. Ranjivosti se mogu smatrati web prijetnjom i zabrinutošću koja omogućuje druge prijetnje. Navedeno područje obično uključuje neki oblik ljudske ili tehničke slabosti koja može dovesti do prodora, zlouporabe ili uništenja sustava.

Ishodi prijetnji mogu dovesti do otkrivanja privatnih podataka, prevarenih korisnika, prekida korištenja računalnog sustava ili oduzimanja privilegija pristupa. Online prijetnje često uzrokuju sljedeće posljedice (Kaspersky, 2023):

- oštećenje reputacije (gubitak povjerenja klijenata i partnera, stavljanje na crnu listu tražilica, ponižavanje, kleveta itd.),
- prekid rada (zastoj u radu, uskraćivanje pristupa web uslugama kao što su blogovi ili oglasne ploče i dr.) te
- krađa (financijski podaci, podaci o identitetu, osjetljivi podaci o potrošačima i dr.).

Internetske prijetnje koje najviše zabrinjavaju putuju internetom kako bi napale više sustava. Ovi agenti prijetnji često koriste kombinaciju ljudske manipulacije i tehničkih naredbi kako bi došli do svojih ciljeva. Online prijetnje ove prirode koriste brojne komunikacijske kanale interneta za širenje. Veće prijetnje koriste globalni internet kako bi odgovorile na prijetnje, dok se ciljanije prijetnje mogu izravno infiltrirati u privatne mreže.

Obično se te prijetnje distribuiraju putem usluga temeljenih na webu. Zlonamjerni akteri te prijetnje radije postavljaju na mjesta gdje će korisnici često s njima komunicirati. Javne web stranice, društveni mediji, web forumi i e-pošta često su idealni za širenje web prijetnji. Korisnici su pogođeni kada koriste zlonamjerne URL-ove, preuzimanja ili daju osjetljive informacije web stranicama i pošiljateljima poruka. Navedeni angažman također može izazvati infekciju i širenje web prijetnji drugim korisnicima i mrežama. Nije nepoznanica da nedužan korisnik samostalno nesvjesno postane prijetnja (Kaspersky, 2023).

3. Cyber kultura i etika hakera

Tijekom ljudske povijesti veliki broj tehnologija se rapidno razvijao. Ipak, brzina širenja Interneta se rijetko može uspoređivati s razvojem bilo koje druge tehnologije. Utjecaj interneta je dalekosežan te privlači veliki broj ljudi. Putem interneta došlo je do značajnih pomaka u ljudskoj komunikaciji i interakciji, brzini i praktičnosti očekivanja, umrežavanju i dr. Cyber kultura smatra se novom kulturom unutar informacijskog društva koja je zastupljena u recentnom društvu (Milardović 2010, 77).

Pod pojmom cyber kulture podrazumijevaju se pojedini kulturni proizvodi i praksa koja je nastala iz internetske i informacijske tehnologije. Također, navedeni pojam može se ticati i supkultura koje su karakteristične za umjetnosti i računalne hobije. Diljem svijeta virtualna stvarnost kao pojam iznimno je poznata. Primjer toga jest marketing putem interneta (Terranova 2004, 133). Naime, putem internetskog marketinga danas se vrši prodaja usluga i roba te se smatra jednim od najvažnijih oblika marketinga u moderno vrijeme.

Cyber kultura ima značajan domet na svim razinama, od lokalne do globalne i to posebice u društvenom umrežavanju, društvenom označavanju, distribucijskom stvaranju i dr. (Gomez-Diago 2012, 59). Takve rutine odlikuju predanošću, empatijom i sudjelovanjem te njima ljudi postaju odgovorni jedni za druge te su izravno uključeni u cyber prostor. Navedeno je izvršilo značajan utjecaj na način razmišljanja ljudi te na čovjekov identitet.

Internet na značajan način vrši utjecaj na svakodnevno funkcioniranje ljudi diljem svijeta. Skoro svaka stvar koji ljudi danas čine je na neki način povezana s korištenjem interneta. Stoga, valja zaključiti kako je život bez interneta nezamisliv jer su brojne čovjekove aktivnosti povezane s internetom (naručivanje hrane, kupnja bijele tehnike, dijeljenje života i sl.). Prije nastanka interneta informacije su se mnogo sporije širile, dok je danas to mnogo ubrzano (Gomez-Diago 2012, 60).

Cjelokupni Internet jest transformiran jer je u ranijem periodu ono bila mreža statičnog oblika koja je bila kreirana da prenosi malu količinu podataka između dva terminala. Dakle, smatrala je svojevrsnim spremištem male količine informacija unutar kojeg je sadržaj održavan i

objavljivan od strane kodera. U recentno vrijeme internetom se šire goleme količine informacija koje se učitavaju i preuzimaju.

Pojedinci se u današnje vrijeme otežano štite od ljudi koji se bave pregledom tuđih podataka jer je veliki broj informacija javno dostupan te postoji vrlo niska razina anonimnosti. Međutim, unutar ovakve komunikacijske okoline korisnici mogu pribaviti veliku količinu informacija koje im trebaju, a sve u cilju olakšanja životnih procesa poput pronalaženja posla, učenja, studiranja, kupovine pojedinih usluga ili proizvoda i dr. (Gomez-Diago 2012, 60). Stoga, iznosi se zaključak kako Internet i cyber okolina imaju i dobre i loše konotacije. Buduća predviđanja ističu kako ljudska svakodnevnica neće biti zamisliva bez korištenja internetskih tehnologija te da će doći do smanjenje potrebe za radnom snagom.

Iako je u današnje vrijeme teško dati bilo kakva predviđanja, u cyber sferi svakako se očekuju rapidne promjene na gotovo dnevnim razinama. Diljem interneta svakim dan je na raspolaganju niz ponuda, društvenih mreža, internetskih stranica koje su sve naprednije. Također, uređaji i tehnologija brzo napreduje i omogućuje korištenje interneta vrlo brzo i efikasno. Promjene su evidentne na dnevnim razinama te se programeri natječu koji će na tržište plasirati nešto inovativno (Davčev i Leškovska-Ačkovska 2008, 76). Postoje tendencije za daljnjim povećanjem brzine širenja protoka informacija, a najnovija mreža jest 5G. Pored navedenog, uočen je i evidentan pad u cijenama informatičkih tehnologija i usluga jer zbog ubrzanog razvoja neki proizvodi niti ne stignu plasirati na pojedino tržište. Ipak, virtualne trgovine su iznimno popularne danas te se unutar domene internetskih tehnologija u recentno vrijeme uvrštavaju i multimedijalni sadržaji poput filmova i glazbe.

Steven Levy tvrdio je kako se jednim od bazičnih principa etike hakera smatra slobodna i neograničena mogućnost pristupanja računalima i što se sve može naučiti u njima o svijetu koji nas okružuje. Naime, ako pojedinoj stvari se ne može otvoreno pristupiti, upravo je zadatak samog hakera da pronađe način na koji će doći do nje (Levy 1994, 2). Raymond je definirao hakersku etiku kao obvezu hakera da razmjenjuje stručna znanja s ostalima te da napravi slobodan oblik softvera kako bi se mogao u bilo kojem trenutku olakšati pristup računalima i informacijama (Raymond 1998, 234). Pekka je naveo kako postoje ukupno tri kategorije motivacija kod hakera. Nazvao ih je Linusov zakon. Naime, pojedinac se razvija kroz nekoliko kategorija, a to su društven (socijalan) život, opstanak i razonoda. U cilju napredovanja pojedinac mora proći kroz sve faze. Navedeni je razvoj primjenjiv i na hakere. Haker računalo

koristi u cilju razonode, ne u egzistencijalne svrhe. Putem programiranja hakera prati osjećaj zadovoljstva (Pekka 2002, 44).

Zatim valja objasniti pojam netike. Pod navedenim pojmom označava se etika mreže te se odnose na hakerov odnosa prema mreži društva koje je međusobno umreženo kao i na obrasce ponašanja u pogledu komunikacije na pojedinoj mreži. Tijekom 1990-tih godina osnovana je međunarodna nevladina organizacija koje je branila privatnost, slobodu govora te prava potrošača koji se koriste Internetom. Na primjeru naše države zanimljivo je istaknuti kako su se hakeri protivili zabranama i cenzurama koje su se zbivale na području Jugoslavije, a posebice zato jer je vladala zabrana emitiranja ratnih izvještaja bilo kakve brste bilo kojim medijem. Naime, iz Srbije je bio izvršen napad na poslužitelje NATO-a. Dakle, vlade teže na vršenju nadzora stanovnika, a koji se provodi na način da se vrši kontrola posjećenih stranica i sadržaja poruka. Poznato je kako web poslužitelji svoje korisnike identificiraju uz pomoć kolačića (engl. cookies). Ipak, nije svaki haker zlonamjeran. Postoje oni koji vode brigu oko etičnog načina ponašanja u današnjim informacijskim tehnologijama i koji se pripravni da ukažu na nedostatke i greške u ponašanju korisnika unutar informacijskih sustava.

Pod pojmom etičnih hakera podrazumijevaju se one osobe koje su položile sigurnosni ispit da se bave sprječavanjem problema u području informatičke sigurnosti (Babić 2009, 121). Smatra se kako je razlika između crnog i bijelog hakiranja autoriziranje klijenata. Naime, hakerska etika podrazumijeva želju za slobodnom pristupu željenim informacijama, a slijedom čega se omogućuje i popravljanje pogrešaka i njihova identifikacija. Putem otvorenih sistema moguće je vršit razmjene opreme te informacija. Ipak birokracija se često javlja kao kočnica ovakvih vrsta međusobnog djelovanja. Motiv etičkih hakera jest vrlo često ukazivanje ne pogreške u sigurnosnim sferama. Ipak, moderni hakeri danas sve češće to fina zbog financijskih pobuda te hakiranje je postalo izvorom nelegalnog načina zarade čime se nadišla inicijalna tendencija za stjecanjem znanja i osjećajem uzbuđenja.

4. Sigurnost na Internetu

Gotovo da nema ograničenja u onome što se može učiti u online prostoru. Internet omogućuje brz pristup informacijama, komunikaciju diljem svijeta i još mnogo toga. Nažalost, internet predstavlja dom određenim rizicima, poput zlonamjernog softvera, neželjene pošte i krađe identiteta. Ukoliko pojedina osoba želi na mreži ostati sigurna, morat će razumjeti te rizike i naučiti kako ih izbjeći.

Naime, kada se koristi internet, pojedina osoba može biti povezana s tisućama drugih računala s kojima vrši razmjenu informacije i različitih podataka, a unutar kojih su uključeni i osobni podatci. Pri tome, iznimno je važno osigurati da je uređaj pojedinca, njegovi podatci i njegova privatnost što sigurnija. Većina ljudi pohranjuje mnogo osobnih podataka na svoja računala. Ukoliko se računalo ne zaštiti na ispravan način dok je na mreži, moguće je da osobni podaci mogu biti ukradeni ili izbrisani bez znanja korisnika.

Sigurnost na internetu smatra se posebnim aspektom koji ima širok koncept unutar kojeg potpadaju računalna i kibernetička sigurnost. Pod navedenim fokus se stavlja na posebne prijetnje te razinu ranjivosti koja se očituje tijekom korištenja interneta, a koje je povezano s internetskim pristupom. Naime, sigurnost na internetu sačinjena je od različitih sigurnosnih taktika čiji je cilj zaštiti transakcije i aktivnosti koje se putem interneta provode. Navedene taktike imaju za cilj štiti svoje korisnike od različitih prijetnji poput hakiranja e-mail adrese, različitih korisničkih sustava, web lokacija ili računalnih sistema. Također, pružaju zaštitu prilikom krađe identiteta ili osobnih podataka od strane hakera (Vuković 2012, 16).

Internetska sigurnost središnji je aspekt kibernetičke sigurnosti, a uključuje upravljanje kibernetičkim prijetnjama i rizicima povezanim s internetom, web-preglednicima, web-aplikacijama, web-mjestima i mrežama. Primarna svrha internetskih sigurnosnih rješenja je zaštititi korisnike i korporativnu IT imovinu od napada koji putuju preko interneta.

Okvir kibernetičke sigurnosti u osnovi je dobrovoljno vodstvo za organizacije koje im pomaže u upravljanju svojim programom i mjerama kibernetičke sigurnosti. Postoje mnogi okviri kibernetičke sigurnosti, iz različitih organizacija, s različitim izgledom, fokusom i jezikom. Organizacije koje ih razvijaju mogu imati različite poslovne modele.

Smatra se kako postoje ukupno četiri stupa kibernetičke sigurnosti, a koji su (Bandler, 2023):

- unaprijediti znanje i svijest,
- poboljšanje sigurnosti računalnih uređaja,
- poboljšanje sigurnosti podataka i
- poboljšanje sigurnosti mreža i korištenja interneta.

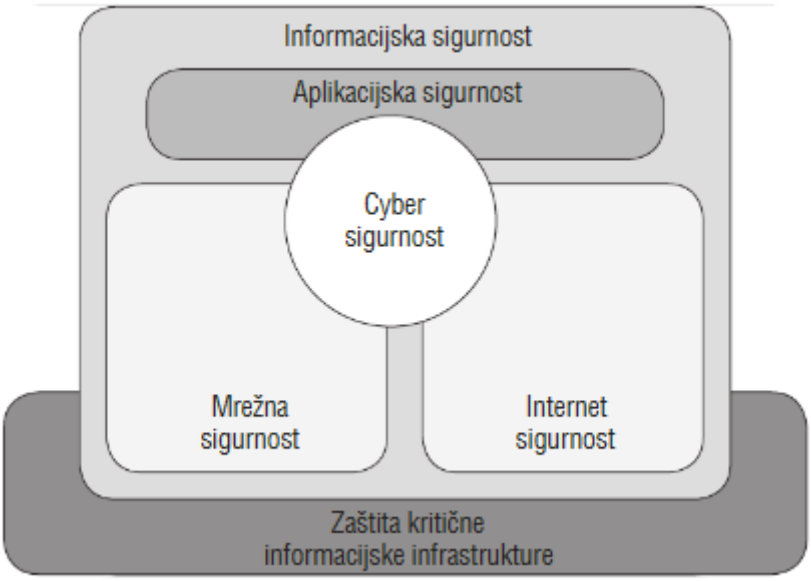
Prethodno navedena četiri stupa dio su kontinuiranog ciklusa poboljšanja. Načela su razumljiva bez specijalizirane obuke u informacijskoj tehnologiji ili informacijskoj sigurnosti. Slijedom navedenog, znanje je na prvom mjestu jer potiče donošenje dobrih odluka za upravljanje i zaštitu informacijskih sredstava i sustava. Znanje pomaže kada se suočite sa sumnjivom e-poštom za prijenos sredstava ili klik na vezu. Stoga, usvajanje okvira ne osigurava sigurnost, učinkovitost niti usklađenost. Ipak, smatra se kako je potrebno provoditi određene mjere i obrasce ponašanja na internetu u cilju otklona online prijetnji i sigurnost boravka na Internetu (Bandler, 2023).

4.1. Kibernetika i informacijska sigurnost

U kontekstu internetske sigurnost valja definirati pojam kibernetike. Naime, ona se smatra skupom raznih znanstvenih disciplina te procesa koji se koriste tijekom vođenja ili upravljanja kompleksnih sustava. u nastavku rada prikazan je odnos kibernetičke sigurnosti sa drugim vrstama sigurnosti (Hamidović 2015, 83).

Cilj informacijske sigurnosti jest pružiti zaštitu u pogledu privatnosti korisnika te omogućiti da su informacije trajno dostupne. Ipak, potrebno je napravit distinkciju između informacijske i kibernetičke sigurnosti. Naime, pod kibernetičkom sigurnosti podrazumijevamo skupinu raznih praksi i obrazaca koji će se koristiti kako bi se pružila sigurnost od napada na internetu. S druge strane, informacijske sigurnost predstavlja samo jednu od poddisciplina unutar kibernetičke sigurnosti (Vuković 2012, 18). U nastavku na Slici 1. prikazan je koncept informacijske sigurnosti.

Slika 1. Prikaz informacijske sigurnosti



Izvor: Hamidović 2015, 83

Nadalje, pod aplikacijskom sigurnošću podrazumijevamo postupak koji se vrši u cilju primjenjivanja ispravnih mjerenja i kontrole nad organizacijskim aplikacijama. Mrežna sigurnost ima zadatak da primjenjuje, kreira i konsekutivno radi na mreži. Nadalje, internetska sigurnost ima zadatak da štiti usluge koje su povezane internetom. Internetska sigurnost čini niz taktika sigurnosnog karaktera koje imaju za cilj zaštitu transakcija i aktivnosti koje se odvijaju na internetu i one također korisnike štite od raznih cyber prijetnji kao što su provaljivanje u tuđe e-mail adrese, te računalne sisteme.

Obzirom na činjenicu da ljudi Internet, a posebice društvene mreže, smatraju personalnim alatom za komuniciranje, iznimno je bitno da štite vlastite informacije koje su im na tim mrežama pohranjene. Naime, plasiranjem takvih informacija na Internet može doći do neovlaštenih proboja i pristupanja istima u cilju oštećivanja druge strane.

Opasnosti u području interneta su goleme, od samog kibernetičkog kriminala pa sve do raznih objava na društvenim mrežama koje mogu imati iznimno negativne posljedice. Ipak, smatra se kako su kibernetički kriminal i hakeri najveća opasnosti na internetu. Postoji niz prijetnji s kojima se ljudi danas suočavaju prilikom korištenja interneta. (Spitzer 2018, 14).

Sigurnost na internetu kroz povijest je imala dinamičan razvoj. Prvo računalo je kreirano 1943. godine. Dva desetljeća nakon njegovog kreirana kibernetički su se napadi smatrali izazovnima. Naime, velikim elektroničkim strojevima mogao je pristupiti iznimno malen broj ljudi, a oni među sobom nisu bili umreženi. Dakle, tek je nekoliko osoba znalo što se raditi s pojedinim računalima pa slijedom toga niti nisu postojale prijetnje u toj sferi. Teorija koja je opisivala računalne viruse pojavila se 1949. godine. Tada je John von Neumann, računalni pionir, iznio pretpostavku o mogućnosti razmnožavanja kompjutorskih programa. Koncem 1950-tih godina evidentirano je telefonsko prisluškivanje. Navedeni pristup bio je temeljen na otmici protokola koji su imali zadatak da telekom inženjerima omoguće vršenje poslova na mreži s udaljene lokacije u cilju vršenja besplatnih poziva čime se izbjegavala naplata istih. Ovi počinitelji ubrzo su stekli popularnost kao zajednica ljudi koja se bavi izdavanjem novina. Unutar ove skupine uvršteni su i Steve Jobs te Steve Wozniak (Chadd 2020, 1).

Zatim se tijekom šezdesetih godina pojavila inicijalna referenca za maliciozno hakiranje unutar Instituta tehnologije u Massachusettsu. Za navedeni period je poznato kako su tadašnja računala bila iznimno velika te su bila zaključana unutar soba koje su imale regulirane temperature. Ovi strojevi bili su iznimno skupi i njima je pristupao ograničen broj programera. Uočeni su pokušaji provaljivanja u sustav od strana osoba koje su imale pristup njemu, a najčešće je bilo riječ o studentima. U ovaj etapi takve vrste napada nisu imali niti geografske, niti političke a niti komercijalne svrhe. Hakeri su u ovo vrijeme u pravilu bili znatiželjni i željeli su unaprijediti sustave kako bi efektivnije i brže radili. U 1967. godini studenti su pozvani od strane IBM-a na testiranje njihovog računala. Nakon inicijalnog testiranja pristupačnih dijelova studenti su imali mogućnost da istraže dublje sfere koje su uključivale učenje jezika sustava, a za što je bilo potrebno ulaženje u druge dijelove navedenog sustava. IBM-u je ovo bilo od iznimnog značaja jer je zaključeno kako studenti zapravo uništili sam sustav slijedom čega su izgrađeni defenzivni načini razmišljanja i mjere koje će u kasnijem periodu biti neizbježne. Protekom vremena proizvodila su se sve manja računala te je njihova cijena postepeno opadala. Stoga, veliki broj poduzeća je svoja novčana sredstva uložilo u tehnologije koje su vršile pohranu podataka. Navedene pohranjene podatke štitile su lozinke (Chadd 2020, 1).

4.2. Razvoj kibernetičke sigurnosti

Samo poimanje kibernetičke sigurnosti pojavio se tijekom 1972. godine kroz projekt naziva ARPANET (engl. The advanced research projects agency network). On se smatra pretečom interneta. Bobo Thomas, istraživač, stvorio je kompjuterski program kojeg je nazvao Creeper. Navedeni se program mogao kretati kroz ARPANET mrežu te je iza sebe ostavljao trag kretanja. Trag je nosio tekst „ja sam Creeper, ulovi me ukoliko možeš“. Izumitelj e-maila, Ray Tomlinson, izradio je program Reaper koji se bavio pronalaskom Creepera i potom ga brisao. Smatra se kako je program Reaper prva prava inačica antivirusa, ali i prvim programom koji se samostalno replicirao, a što znači da je postao ujedno i prvi računalni crv. Slijedom navedenog, postalo je iznimno bitno ponuditi rješenja za sve izazove koje su donijele nove tehnologije jer je rapidno porastao broj ljudi i poduzeća koji su imaju telefone u cilju kreiranja udaljenih mreža. Svaki hardver koji je bio povezan shvaćao se kao nova točka ulaza koja je trebala zaštitu. S početkom frekventnijeg korištenja računala došlo je i do porasta umrežavanja. Vlade država su tada shvatile da je sigurnost u tim područjima iznimno bitna te da bi pristupanja mreži koja nisu autorizirana bila pogubna.

Stoga, došlo je do kreiranja prvih zaštita namijenjenih za računala. Kreirali su ih ARPA i ESD zajedno sa Air Fore-om Sjedinjenih Američkih Država te nizom drugih organizacija koje su zajedno radile na izgradnji jezgre koja je jamčila sigurnost računalnih sustava. navedeno je poznato pod nazivom HIS level 68. Postojao je i projekt ARPA-e koji je proučavao zaštitu i sigurnost pojedinih operativnih sustava. Istraživanje se provodilo na način da se vršila identifikacija automatiziranih tehnika za detekciju potencijalnih prijetnji unutar pojedinog software-a. Kibernetička sigurnost i njezin koncept razvili su se do sredine 1970-ih godina. Tijekom 1979. godine Kevin Mitnick, tada šesnaestogodišnjak, hakirao je ARK kompjuter koji je bio smješten unutar korporacije koja se bavila digitalnom opremom koja se koristila tijekom gradnje opravitnih sustava. Mitnick je hakirao na način da je stvorio kopiju tog softvera (Chadd 2020, 2).

Tijekom 1980. godine zabilježen je povećan broj napada od velike važnosti i to na AT&T, CSS te nacionalni knjižnicu Los Almos. U 1983. godini pojavljuje se upotreba izraza kao što su računalni virus i trojanski konj. Tijekom trajanja hladnog rata došlo je do razvoja kibernetičke špijunaže. Tijekom 1985. godine Ministarstvo obrane Sjedinjenih Američkih Država je

obznanilo koji su kriteriji za ostvarenje sigurnosti pojedinog računalnog sustava te unutar toga sadržana su pravila sukladno kojima se može izraditi procjena nivoa povjerenja u pojedini softver te o sigurnosnim mjerama koje su eventualno potrebne. Usprkos svemu tome tijekom 1986. godine Marcus Hess, njemački haker, spojio su na ARPANET korištenjem mrežnog usmjerivača (engl. gateway) te je u svoj pohodu hakirao oko 400 vojnih kompjutera u cilju prodaje dobivenih informacija KGB-u. uskoro su brojni korisnici shvatili kako se povećanja kod veličine datoteka mogu shvatiti kao pokušaji hakiranja. Stoga, smanjena memorija pojedinog operativnog sustava ukazuje na pokušaj hakiranja (Chadd 2020, 3).

Godina 1987. zabilježena je kao početna za komercijalan antivirus. Radilo se o McAfee-u i o Norton Antivirusnim programskim rješenjima. Do konca 1988. godine veliki broj tvrtki diljem svijeta etabiliralo je sferu kibernetičke sigurnosti, a primjer toga je Avast. Dakle, tvrtke su shvatile kako imaju mogućnost reagiranja samo na napada koji su postojani jer je bilo teško u rad pustiti nadograde (engl. update).

Prvi polimorfan virus kreiran je 1990. godine. Pod njime podrazumijeva se kod koji će mutirati za vrijeme čega će se originalan algoritam čuvati bez izmjene u cilju izbjegavanja detektiranja. Naime, baza prvih antivirusa bila je digitalan potpis koji je vršio usporedbu zapisa s bazom koja je sadržavala potpise virusa. Zbog toga često je dolazilo do upozorenja koja su bila lažna (engl. false positives). Korisnici su bili frustrirani jer su ovi postupci koristili veliku količinu računalne energije. U 1992. godini došlo je do pojave prvog anti-virusnog programa. Do konca 1996. godine brojni virusi su se koristili novim tehnologijama i različitim inovativnim metodama poput metoda prikrivanja, polimorfnosti ili korištenjem makro virusa što je antivirusnim tvrtkama postavilo brojne izazove. Tijekom 1990-tih godina rapidno se povećao broj virusa i malware-a sa deset tisuća na više od 5 milijuna. Tek se 2007. godine pojavila nova metoda naziva heuristička detekcija koja je imala sposobnost da se nosi s golemom količinom varijanti virusa. Započelo je korištenje generičkih potpisa u cilju detekcije virusa unatoč činjenici što bi prijetnje bile sakrivene u beznačajnom kodu. Koncem 1990. godine putem e-maila utkan je put za nove viruse. U 1999. godini došlo je do puštanja Melisa virusa. Melisa virus ulazio je na računala korisnika uz pomoć word dokumenta slijedom čega bi poslao kopije putem e-maila na prvih 50 redoslijedno navedenih adresa koje je osoba imala u Microsoft Outlook-u. Utvrđena je šteta iznosila oko 80 milijuna dolara te Melisa virus do recentnog vremena je ostao jedan od virusa koji se najbrže širio (Chadd 2020, 4).

Kada je došlo do pojave interneta sve je veći broj organizacija i domova, tada su kibernetički kriminalni na raspolaganju imali sve veću količinu uređaja i softvera na koje su mogli vršiti svoje napade jer je simultano došlo i do povećanja količine podataka. Tijekom 2001. godine došlo je do pojave novih oblika prijetnji u sklopu kojih nije bilo potrebno da korisnik preuzme datoteku već je posjet zaraženoj stranici bio dovoljan. Razvijanjem napada koji su se koristili rupama unutar sigurnosnih mjera rezultiralo je beskorisnošću antivirusnih programa. Glavni izazov se nalazio u činjenici što je antivirusni program iznimno usporavao pojedino računalo. Rješenje ovog problema bilo je premještanje tog softvera u oblak (engl. cloud).

Tijekom 2007. godine sigurnost (engl. security) se kombinirala s cloud tehnologijom i s istraživanjem prijetnji (engl. threat inteligence) unutar jednog antivirusnog proizvoda. Kao nova inovacija pojavila se i OS-sigurnost, a koja podrazumijeva kibernetičku sigurnost koja je implementirala u pojedini operativan sistem i koja je pružala dodatnu razinu zaštite. U 2010. godini došlo je do povećanja napada i to posebice u području nacionalne sigurnosti te su njihove posljedice brojile štetu u milijunima dolara. WannaCry ransoware je u 2017. godini u jednom danu uspio infiltrirati u 230 000 računala.

Aktualan proces digitalizacije omogućuje hakerima brojne prilike kako bi mogli izvesti napade na sustave. Slijedom navedenog, sve je više tražen kibernetički oblik sigurnosti koji je baziran na pojedini posao. Tijekom 2011. godine od strane Avasta objavljen je prvi proizvod za korištenje od strane poslovnih organizacija. S razvojem brojnih antivirusnih programa paralelno se razvijao i broj metoda kojeg su osmišljavali kibernetički kriminalci, a sve kako bi mogli izvršiti napade na sustave. Među poznatim metodama navode se socijalni inženjering te multi-vector napadi ipak, unutar kibernetičke sigurnosti nove generacije koriste se diferencirani pristupi u cilju povećanja identifikacije novih oblika prijetnji, a čime simultano dolazi do smanjenja napada koji su „false-positive“. Pod navedenim metodama valja spomenuti zaštitu u stvarnom vremenu, analiziranje ponašanja pojedine mreže, autentifikaciju putem više faktora i dr. (Chadd 2020, 5).

Postepeni razvoj računalnih tehnologija te povećanje brzine interneta rezultiralo je povećanjem površina na kojima se mogu dogoditi napadi. Dakle, sa većim brojem računala i aplikacija koje su međusobno povezane na pojedinog mreži, raste i broj napada. Poznata je činjenica da se informacije smatraju svojevrsnim oblikom imovine koji ima vlastitu vrijednost. Navedenu činjenicu hakeri u cijelosti žele iskoristiti. Stoga, kibernetička sigurnost u današnje vrijeme je

postala vrlo bitna sfera. Pored toga, čuvanje podataka je postalo iznimno izazovno za domove kao i za poduzeća.

4.3. Kibernetički kriminal

U novije vrijeme naše se društvo sve više oslanja na internet i druge alate informacijske tehnologije za uključivanje u osobnu komunikaciju i obavljanje poslovnih aktivnosti. Dok ti razvoji omogućuju ogroman dobitak u produktivnosti, učinkovitosti i komunikaciji, oni također stvaraju rupu u zakonu koja može potpuno uništiti organizaciju. Korištenje interneta također ima i prednosti i nedostatke. Najgori nedostatak interneta je kibernetički kriminal. Izraz kibernetički kriminal može se koristiti za opisivanje bilo koje kriminalne aktivnosti koja uključuje računalo ili internetsku mrežu. Ovaj izraz se koristi za zločine kao što su prijevara, krađa, ucjena, krivotvorenje i pronevjera, u kojima se koriste računala ili mreže (Omodunbi et. al. 2016, 37).

Naime, kibernetički kriminal definiran je kao vrsta zločina počinjenog od strane kriminalaca koji se koriste računalom kao alatom i internetom kao vezom kako bi postigli različite ciljeve kao što su ilegalno preuzimanje glazbenih datoteka i filmova, piratstvo, slanje neželjene pošte i voli. Kibernetički kriminal razvija se iz pogrešne primjene ili zlouporabe internetskih usluga. Koncept kibernetičkog kriminala je povijesni. Otkriveno je da se prvo objavljeno izvješće o kibernetičkom kriminalu dogodilo na glavnom računalu 1960-ih. Budući da ta računala nisu bila spojena na internet ili s drugim računalima, kazneno djelo su počinili poslodavci unutar tvrtke, stoga je preusmjereno na računalni kriminal, a ne na kibernetički kriminal (Maintanmi et. el. 2013, 46).

Opasnosti u području kibernetike sežu od infiltracija u ključne strukture te prikupljanje podataka pa sve do različitih krađa identiteta i grubih napada. Pod online prijetnjama podrazumijevamo koje za cilj imaju uništiti, omesti ili ukrasti određene podatke u digitalnom obliku. Različiti računalni virusi, povreda i infiltracija podataka te napadi uskraćenjem usluge neki su od primjera najčešćih rizika. Obzirom da su ljudi u recentno vrijeme sve više ovisni o tehnologiji, cyber opasnosti i prijetnje su značajno napredovale te su one sve više prisutne. Naime, one predstavljaju veliki rizik za razna poduzeća te osobe. Smatra se kako je primaran korak u obrani protiv cyber prijetnji i rizika njihovo razumijevanje (Taylor 2023, 1).

Naime, veliki broj korisnika interneta, a posebice društvenih mreža, nije svjesno velikog broja sigurnosnih rizika koji su postojani u navedenim mrežama. Unutar te sfere dolazi do redovnih kršenja privatnosti, krađa identiteta i dr. Slijedom navedenog, nedavne studije su pokazale kako korisnici interneta spremno i s lakoćom iznose privatne i osobne podatke poput kuće adrese, datuma rođenja, e-mail adrese i sl. Ukoliko navedene informacije dođu u pogrešne ruke, mogu biti korištene da se nanese šteta takvim korisnicima u virtualnom svijetu (Fire el al. 2014, 2019). Današnji kibernetički kriminal je sve veća prijetnja svim korisnicima interneta i računala, kao i društvu općenito. Stoga su vlade raznih zemalja, policijski odjeli i drugi obavještajni odjeli sada strogi i reakcionarni prema ovim novonastalim cyber prijetnjama i širenju cyber kriminala (Sekhar Biswal, Kumar Pani 2021, 1).

U posljednjih nekoliko godina cyber napadi su postali sve češći te na njih gotovo nitko nije imun, od pojedinaca pa do državnih institucija. Opasnosti koje su povezane sa povredom podataka i cyber napadima u konstantnom su porastu obzirom da se veliki broj osjetljivih informacija čuva i dijeli online putem. Cyber napadi mogu rezultirati nestankom električne energije, kvarovima na vojnoj opremi te povredom državnih tajni. Također, može doći i do krađe vrijednih i osjetljivih podataka poput medicinskih dokumentacija. Može doći do poremećaja u računalnim i telefonskim mrežama ili se u cijelosti mogu paralizirati sustavi i to na način da podatke učine nedostupnima. Cyber prijetnje mogu uvelike utjecati na redovno funkcioniranje svakodnevnog života današnjice. Naime, rizici cyber sigurnosti prožeti su kroz svaku organizaciju i ne potpadaju uvijek pod izravnu kontrolu IT odjela. Čelnici u poslovnoj sferi koračaju naprijed sa svojim digitalnim poslovnim inicijativama te na dnevnoj razini donose odluke koje povezane sa tehnološkim rizicima (Taylor 2023, 1).

Slijedom navedenog, potrebno je analizirati koji su uzročnici cyber napada. Razumijevanje podrijetla napada na pojedinu cyber sigurnost se smatra ključnim korakom kod kreiranja tehnika za ublažavanje i prevenciju cyber napada. Kao prvi uzrok može se navesti ljudska pogreška. Putem pojedinačnih pogrešaka kao što su klikanje na stranice koje kradu identitet ili nepoštivanjem sigurnosnih mjera, korisnici vlastite sustave izlažu potencijalnim cyber napadima. Sljedeći uzrok cyber napada može biti zastarjeli softver jer softver i sigurnosni sustav koji nije ažuriran može mrežu izložiti cyber prevarantima koji takvu ranjivost mogu iskoristiti. Neadekvatna autentifikacija također je uzrok cyber napada jer ukoliko autentifikacija nije dvofaktorska tada se sustav može izložiti napadima. Uzrok cyber napada može biti i napad

jedne zemlje protiv druge u cilju prekida ili nanošenja štete bazičnoj infrastrukturi poput bankarskih sistema ili električne mreže.

5. Hakerski napadi i tehnike sprječavanja hakerskih napada

Internet je učinio svijet manjim na mnoge načine, ali nas je također otvorio utjecajima koji nikada prije nisu bili tako raznoliki i tako izazovni. Brzo kako je rasla sigurnost, svijet hakiranja je rastao brže. Kibernetička sigurnost u prvom redu podrazumijeva da tvrtke koje pružaju računalstvo u oblaku rade to i samo to kako bi te tvrtke bile iznimno dobro zaštićene najnovijom vrhunskom tehnologijom šifriranja. Raspon operacija kibernetičke sigurnosti uključuje zaštitu informacija i sustava od velikih kibernetičkih prijetnji. Ove prijetnje imaju mnoge oblike. Kao rezultat toga, držanje koraka sa strategijom i operacijama kibernetičke sigurnosti može biti izazov, osobito u vladinim i poslovnim mrežama gdje, u svom najinovativnijem obliku, kibernetičke prijetnje često ciljaju na tajnu, političku i vojnu imovinu nacije ili njezinog stanovništva (Nandhini 2018, 125).

Vrlo često zbog neznanja i površnih načina zaštite brojne fizičke i pravne osobe mogu biti žrtvama napada hakera. Ukoliko nije poznato na koji je način napad izvršen tada nije moguće niti odrediti na koji će se način pojedinci obraniti od istog. Hakerski napadi potpadaju u sferu računalnog kriminala. Računalni kriminal može se definirati kao niz kaznenih djela počinjenih na pojedinom području kojima se u svojoj ukupnosti izravno utjecalo na dostupnost, korištenje te cjelokupnost programske, podatkovne ili tehničke baze pojedinog kompjuterskog sistema ili na tajnost podataka u digitalnom obliku (Dragičević 2004, 113).

Hakerski napad izvodi se sa zlonamjernom namjerom kada akter prijetnje pokuša iskoristiti ranjivost ili slabost u sustavu ili pojedincima u organizaciji. Ovi napadi prijete krađom, izmjenom, uništenjem, onesposobljavanjem ili dobivanjem pristupa ili iskorištavanjem neovlaštene imovine. Sprječavanje provale u pojedinu mrežu i njezine sustave zahtijeva zaštitu od raznih hakerskih napada. Za svaki napad mora se primijeniti i upotrijebiti odgovarajuća protumjera kako bi se odvratilo od iskorištavanja ranjivosti ili slabosti (Swanagan 2022, 1).

Pored navedenog, kod hakerskih napada postoje različiti ciljevi te metode koje se koriste prilikom napada. Kao ciljevi spominju se korisničke lozinke i njihovo otkrivanje, otkrivanje raznih informacija i podataka, napad na datoteke koje sadrže različite identifikacijske informacije, otkrivanje podataka o kreditnim karticama, te napadi koji onemogućuju korištenje kompjuterskog sustava. Pri tome valja istaknuti kako pojedini haker će najviše biti zainteresiran

za otkrivanjem lozinki, informacija, brojeva kreditnih kartica, podataka, identifikacijskih brojeva te web stranica (Dragičević 2004, 115).

Šteta koja nastaje kompjuterskim kriminalom može biti u financijskom obliku, nefinancijskom obliku te u kombiniranom obliku. Kod štete u financijskom obliku kao cilj pojedinog kriminalnog djela navodi se pribavljanje vlastite financijske koristi ili na nekog drugog. Šteta u nematerijalnom obliku kao cilj kriminalnog djela navodi otkrivanje različitih podataka ne nedopušten način. Kod kombiniranog oblika štete kompjuterskog kriminala cilj pojedinog kriminalnog dijela ima financijsku i materijalnu komponentu (Babić 2009, 128).

Smatra se kako je slabo kontroliranje interneta okolnost koja hakerima olakšava njihove napade. Na internetu ne postoje službe koje mogu sprječavati prijestupnike. Ipak, vrlo malen broj osoba i poduzeća prijavljuje napade hakera. Upravo se zbog toga hakeri iznova ohrabruju za njihove pothvate. Primarni razlozi neprijavljivanja hakerskih napada su neznanje i loša reputacija. Pod neznanjem smatra se činjenica kako brojna poduzeća nisu niti svjesna da su napadnuta. Naime, kada bi poduzeća ili osobe na vrijeme saznale da su pod napadom hakera tada bi moglo doći do šteta manjih razmjera. Osim toga, mjesto na kojemu je izvršen hakerski napad može se ponovno koristiti ukoliko ne dođe do otkrića napada. Također, smatra se kako je jedini način da pojedina web lokacija bude jest da osigura da su sve druge web lokacije sigurne. Daljnji argument zbog kojeg se ne vrše prijave hakerskih napada jest strah od loše reputacije, a koji se pogotovo odnosi na poduzeća. Naime, u slučaju poduzeća vrlo vjerojatno bi došlo do gubitka povjerenja i prestanka korištenja usluge od strana korisnika u situaciji otkrivanja da je poduzeće bilo žrtva napada hakera. ipak, evidentno je kako upotreba interneta u komercijalne svrhe te u poslovne svrhe i dalje konsekutivno raste neovisno o manama i nedostatcima sustava. smatra se kako investiranjem u sigurnost se ne daje nikakva direktna korist. Naime, korist u sferi sigurnosti biti će vidljiva nakon što poduzeće ili osoba budu napadnuti od strane hakera te kada se utvrdi je li se nastala šteta mogla umanjiti ulaganjem u sigurnost sustava (Dragičević 2004, 120).

Također, u posljednjih dvadeset godina nije se osmislila dostupna dnevna tehnologija obrane protiv hakerskih napada osim antivirusa. Ipak, u današnje vrijeme virusi nisu u velikoj mjeri aktivni jer je hakerima danas cilj podatke oteti i unovčiti, dok ih virusom uništava. Ljudi danas veliku dozu povjerenja ulažu u tehnologije, a velika većina te sfere nije pod zakonskom regulacijom. Jedno od općih pitanja u razvoju cyber-zakona je priroda samog cyber-prostora,

koji je nov i mlad. Tradicionalni zakoni stoga neće biti učinkoviti u borbi protiv raznih vrsta aktivnosti koje se provode u kibernetičkom prostoru (Bhasin 2007, 1624). Još jedan problem zaštite koji se pojavljuje jest nedovoljno razumijevanje principa na koji rade današnji uređaji. Ljudi posjeduju televizije, mobilne uređaje i računala bez znanja o tome na koji se način vrši uspostava poziva ili na koji način dolazi do nastanka fotografija koje se pojavljuju n takvim uređajima.

5.1. Hakerski alati i napadi

Primarno se hakerski napadi mogu podijeliti sukladno nekoliko različitih tipova, a to su:

- mrežni napadi,
- bežični napadi,
- napadi zlonamjernim softverom i
- napadi društvenim inženjeringom.

Mrežni napadi su pokušaji iskorištavanja ranjivosti ili slabosti mreže ili njezinih sustava uključujući poslužitelje, vatrozidove, računala, usmjerivače, preklopnike, pisače i još mnogo toga. Cilj mrežnog napada može biti krađa, izmjena ili uklanjanje pristupa vrijednim podacima ili rušenje mreže. Naime, napadi na mreže postali su češći posljednjih godina djelomično zato što mala i srednja poduzeća ne ulažu dovoljno brzo u osiguranje svojih sustava. Kao rezultat toga, hakeri napadaju tvrtke jer je njihove sustave često lakše kompromitirati. Ostali razlozi uključuju porast haktivizma (engl. hacktivism), upotrebu vlastitog uređaja (engl. Bring your own device – BYOD) i aplikacije temeljene na oblaku. Uobičajeni mrežni napadi uključuju: uskraćivanje usluge (DoS), distribuirano uskraćivanje usluge (DDoS), napadi prekoračenja međuspremnika, Ping napadi, SYN Poplava, DNS pojačanje, Stražnja vrata, Lažiranje, Štrumpf napad, TCP/IP otmica, Čovjek u sredini napada, Replay napadi, DNS trovanje, ARP trovanje, Domain Kiting, Tiposquatting, napadi na strani klijenta (Swanagan 2022, 2).

Bežični napad uključuje prepoznavanje i ispitivanje veza između svih uređaja povezanih na pojedinu WiFi mrežu. Izraz WiFi odnosi se na bežičnu mrežnu tehnologiju koja koristi radiovalove za uspostavljanje bežičnih mrežnih veza. Zbog prirode WiFi-a i njegovih metoda za pružanje pristupa mreži, zlonamjerni hakeri često odlučuju prodrijeti u neku organizaciju ugrožavanjem njezine WiFi mreže i odgovarajućih infrastrukturnih uređaja. Pri tome, domovi

i privatni korisnici su također u opasnosti, posebno zbog porasta broja uređaja i uređaja povezanih s internetom stvari (engl. Internet of Things-IoT). Uobičajeni bežični napadi uključuju: emanaciju podataka, ometanje, bluetooth ranjivosti, komunikacija kratkog dometa, deautentifikacija i rastavljanje, njuškanje i prisluškivanje, bežični napadi ponavljanja, WPS napadi, WEP/WPA napadi, IV Napad, TKIP napad, WPA2 napadi te usluge upravljanja ranjivošću poduzeća (Swanagan 2022, 3).

Zlonamjerni softver ili engl. Malware svaki je dio softvera koji je izrađen s namjerom nanošenja štete podacima, uređajima ili ljudima. Sustavi zaraženi zlonamjernim softverom pokazat će simptome kao što su sporiji rad, slanje e-pošte bez radnje korisnika, nasumično ponovno pokretanje ili pokretanje nepoznatih procesa. Postoje tisuće varijanti zlonamjernog softvera i različitih vrsta zlonamjernog softvera među kojima su najpoznatiji virusi, keyloggeri, crvi, trojanci, ransomware, logička bombe, adware, špijunski softveri, rootkitovi i dr. (Swanagan 2022, 4).

Posljednji tipovi su napadi društvenim inženjeringom. Društveni inženjering pokušaj je manipuliranja korisnikom da daje osjetljive informacije kao što su vjerodajnice korisničkog računa, prijenos sredstava ili osobni podaci. Smatra se kako je ovaj oblik cyber napada jedan od najpopularnijih za postavljanje zlonamjernog koda na mrežu. Prema dostupnim podacima, 98% cyber napada oslanja se na društveni inženjering. Većina ljudi je upoznata s tehnikama krađe identiteta putem e-pošte jer je to postalo bitna komponenta svakog programa za kibernetičku sigurnost i često je uključeno u druga IT rješenja. Uobičajene vrste napada društvenim inženjeringom uključuju krađu identiteta putem e-pošte, pretekstiranje, tailgating, whaling i dr. (Swanagan 2022, 4).

Prilikom hakerskih napada hakeri se koriste različitim metodama. Među najpoznatijim metodama ubrajaju se varanje ili maskiranje (engl. deception, masquerading), ispitivanje, spoofing ili pogađanje (engl. guessing, probe), socijalni inženjering (engl. social engineering), prisluškivanje (engl. eavesdropping, wiretapping), pretraživanje (engl. scanning), druženje (engl. socializing), optički način špijuniranja (engl. optical spying), programske manipulacije te kompromitiranje (engl. compromising).

Maskiranje ili varanje tiče se lažnog načina predstavljanja u cilju stjecanja povjerenja. Pod ispitivanjem se na slijepo pogađaju nečije lozinke. Spoofing se tiče raznih metoda koje se

koriste kako bi se došlo do traženih podataka i to na način da se iskoriste slabosti koje ima neki IP protokol. Pretraživanjem se vrši označavanje određenog broja nedopuštenih pokušaja da se dođe do raznih informacija ili proboja u sustava korištenjem alata koji su automatizirani. Društveni inženjering se može pojaviti u obliku engl. shoulder surfinga unutar kojeg haker ima izravan uvid tijekom postupka unosa lozinke. Putem prisluškivanja telefonskih razgovora hakeri mogu doći do željenih informacija. Pojmovi engl. dustbin diving, scavenging shvaćaju se kao pretraživanje tuđeg smeća ili raznih bilješki kako bi se pronašle različite lozinke. Optički način špijuniranja jest presretanje, snimanje ili promatranje elektromagnetskih zračenja s ekrana računala. Programskim manipulacijama poput engl. pocket sniffera ili trojanskih konja može se doći do lozinki korisnika. Putem iskorištavanja i podmićivanja haker može pridobiti veliki broj informacija za podvođenje kriminalnih radnji. Postoje tzv. crni i bijeli hakeri. Crni hakeri imaju negativne motive, dok bijeli hakeri žele sa svojim spoznajama spriječiti i zaštiti korisnike od napada crnih hakera.

Postoji nekoliko bazičnih koraka koje hakeri poduzimaju prilikom vršenja napada. Pod prvim korakom smatra se pasivan izvid. Unutar ovog koraka haker na pasivan način vrši prikupljanje različitih informacija (engl. information gathering) koje su povezane s metom napada. Putem pasivnog napada ne dolazi do izravnog pristupanja, no njime se on osigurava. Pasivan izvid može se vršiti putem razgovora ili promatranjem. Cilj je dobiti relevantne podatke. Njuškanje (engl. sniffing) smatra se još jednim oblikom pasivne vrste napada koje odlikuje promatranjem prometa koji se odvija na pojedinoj mreži. Unutar toga postoje posebni programi koji se bave izvlačenjem i pohranom lozinki. Sljedeći je korak aktivnog upoznavanja ili skeniranja. U ovom koraku nastoji se otkriti koje su slabosti unutar pojedinog sustava. Ukoliko se pronađu greške u sferi sigurnosti tada se prelazi u nadolazeću fazu, a koja se tiče iskorištavanja pojedinog sustava. U fazi u kojoj se iskorištava sustav dolazi do pristupanja sustavu unutar kojeg haker sebi podiže opseg ovlasti ili onemogući korisnicima pristupanje podatcima. Unutar ove faze haker vrlo često koristi jedno računalo kako bi podmetnulo napad na drugo računalo i time sakrio vlastite tragove. U ovoj fazi evidentiraju se napadi na razne aplikacije, konfiguracije te operativne sustave. Nadolazeća faza tiče se prijenosa programa unutar koje haker u sustav učitava programe koji će mu koristiti kako bi se omogućio veći pristup ili može učitati alate kojima će kompromitirati druge sustave. Potom slijedi faza preuzimanja podataka koja je karakteristična za velike skupove podataka tijekom postupka špijunaže. U fazi održavanja pristupa sustavu koriste se tzv. stražnja vrata, a koja mogu biti korisnički račun koji je dodan i putem kojeg se haker priključuje pojedinom sustavu, a može biti i trojanski konj ili neka

sistemska datoteka koja je prepisana u verziju sa sakrivenim značajkama (engl. system file). Posljednja faza jest ona u kojoj se sakrivaju tragovi, čisti se aktivnosti te se isključuje iz pojedinog sustava (Cole 2001, 34).

Nadalje, evidentno je kako je sigurnost iznimno bitan dio svake organizacije i svake pojedine osobe. Vrlo često ne postoji svijest o mrežnoj sigurnosti sve do trena dok ista ne bude žrtva napada. Ipak, postoje različite vrste napada koje hakeri koriste, a koje će biti analizirane u nastavku rada.

Prvo svakako valja spomenuti računalne viruse. Računalni virus jest softverski program koji se može širiti s jednog računala na drugo računalo ili s jedne mreže na drugu mrežu bez znanja korisnika i izvodi zlonamjerne radnje. Ima sposobnost oštetiti podatke, uništiti datoteke, formatirati tvrde diskove ili učiniti diskove nečitljivima. Postoji mnogo načina na koje se virus ili računalni virus mogu širiti, a koji su klik na izvršnu datoteku, posjet zaraženoj web stranici, pregledavanje oglasa zaražene web stranice, zaraženi prijenosni uređaji za pohranu, kao što su USB pogoni, otvaranje neželjene e-pošte ili privitka e-pošte te preuzimanje besplatnih igara, alatnih traka, medijskih player-a i drugih uslužnih programa sustava.

Zatim slijedi napada zvan engl. Man in the middle (čovjek u sredini). Čovjek u sredini vrsta je kibernetičkog napada u kojem se zlonamjerni napadač ubacuje razgovor između pošiljatelja i primatelja, oponaša i pošiljatelja i primatelja te u konačnici dobiva pristup njihovim informacijama. Unutar ovog napada, čini se da i pošiljatelj i primatelj normalno komuniciraju. Pošiljatelj ne razumije da je primatelj zlonamjerni napadač i napadač koji pokušava pristupiti ili urediti poruku prije ponovnog slanja do primatelja. Uobičajeni oblik napada Čovjeka u sredini je komunikacija putem interneta, poput e-pošte, pregledavanja weba, društvenih medija itd. unutar ove sfere, engl. spoofing ili prijevara se smatra još jednom vrstom hakerskom napada gdje napadač pokušava upotrijebiti računalo, uređaj ili mrežu kako bi prevario druge mreže sustava maskirajući se u legitimnog korisnika. Postoji nekoliko vrsta lažiranja unutar kojih je IP spoofing jedna je od najčešćih vrsta napada. Naime, IP spoofing je tehnika napada gdje haker dobiva pristup računalnoj mreži slanjem poruka računalu s IP adresom. Zatim ta IP adresa pokazuje da poruka dolazi od pouzdanog domaćina tako da izgleda kao da je autentična čime se ostvaruje namjera prijevare. U IP spoofing napadu, haker prvo pronalazi IP adresu pouzdanog hosta, a zatim mijenja zaglavlja paketa tako da se čini da paketi dolaze s tog pouzdanog domaćina (Touhid 2019, 2).

Uskraćivanje usluge (engl. Denial-of-Service) je napad koji isključuje stroj ili mrežu i čini ih nedostupnima korisnicima. Obično preplavljuje ciljani sustav zahtjevima sve dok se normalni promet ne može obraditi, što rezultira uskraćivanjem usluge korisnicima. Navedeno se događa kada napadač spriječi legitimne korisnike u pristupu određenim sustavima, uređajima ili drugim mrežnim resursima.

Potom valja istaknuti engl. Malware. Malware se sastoji od softverskog programa ili koda koji su razvili hakeri. Dizajniran je za nanošenje velike štete sustavima ili za dobivanje neovlaštenog pristupa računalnoj mreži. Zlonamjerni softver isporučuje se u obliku veze ili datoteke putem e-pošte te zahtijeva od korisnika da klikne na vezu kako bi pokrenuo zlonamjerni softver. Postoje različite vrste zlonamjernog softvera kao što su računalni virusi, crvi, trojanski konj, špijunski softver i drugo (Touhid 2019, 3).

Pod engl. Phishing smatra se vrsta napada društvenog inženjeringa koji pokušava doći do osjetljivih i povjerljivih podataka kao što su korisnička imena, lozinke, podaci o kreditnim karticama, mrežne vjerodajnice itd. U navedenom phishing napadu, napadač šalje phishing e-poštu žrtvama kako bi ukrao vjerodajnice za prijavu i podatke o računu (Vigderman, Turner 2023, 1).

Računalni crv (engl. computer worm) je vrsta mrežnog napada koji se širi unutar vlastite povezane mreže i kopira se s jednog računala na drugo računalo. Može se replicirati bez ikakve ljudske pomoći i ne mora se priključiti na softverski program kako bi oštetio podatke. Crvi mogu iskoristiti sigurnosne rupe u softveru i pokušati pristupiti kako bi ukrali osjetljive podatke, oštetili datoteke i instalirali „stražnja vrata“ za daljinski pristup sustavu (Touhid 2019, 4).

Zanimljiva je i tehnika otmice sesije engl. session hijacking. Kada pojedinac pojesti neko web mjesto, dobiva jedinstveni ID sesije između njega i web mjesta. Napadači mogu oteti sesiju i predstavljati se kao računalo ili web-mjesto, tražeći privatne podatke i posljedično ukrasti podatke osoba (Vigderman, Turner 2023, 1).

Zatim slijedi engl. Rootkit. Rootkit jest zlonamjerni program koji se instalira i potom izvršava kod na sustavu bez pristanka korisnika kako bi dobio pristup sustavu računalu ili mreži. Obično se instalira putem iskorištavanja ranjivosti sustava, taktika društvenog inženjeringa, ukradenih

lozinki ili tehnika krađe identiteta bez znanja žrtve. Postoje različite vrste Rootkit virusa kao što su Bootkit-ovi, Rootkit-ovi firmvera (engl. firmware) i Rootkit-ovi na razini kernela i Rootkit-ovi aplikacija.

Potom valja istaknuti engl. SQL injection. Ova vrsta napada posebno cilja poslužitelje koji pohranjuju kritične podatke u obliku SQL programskog jezika. Promjena temeljnog koda web-mjesta može uzrokovati da web-mjesto otkrije osjetljive ili povjerljive informacije koje obično ne bi (Vigderman, Turner 2023, 1).

Trojanski konj (engl. Trojan horse) je vrsta zlonamjernog koda ili programa koji su razvili hakeri kako bi se prerušili u legitiman softver kako bi dobili pristup sustavima žrtve. Osmišljen je za brisanje, modificiranje, oštećenje, blokiranje ili neku drugu štetnu radnju na pojedinim podacima ili mreži. Žrtva prima e-poruku s privitkom koji izgleda kao službena e-pošta. Privitak može sadržavati zlonamjerni kod koji se izvršava čim žrtva klikne na privitak.

Zatim slijedi engl. Logic bomb. Logična bomba jest zlonamjerni program ili dio koda koji je ubačen u pojedini operativni sustav ili računalnu mrežu te koji nakon određenog vremena utječe na zlonamjernu funkciju. Navedeni kod se može umetnuti u postojeći softver ili u druge oblike zlonamjernog softvera kao što su virusi, crvi ili trojanski konji i sl. Njegova glavna svrha jest brisanje ili mijenjanje podataka, ponovno formatiranje tvrdog diska i stvaranje drugih zlonamjernih radnji na pojedini datum (Touhid 2019, 3).

Potom se navodi engl. ransomware. Ransomware jest vrsta zlonamjernog softvera ili IT sigurnosnih prijetnji koje blokiraju pristup računalnom sustavu i zahtijevaju bitcoin kako bi pristupile sustavu. Najopasniji ransomware napadi su WannaCry, Petya, Cerber, Locky i CryptoLocker itd.

U konačnici, sve navedene vrste napada obično se u računalni sustav unose prilikom preuzimanja, instalacije i otvaranja zlonamjernih privitaka e-pošte, instalacijom softvera koji su zaraženi ili instalacijom zaraženih aplikacija, posjećivanjem zlonamjernih web stranica i klikom na veze ili fotografije koje nisu pouzdane.

5.2. Tehnike sprječavanja hakerskih napada

Postoji nekoliko bazičnih problema koji utječu na porast broja napada hakera. Poznata je činjenica kako Internet ima veliki broj informacija te resursa koji napadačima olakšavaju počinjenje raznih hakerskih napada. Ukoliko neki haker i ne zna na koji način počiniti napad, ima mogućnost da određeni period proučava određenu metu do onog trena kada se odluči provest napad jer je uočio u kojim je točkama meta slaba.

Cyber napad je namjerno iskorištavanje pojedinog sustava i/ili mreže. Naime, cyber napadi koriste zlonamjerni kod kako bi kompromitirali pojedino računala ili podataka u cilju krađe, „curenja! ili zadržavanja podataka kao „taoca“. Prevencija cyber napada ključna je za svaku tvrtku i organizaciju. Uobičajeni primjeri cyber napada su krađa identiteta, prijevara, iznuda, Malware, phishing, spam, spoofing, spyware, trojanci i virusi, ukradeni hardver, poput prijenosnih računala ili mobilnih uređaja, uskraćivanje usluge i distribuirani napadi uskraćivanja usluge, kršenje pristupa, krađa zaporki, infiltracija u sustav, oštećenje web stranice, zloupotreba instant poruka, krađa intelektualnog vlasništva (IP) ili neovlašteni pristup i dr. (Leaf 2022, 1).

U pogledu načina zaštita postoje različite tehnike. Primarno je potrebno postaviti sustav koji bi alarmirao korisnika u slučaju ulaska neovlaštenih osoba u sustav. Zatim se preporučuje fizička biometrijska zaštita kako bi se otklonila mogućnost neovlaštenih ulaza u sustav. Navedena provjera pristupa bi identificirala osobu i putem autorizacije dao bi se uvid u pristupe te prava koje pojedina osoba ima. Identifikacija i autorizacija može se vršiti putem analiziranja glasa osobe, otiskom prsta, skeniranjem lica ili oka, magnetskim čipom i sl. Digitalni certifikati olakšavaju utvrđenje identiteta pojedine osobe jer se koriste kriptografijom unutar digitalne isprave (Dragičević 2004, 51).

Nadalje, potrebno je uspostavit sustav nadzora nad mrežnim sustavom i računalnim sustavom. Također, potrebno je i provjeravati osobe koje koriste mrežni i računalni sustav (tko, što i kako). Osim toga, potrebni su alati koji se bave identifikacijom slabosti unutar pojedinog sustava čime identificiraju potencijalne hakerske pristupe. Preporučuje se korištenje digitalnog potpisa jer ona garantira verificirane autentične poruke. Naime, digitalni potpis bave se izračunom zbroja poruke. Ukoliko je zbroj jedan u trenutku slanja i u trenutku primanja pojedine poruke, tada se

smatra da je takva poruka vjerodostojna. Također, bitno je imati utemeljenu zaštitu od vanjskih čimbenika poput nestanka struje. Osiguravajuća cyber služba kod poduzeća također je poželjna. Kod velikih korporacija preporuka jest imati evidenciju prijava izlaska i ulaska u sustav kao jednu od metoda kojom se želi kontrolirati promet unutar nekog sustava (Dragičević 2004, 53).

Nadalje, uobičajeni načini za sprječavanje naprednijih cyber napada uključuju razvoj programa za upravljanje ranjivostima, provođenje rutinskog testiranja penetracije, implementacija sigurnosnih informacija i upravljanja događajima (SIEM), uvođenje softvera za otkrivanje i sprječavanje upada (IDS i IPS), izrada programa za sprječavanje gubitka podataka (DLP) te izvođenje statičke analize koda (Swanagan 2022, 1).

Jedan od najčešćih načina na koji hakeri dolaze do određenih podataka unutar tvrtki je preko njihovih vlastitih zaposlenika. Naime, hakeri će poslati lažne e-poruke u kojima će se lažno predstaviti kao netko u unutar pojedine organizaciji i tražit će osobne podatke ili pristup određenim datotekama. Veze se često čine legitimnim nevještom oku. Zbog toga je svijest zaposlenika unutar pojedine organizacije vitalna. Smatra se kako je jedan od najučinkovitijih načina zaštite od kibernetičkih napada i svih vrsta povreda podataka redovna oduka i edukacija zaposlenika o prevenciji kibernetičkih napada i informiranje o aktualnim kibernetičkim napadima.

U jednom intervju s nekadašnjim hakerom Kevinom Mitnickom ustanovljeno je kako su osnovne metode kojima hakeri napadaju korisnike izloženost mrežnih usluga, ljudski faktor kod korištenja socijalnog inženjeringa te izloženost aplikacija. Prilikom vršenja testa sigurnosti Mitnick je istaknuo kako treba obratiti pažnju na unutarnje i vanjske mreže, bežičan Internet te na aplikacije s weba. Kao pogreške Mitnick je naveo ostavljanje dostupnih baza podataka koje posjeduju razne informacije, korištenje usluga unutar oblaka, korištenje web aplikacija koje nisu prošle sigurnosne testove te neredovito ažuriranje (PBS 2020, 1).

Osim navedenog, potrebno je redovno održavati i obnavljati softver i sustav. Vrlo često hakeri pojedine sustave napadaju jer sustav ili softver nisu u potpunosti ažurirani, čime su oni slabi i izloženi riziku hakiranja. Navedene slabosti bivaju iskorištene od strane hakera koji putem njih žele ostvariti pristup pojedinog mreži. Jednom kada uspiju ući postaje kasno za poduzimanje radnji prevencije. U cilju suprotstavljanja navedenom potrebno je uložiti u sustav za upravljanje

zakrpama koji će se baviti upravljanjem svim ažuriranjima softvera i sustava, čime će pojedini sustav biti otporan i ažuran.

Osiguranje zaštite krajnje točke također jest jedan od načina kojim se može spriječiti hakerski napad. Zaštita krajnjih točaka štiti mreže koje su daljinski premoštene s uređajima. Mobilni uređaji, tableti i prijenosna računala koji su povezani s korporativnim mrežama daju pristupne putove sigurnosnim prijetnjama. Te je staze potrebno zaštititi posebnim softverom za zaštitu krajnjih točaka. Osim toga, preporučuje se instalirati i vatrozid. Naime, postoji toliko mnogo različitih vrsta sofisticiranih povreda podataka, a nove se pojavljuju svaki dan. Postavljanje mreže iza vatrozida predstavlja jednog od najviše efektivnih oblika zaštite od hakera. Putem sustava vatrozida blokiraju se potencijalni napadu na sustav ili mrežu prije nego li nastaje šteta (Leaf 2022, 2).

Također, preporučuje se izrada sigurnosnih kopija podataka. U slučaju napada hakera od iznimne je koristi posjedovanje sigurnosne kopije podataka kako bi se izbjegao njihov gubitak koji može u pojedinim slučajevima imati i dalekosežne posljedice. Potrebno je i vršiti kontrolu nad osobama koje mogu pristupati pojedinom sustavu. Naime, pojedinac može jednostavno ući u neko poduzeće i priključiti USB ključ koji sadrži zaražene datoteke u jedno računalo, čime mu se dopušta pristup cjelokupnoj mreži. Dakle, u cilju kontrole nad pristupanjem računalima, preporuča se instalacija perimetarskog sigurnosnog sustava u cilju sprječavanja potencijalnih hakerskih napada. Osim toga, iznimno je važna i sigurnost wifi-a. Potrebno je štiti i skrivati pojedinu wifi mrežu. Naime, putem nje haker može se povezati sa zaraženim uređajima čime cjelokupni sustav se izlaže opasnosti. Uz bežičnu tehnologiju koja se svakodnevno sve više razvija, postoje brojni uređaji koji se mogu spojiti na pojedinu mrežu i izvršit ugrozu. Također, preporuka jest da se koristi steganografija (sposobnost pisanja tajnih poruka) kako bi se u dijelove informacijskog sustav koji nisu iskorišteni ubacile informacije (Dragičević 2004, 33).

Nadalje, kada je riječ o korporacijama ili organizacijama, potrebno je da svaki zaposlenik ili član ima vlastiti osobni račun. Dakle, svaki zaposlenik podnosi vlastitu prijavu za svaku aplikaciju i program. Nekoliko korisnika koji se povezuju pod istim vjerodajnicama mogu ugroziti poslovanje. Dakle, odvojene prijave za svakog člana osoblja pomoći će kod smanjenja broja fronti za potencijalni napad. U pravilu se korisnici prijavljuju samo jednom dnevno te koriste samo vlastiti skup prijava. Veća sigurnost nije jedina prednost jer se dobiva i poboljšana upotrebljivost. Također, posjedovanje upravljanih administratorskih prava i blokiranje osoblja

prilikom instalacije ili pristupanju određenim podacima ili sadržajima unutar pojedine mreže korisno je za sigurnost i otklon potencijalnih napada hakera. U svezi prethodno navedenog, prilikom izrade lozinki za pristupanje različitim sadržajima potrebno je postavljati različite lozinke za svaku pojedinu aplikaciju. Navedeno se smatra prednošću u pogledu sigurnosti te čestim promjenama osigurava se zaštita od unutarnjih i vanjskih prijetnji (Leaf 2022, 3). U pogledu lozinki, preporuka jest da pojedina lozinka bude što složenija te da se redovno mijenja. Ustanovljeno je kako za jaku lozinku je potrebno da ona ima kombinaciju malenih i velikih slova, znakova, brojeva te da bude dulja od 7 znakova.

Osim navedenog, jedna od tehnika sprječavanja napada hakera jest korištenje enkripcije. Enkripcija je sigurnosna metoda u kojoj su podaci kodirani na siguran način tako da im samo ovlašteni korisnik može pristupiti. Zaštitit će podatke o mreži od krađe ili ugrožavanja. Metoda šifriranja štiti osjetljive podatke kao što su mrežne vjerodajnice i brojevi kreditnih kartica kodiranjem i pretvaranjem informacija u nečitljiv šifrirani tekst (Touhid 2019, 5).

Test sigurnosti pojedinog sustava može se provjeriti putem testiranja penetracije (engl. penetration testing). Navedeni oblik testiranja odvija se tako da se preuzima uloga hakera u napadu na pojedini sustav i prilikom toga se uzima veliki raspon alata koji služe za izradu procjene razine ranjivosti pojedinog sustava (Peter 2018, 22). Ukoliko se pronađu točke nesigurnosti, nastoji ih se iskoristiti. Po dovršetku testa korisnika se informira o slabostima pojedinog sustava te na koji se način te slabosti mogu iskoristiti kako bi se izvršio popravak nedostataka (Vodafone Business 2014, 13).

Posjedovanje SSL certifikata također je jedna od tehnika za priječit hakerski napad. SSL je kratica za engl. Secure Sockets Layer a koja se smatra globalnim standardnim sigurnosnim protokolom koji uspostavlja sigurnu vezu između web poslužitelja i internet preglednika. Dakle, ovaj certifikat osigurava da svi podaci koji prolaze kroz mrežu između web poslužitelja i preglednika ostanu šifrirani i sigurni. Ukoliko pojedina osoba ili organizacija stvoriti sigurnu vezu, tada mora instalirati SSL certifikat na web poslužitelj i on služi kako bi provjerio autentičnost aplikacije ili web stranice te da šifrira podatke koji se prenose internetom (Touhid 2019, 6).

Osim toga, preporuča se i korištenje vatrozida za web aplikacije (engl. Web Application Firewall – WAF). Vatrozid web aplikacije predstavlja alat za rješavanje kibernetičke sigurnosti

koji se temelji na aplikaciji i koji je dizajniran za zaštitu aplikacija i mobilnih aplikacija filtriranjem i nadzorom HTTP štetnog prometa. WAF obično štiti softver ili aplikaciju od različitih vrsta kibernetičkih napada poput cross-site-scripting (XSS), inkluzija datoteka, SQL injection, session hijacking, Layer 7 DoS i sl. (Touhid 2019, 7). pnajpoznatiji primjeri WAF-a danas su Symantec WAF, Barracuda WAF, Fortinet FortiWeb, Citrix NetScaler AppFirewall i dr.

Posljednja tahnika, te u aktualno vrijeme iznimno popularna i reklamirana, jest korištenje virtualnih privatnih mreža (engl. Virtual Private Network – VPN). Virtualna privatna mreža je tehnologija koja stvara sigurnu i šifriranu vezu preko manje sigurne mreže, kao što je internet. Virtualne privatne mreže najčešće koriste korporacije kako bi zaštitile svoje osjetljive podatke od kibernetičkih napadača, ali sve je veća primjena i kod fizičkih osoba. Ovo je sigurna metoda povezivanja koja se koristila za dodavanje sigurnosnih značajki i privatnosti javnim i privatnim mrežama kao što su Wi-Fi Hotspots i Internet. Kao primjer toga može se navesti situacija u kojoj iako pojedina osoba živi u San Franciscu, putem korištenja virtualne privatne mreže može se prikazati da živi u nekom drugom mjestu kao New York, Texas, Miami i sl. (Touhid 2019, 8).

6. Zaključak

U današnjem međusobno povezanom svijetu kibernetička sigurnost velika je briga koja utječe na sve kutove kibernetičkog prostora. To varira od velikih korporacija i vlada kojima su ugroženi osjetljivi podaci do povremenih kućnih korisnika koji se susreću s brojnim vrstama hakerskih napada koji nanose štetu njihovom sustavu. Kako se Internet i razne nove aplikacije društvenih medija razvijaju sve većom brzinom, broj povezanih potencijalnih ranjivosti i povezanih vektora napada također raste. Stoga, povećani broj računala i uređaja koji se međusobno povezuju na raznim mrežama uzrokuje i porast broja cyber napada.

Cyber kultura podrazumijeva praksu i kulturne proizvode koji deriviraju iz informacijskih tehnologija i interneta. Informacijska sigurnost ima za cilj pružiti zaštitu glede privatnosti korisnika i omogućit trajnu dostupnost informacija. Postoje brojne vrste kibernetičkih kriminala a novi oblici se konstantno razvijaju. Uzročnici su primarno ljudskog faktora, a potom su tu zastarjeli softveri koji se nisu pravovremeno ažurirali te neadekvatni načini autentifikacije.

Hakere je inicijalno motivirala znatiželja i činili su hakerske aktivnosti u višku svog slobodnog vremena. Danas, uz hakere se veže pojam koristi i financijske dobiti, te oni podvode takve aktivnosti ne bi li pribavili informacije koje bi potom prodali nalogodavcu ili zainteresiranim osobama i zaradili. Informacije su danas kao imovina i imaju svojevrsnu vrijednost, pa je samim time i njihovo čuvanje iznimno bitno.

Nadalje, evidentno je kako hakere motivira društven (socijalan) život, opstanak i razonoda. Postoji nekoliko tipova hakerskih napada a to su mrežni, bežični, napadi društvenim inženjeringom te napadi putem zlonamjernog softvera. Unutar navedenog postoje brojne podvrste a struktura navedene podjele će se u budućnosti svakako mijenjati zbog rapidnog razvoja interneta i internetskih tehnologija. Za sprječavanje napada hakera ustanovljene su brojne tehnike od kojih se najvažnijim smatra postavljanje „jakih“ lozinka, autentifikacija u dva koraka, enkripcija, SSl cetifikat, VPN, redovno ažuriranje softvera, instalacija softvera za uklanjanje i sprječavanje raznih virusa, adwarea i sl. ali i svakako izrada sigurne kopije podatak ukoliko dođe do hakerskog napada.

Zaključno, područje kibernetičke sigurnosti veoma je rizično iako većina korisnika nije toga svjesna. Njegov najveći nedostatak jest nedovoljna zakonska regulativa koja bi regulirala ovo područje kao i adekvatne penalizacije za hakere. Naime, aktualni tradicionalni zakoni ne smatraju se dovoljno učinkovitima da se bore protiv velikog broja različitih vrsta aktivnosti unutar kibernetičkog prostora.

7. Sažetak na engleskom jeziku

Online threats are a daily part of the modern world. The Internet circulates a large number of information and users. This is precisely why user data is often the target of hackers. Cyber culture implies social conditions that have arisen as a result of the widespread use of computer networks for the purpose of communication, entertainment or business. When carrying out attacks, hackers use different tools and constantly come up with new techniques in order to obtain information that they can further monetize. It is believed that the motives of hackers were primarily a desire for fame or available free time, but nowadays hackers are motivated by monetary earnings from the data they obtain through hacking. In addition to the above, in order for a hacker to carry out an attack, he goes through several procedural phases, namely the preparation phase, the illegal phase and the execution phase. In response to increasingly frequent hacker attacks, there are numerous techniques to prevent hacker attacks and eliminate the threat. Therefore, through the analysis of online threats and ways to plan them, they want to present the correct ways of acting on the Internet in order to protect devices and the information found on them.

Keywords: hackers, attacks, security

Literatura

1. Babić, V., 2009. *Kompjuterski kriminal*, Rabic, Sarajevo.
2. Bandler, J., 2023. *Cybersecurity Frameworks and the Four Pillars of Cybersecurity*. https://westfaironline.com/courts/cybersecurity-frameworks-and-the-four-pillars-of-cybersecurity/#:~:text=The%20four%20pillars%20are%3A,Improve%20data%20security (pristupljeno 1. lipnja 2023.)
3. Bhasin, M., 2007, *Mitigating Cyber Threats To Banking Industry*, The Chartered Accountant, br. 4., str. 1618-1624. https://www.researchgate.net/profile/Madan-Bhasin/publication/286711208_Mitigating_Cyber_Threats_To_Banking_Industry/links/566d2c0608ae1a797e3e68e5/Mitigating-Cyber-Threats-To-Banking-Industry.pdf (pristupljeno 30. travnja 2023.)
4. Chadd, K., 2020. *The History Of Cybercrime And Cybersecurity*, 1940-2020, CyberCrime Magazine, Češka. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/ (pristupljeno 14. travnja 2023.)
5. Cole, E., 2001. *Hackers beware*, New riders Publishing. https://doc.lagout.org/security/Hackers%20Beware.pdf (pristupljeno 1. svibnja 2023.)
6. Davčev, V., Leškovska-Ačkovska, E., 2008. *Tehnologija kao oblikovateljica ljudske kulture: tehnološke i psihološke posljedice*. Filozofska istraživanja, Vol. 28 No. 1, str. 75-82. https://hrcak.srce.hr/clanak/36483%3f (pristupljeno: 15. travnja 2023.)
7. Dragičević, D., 2004. *Kompjutorski kriminalitet i informacijski sustavi*, Informator, Biro sustav
8. Fire, M., Goldschmidt, R., Elovici, Y., 2014. *Online Social Networks: Threats and Solutions*, IEEE Communications Surveys & Tutorials, vol. 16., br. 4.: str. 2019-2036. https://ieeexplore.ieee.org/abstract/document/6809839 (pristupljeno 14. travnja 2023.)
9. Gómez-Diago, G., 2012., *Cyberspace and Cyberculture*, u knjizi: Encyclopedia of Gender in Media.Chapter: Cyberspace and Cyberculture, str. 58-60.
10. Hamidović, H., 2015. *Mjesto i uloga cyber sigurnosti u razvoju modernih društava*, Sarajevski žurnal za društvena pitanja, vol 4, br. 1-2., str. 81-93. https://www.researchgate.net/publication/302901758_Mjesto_i_uloga_cyber_sigurnosti_u_razvoju_modernih_drustava (pristupljeno 14. travnja 2023.)
11. Kaspersky, 2023. *What are web threats*?. https://www.kaspersky.com/resource-center/threats/web (pristupljeno 1. lipnja 2023.)

12. Leaf, 2022. *10 Ways to Prevent Cyber Attacks*. https://leaf-it.com/10-ways-prevent-cyber-attacks/ (pristupljeno 12. travnja 2023.)
13. Levy, S., 1994. *Hackers: Heroes of the computer revolution*, Delta Book, New York
14. Maitanmi, O., Ogunlere, S., Ayinde S., Adekunle, Y., 2013, *Impact of Cyber Crimes on Nigerian Economy*, The International Journal of Engineering and Science, IJES, vol. vol 2(4), str. 45–51. https://www.theijes.com/papers/v2-i4/part.%20(4)/H0244045051.pdf (pristupljeno 1. svibnja 2023.)
15. Milardović, A., 2010. *Globalno selo: sociologija informacijskog društva i cyber kulture, Centar za politološka istraživanja*, Zagreb
16. Nadhini S., 2018. *Overview of Cyber Security*, International Journal of Advanced Research in Computer and Communication Engineering, vol. 7., br. 11., str. 125-128. https://hozir.org/pars_docs/refs/530/529603/529603.pdf (pristupljeno 1. svibnja 2023.)
17. Omodunbi F., Odiase, P., Olaniyan, P., Esan, A., 2016, *Cybercrimes in Nigeria: Analysis, Detection and Prevention*, FUOYE Journal of Engineering and Technology,Volume 1, Issue 1, str. 37-42. https://core.ac.uk/reader/235186040 (pristupljeno 1. svibnja 2023.)
18. PBS, 2020. *The testimony o fan ex-hacker*, https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html (pristupljeno 1. svibnja 2023.)
19. Pekka, H., 2022. *Hakerska Etika i duh informacijskog doba*, Jesenski i Turk Zagreb
20. Peter K., 2018, *The hacker Playbook 3; practical guide to penetration testing*, Publication Secure Planet LLC, USA
21. Raymond, E., Steele, G., 1996. *The new hacker's dictionary Cambridge*, Mass, London, The MIT Press
22. Sekhar B., Chandra, Kumar Pani, Subhendu 2021. *Cyber-Crime Prevention Methodology*, Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, chapter 14. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119711629.ch14 (pristupljeno 1. svibnja 2023.)
23. Spitzer, M., 2018, *Digitalna demencija: kako mi i naša djelca silazimo s uma*, Naklada Ljevak, Zagreb
24. Swanagan, M., 2022. *How to prevent cyber Attacts and Threats*, https://purplesec.us/resources/prevent-cyber-

attacks/#:~:text=Common%20ways%20to%20prevent%20more,information%20and%20event%20management%20(SIEM) (pristupljeno: 15. travnja 2023.)

25. Taylor, H., 2023. *What are cyber threats and how to safeguard your data*, https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them (pristupljeno 22. travnja 2023).
26. Terranova, T,, 2004. *Network culture: politics for the Information age*. London, Ann Arbor: Pluto Press
27. Touhid, A., 2019. *Types of Network Attacks and Prevention Techniques*, https://cyberthreatportal.com/types-of-network-attacks-and-prevention/ (pristupljeno 22. travnja 2023.)
28. Vigderman, A., Tuner, G., 2023. *Does Antivirus Stop Hackers?*, https://www.security.org/antivirus/hackers/#:~:text=Antivirus%20software%20immunizes%20our%20computers,)%2C%20and%20other%20malicious%20programs (pristupljeno 22. travnja 2023).
29. Vodafone Business 2014, *Cyber Security: Interview with an ethical hacker*, Episode 5, Youtube, https://www.youtube.com/watch?v=GVDFM9X1prI (pristupljeno: 15. travnja 2023.)
30. Vuković, H., 2012. *Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj*. National security and the future, vol. 13, br. 3, str. 12-31. https://hrcak.srce.hr/100728 (pristupljeno: 15. travnja 2023.)

Prilozi