Pregled metoda i alata zaštite osobnih računala od kibernetičkih prijetnji

Paun, Luka

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Luka Paun

PREGLED METODA I ALATA ZAŠTITE OSOBNIH RAČUNALA OD KIBERNETIČKIH PRIJETNJI

ZAVRŠNI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Informacije i komunikacije**

ZAVRŠNI ZADATAK br. 6130

Pristupnik: **Luka Paun (0246071770)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Pregled metoda i alata zaštite osobnih računala od kibernetičkih prijetnji**

Opis zadatka:

U okviru završnog rada potrebno je pružiti pregled najčešćih i najučestalijih kibernetičkih prijetnji te aktualnih metoda zaštite korisničkih računala. Nastavno, potrebno je analizirati dostupne programske alate namijenjene zaštiti krajnjih računala i korisnika od kibernetičkih prijetnji. Na temelju provedene analize potrebno je pružiti smjernice za prevenciju određenih kibernetičkih napada te planirati mogućnosti reaktivnih aktivnosti u slučaju uspješno provedenog kibernetičkog napada.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

PREGLED METODA I ALATA ZAŠTITE OSOBNIH RAČUNALA OD KIBERNETIČKIH PRIJETNJI

OVERVIEW OF CYBER THREAT SECURITY METHODS AND TOOLS FOR PERSONAL COMPUTERS

Mentor: dr. sc. Ivan Cvitić

Student: Luka Paun

JMBAG: 0246071770

Zagreb, svibanj 2021.

PREGLED METODA I ALATA ZAŠTITE OSOBNIH RAČUNALA OD KIBERNETIČKIH PRIJETNJI

SAŽETAK

Ovaj završni rad prikazuje metode i alate za zaštitu osobnih računala od kibernetičkih prijetnji. Također su opisane različite metode i programska rješenja koja se koriste za zaštitu računala. Svijet se danas oslanja na tehnologiju više nego ikad prije. Kao rezultat, generiranje digitalnih podataka naglo je porastao unatrag samo jednog desetljeća. Korisnici velik dio podataka pohranjuju na računala i prenose ih preko mreže. Svi uređaji i njihovi temeljni sustavi imaju ranjivosti koje ugrožavaju osobna računala i njihove podatke. U ovom radu analizirane su metode i alati za zaštitu osobnih računala od kibernetičkih prijetnji te su utvrđene smjernice prevencije i planiranje odaziva na kibernetičke napade. Provedenom analizom definirano je na koji način zaštititi osobno računalo od kibernetičkih prijetnji, bilo to uklanjanjem ili sprječavanjem, minimiziranjem štete koju ona može prouzročiti ili otkrivenjem i prijavljivanjem štete kako bi se mogle poduzeti korektivne mjere.

KLJUČNE RIJEČI: osobna računala; zaštita računala; kibernetičke prijetnje

SUMMARY

This bachelor's thesis shows methods and tools for protecting personal computers from cyber threats. Various methods and software solutions used to protect computers are also described. The world today relies on technology more than ever before. As a result, generation of digital data has skyrocketed in just one decade. Users store much of their data on personal computers and transmit them over a network. All devices and their core systems have vulnerabilities that threaten organizations and their data. This thesis analyzes methods and tools to protect PCs from cyber threats and sets out guidelines for preventing and planning response to cyber attacks. The analysis defines how to protect your personal computer from cyber threats, whether by removing or preventing it, minimizing the damage it may cause, or by detecting and reporting it so that corrective action can be taken.

KEY WORDS: personal computers; computer protection; cyber threats

Sadržaj

1. Uvod

Kibernetička prijetnja je zlonamjeran čin usmjeren na krađu ili uništavanje podataka, računalnih mreža, intelektualnog vlasništva ili dobivanje neovlaštenog pristupa. Bilo da se radi o rezervaciji hotelske sobe ili naručivanju večere ili pozivanju taksija, uvijek se koristi Internet i samim time stalno se generiraju podaci. Ti se podaci općenito pohranjuju u oblaku koji je u osnovi poslužitelj podataka velikih kapaciteta pohrane, obrade i brzine prijenosa ili podatkovni centar kojem se može pristupiti na mreži. Također koriste se različiti uređaji za pristup tim podacima.

U računalnom kontekstu sigurnost se sastoji od kibernetičke sigurnosti i fizičke sigurnosti. Oba se koriste za zaštitu od neovlaštenog pristupa podatkovnim centrima i drugim računalnim sustavima. Informacijska sigurnost osmišljena je za održavanje povjerljivosti, cjelovitosti i dostupnosti podataka u podskupu kibernetičke sigurnosti. Upotreba kibernetičke sigurnosti može pomoći u sprječavanju kibernetičkih napada, ugrožavanju podataka, krađe identiteta i pomoći upravljanja rizicima.

Predmet analize ovog završnog rada su metode i alati zaštite osobnih računala od kibernetičkih prijetnji. Metode i alati zaštite opisane su u trećem i četvrtom poglavlju, dok su u petom i šestom poglavlju navedene smjernice prevencije i planiranje odaziva na kibernetičke prijetnje.

Cilj i svrha izrade ovog završnog rada je analiza mogućnosti metoda i zaštite osobnih računala od kibernetičkih prijetnji te opis njihovog provođenja.

Završni rad sastoji se od 6 poglavlja:

1. Uvod
2. Pregled kibernetičkih prijetnji
3. Metode zaštite računala od kibernetičkih prijetnji
4. Programski alati za zaštitu računala od kibernetičkih prijetnji
5. Smjernice prevencije i planiranje odaziva na kibernetičke napade
6. Zaključak

U drugom poglavlju definirani su pojmovi povjerljivosti, integriteta i dostupnosti, prikazana je zastupljenost kibernetičkih napada, objašnjeni su pojmovi mrežno temeljnih napada i napada temeljenih na informacijskom sustavu, te je objašnjen način širenja kibernetičkih prijetnji.

U trećem poglavlju opisane su različite metode zaštite računala od kibernetičkih prijetnji te njihovi utjecaji gdje su najčešće mete osobni i osjetljivi podaci korisnika.

Četvrto poglavlje obuhvaća programske alate za zaštitu računala od kibernetičkih prijetnji. Opisani su softveri koji služe za detektiranje, izolaciju i blokiranje raznih kibernetičkih prijetnji.

U petom poglavlju opisane su smjernice prevencije kibernetičkih napada. Opisani su pojmovi prijetnje, ranjivosti i rizika te zašto je bitno imati kontrolu nad tim čimbenicima. Također, definirano je planiranje odaziva na kibernetičke prijetnje te su definirane i objašnjenje pojedine faze planiranja odaziva na kibernetičke prijetnje.

2. Pregled kibernetičkih prijetnji

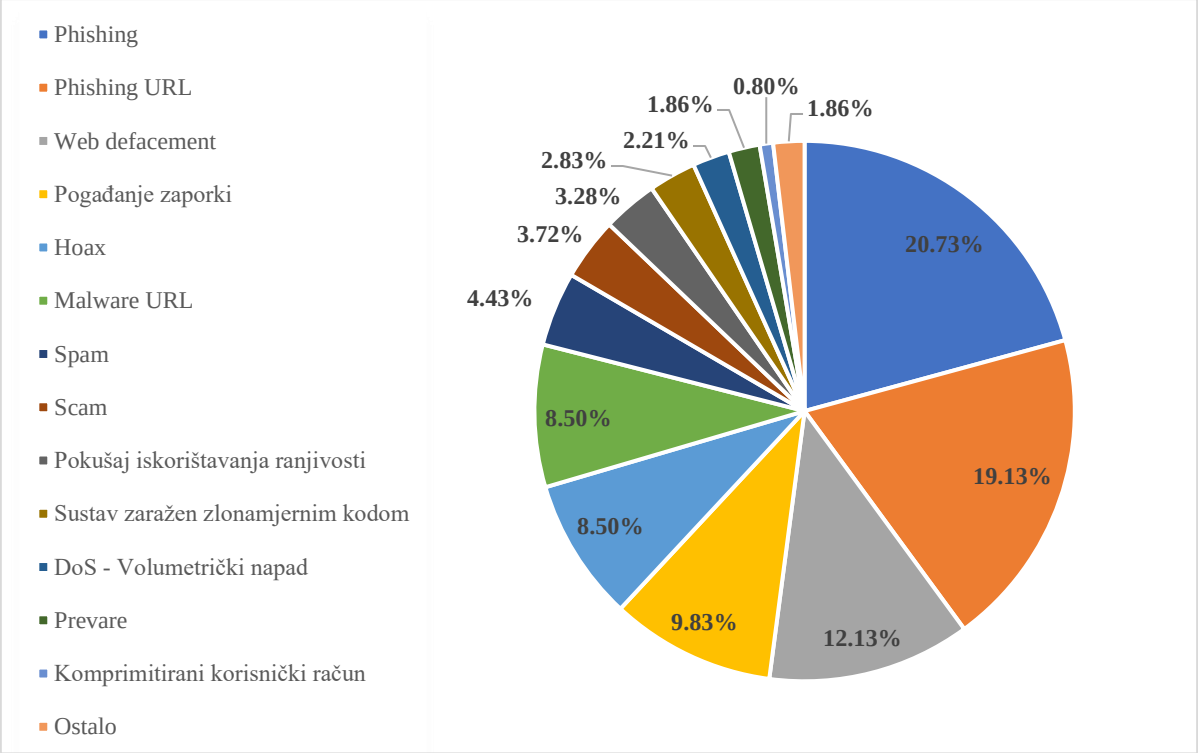
Kada se govori o kibernetičkoj sigurnosti, postoje tri glavne aktivnosti od kojih se osobna računala pokušavaju zaštititi, a to su: neovlaštena izmjena, neovlašteno brisanje i neovlašteni pristup. Oni su sinonimni s vrlo poznatom CIA trijadom, koja označava povjerljivost, integritet i dostupnost (engl. *Confidentiality, integrity and availability – CIA*). CIA trijada također se naziva tri stupa sigurnost, a većina sigurnosnih politika većih organizacija, pa čak i manjih tvrtki, temelji se na ova tri načela.

Povjerljivost je jednaka privatnosti. Mjere poduzete kako bi se osigurala povjerljivost osmišljene su kako bi se spriječilo da osjetljive informacije dođu do pogrešnih ljudi, osiguravajući da ih pravi ljudi zapravo mogu dobiti. Pristup mora biti ograničen na one ovlaštene za pregled predmetnih podataka. Uobičajeno je da se podaci kategoriziraju prema količini i vrsti štete koja bi se mogla učiniti ako padnu u pogrešne ruke. Prema tim kategorijama mogu se provesti više ili manje stroge mjere.

Integritet uključuje održavanje dosljednosti, točnosti i pouzdanosti podataka tijekom cijelog životnog ciklusa. Podaci se ne smiju mijenjati u tranzitu i moraju se poduzeti koraci kako bi se osiguralo da neovlaštene osobe ne mogu mijenjati podatke. Te mjere uključuju zaštitu datoteka i kontrole korisničkog pristupa. Osim toga, moraju postojati neka sredstva za otkrivanje bilo kakvih promjena u podacima koje mogu nastati kao posljedica događaja koji nisu uzrokovani ljudskim djelovanjem, kao što su elektromagnetski impulsi ili pad servera. Neki podaci mogu uključivati kontrolne zbrojeve (engl. *checksum*) ili čak kriptirane kontrolne zbrojeve za provjeru integriteta. Redundantnost ili sigurnosne kopije moraju biti dostupe za vraćanje zahvaćenih podataka u ispravno stanje.

Dostupnost se osigurava rigoroznim održavanjem cjelokupnog hardvera, izvođenjem hardverskih popravaka odmah kada je to potrebno i održavanjem ispravnog funkcionalnog okruženja operativnog sustava bez softverskih sukoba. Također je važno biti u tijeku sa svim potrebnom nadogradnjama sustava. Jednako je važno osigurati odgovarajuću propusnost komunikacije i spriječiti pojavu uskog grla (engl. *bottleneck*). Redundancija, prebacivanje u slučaju pogreške (engl. *failover*) i klasteri visoke dostupnosti mogu ublažiti ozbiljne posljedice kada se pojave problemi s hardverom. Brz i prilagodiv oporavak od katastrofa ključan je za najgore scenarije u kojima se kapacitet oslanja na postojanje sveobuhvatnog plana oporavka od katastrofa, [1].

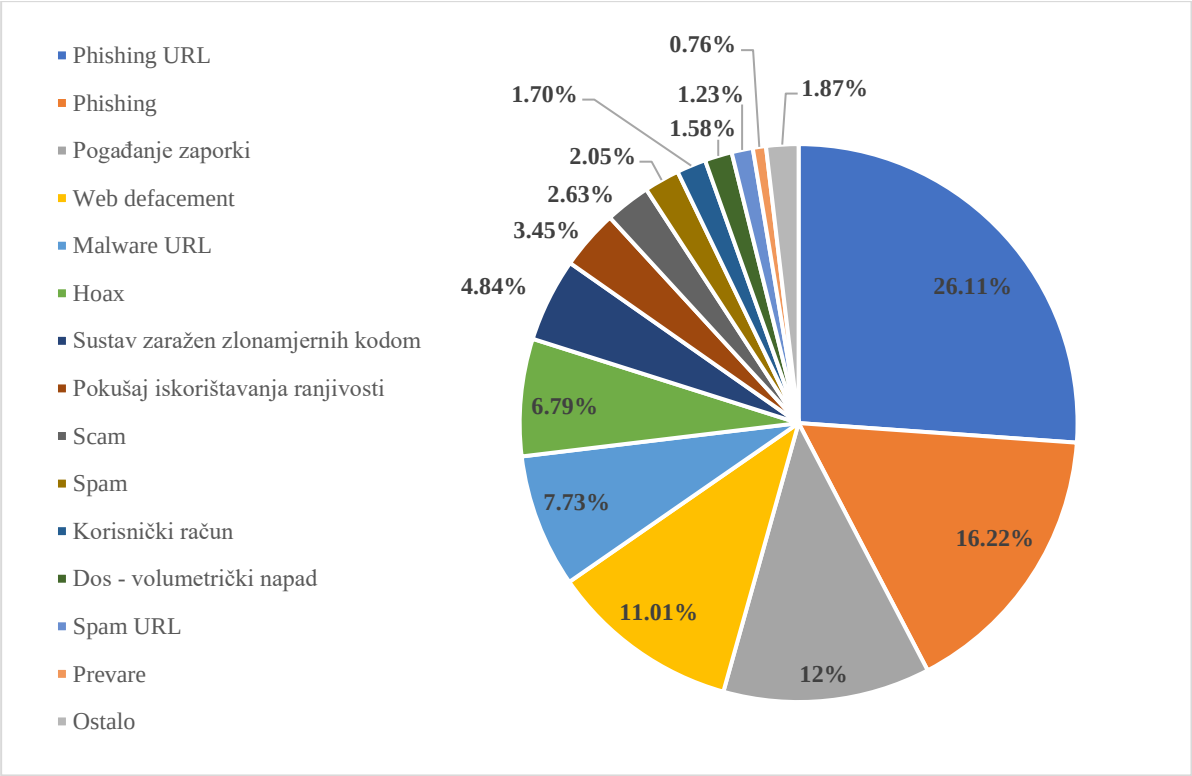
Zastupljenost prijavljenih kibernetičkih prijetnji ovisno o vrsti napada najbolje je prikazati pomoću grafičkog prikaza statističkih podataka o broju prijava i vrsti prijetnji, kao što prikazuje slika 1. za podatke iz 2019. godine i slika 2. za podatke iz 2020. godine.



Slika 1. Zastupljenost kibernetičkih napada po vrsti za 2019. godinu

Izvor: [2]

Na slici 1. može se primijetiti zastupljenost napada krađom identiteta od ukupno skoro 30% naspram ostalih vrsta kibernetičkih napada, nakon kojih slijede *Web defacement* napadi (napad u kojem se mijenja izgled naslovne strane komprimirane *web*-stranice) te kibernetički napadi poput *brute-force* i zlonamjernih softvera.



Slika 2. Zastupljenost kibernetičkih napada po vrsti za 2020. godinu

Izvor: [3]

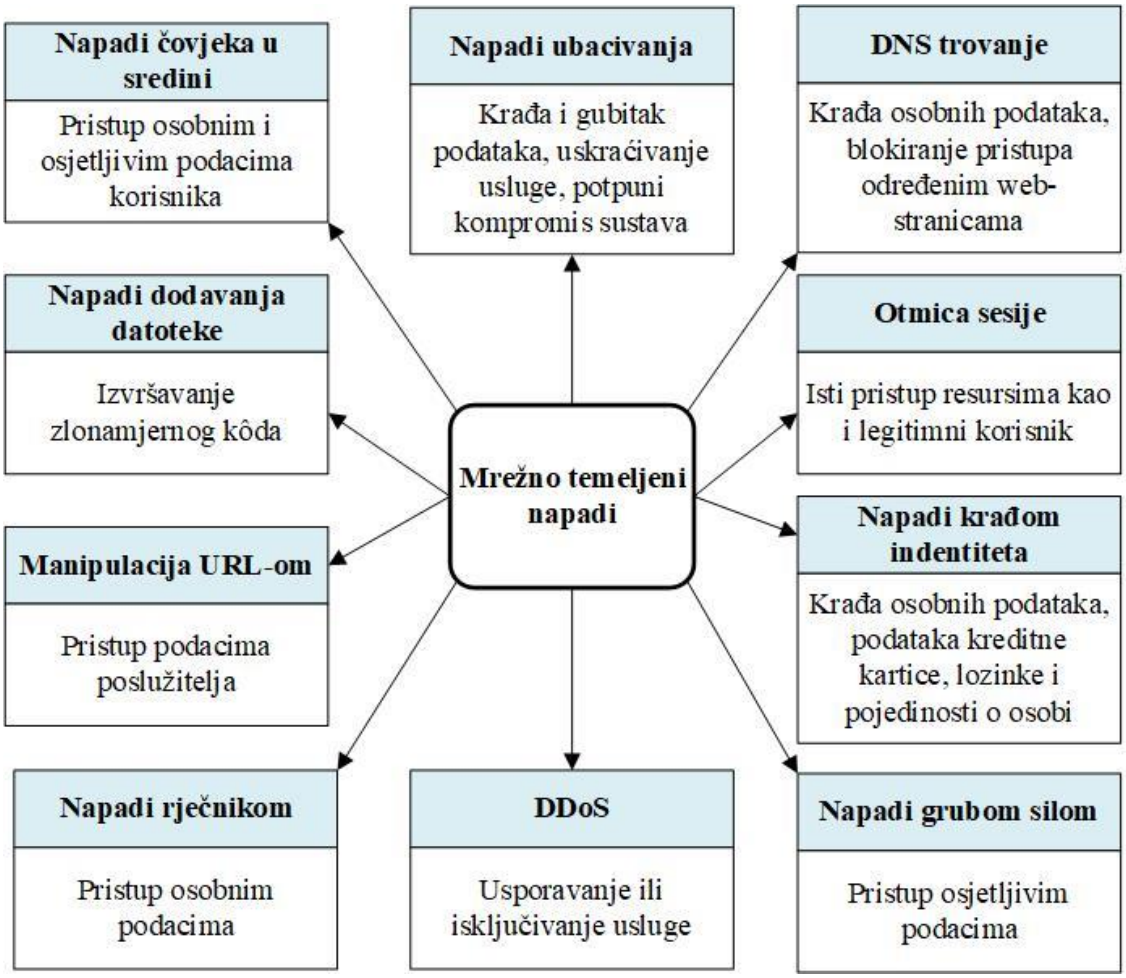
Na slici 2., jasno je vidljivo kako napadi krađom identiteta i dalje imaju zastupljenost oko 30%, međutim vidljiv je i porast *brute-force* napada kao i zlonamjernih softvera.

Kibernetičke prijetnje mogu se klasificirati na sljedeće kategorije:

1. Mrežno temeljeni napadi (engl. *Web-based attacks*)
2. Napadi temeljeni na informacijskom sustavu (engl. *System-based attacks*)

2.1. Mrežno temeljeni napadi

Kada napadači iskoriste ranjivosti u kodiranju kako bi dobili pristup poslužitelju ili bazi podataka, ove vrste prijetnji kibernetičkih napada poznate su kao napadi sloja aplikacije. Korisnici Interneta vjeruju da će osjetljivi i osobni podaci koje podijele na *web*-stranici biti sigurni i privatni. Napadi temeljeni na *web*-u mogu ugroziti privatne informacije kao što su korisnikova kreditna kartica, medicinske informacije, privatne slike i *chat*-ovi, što dovodi do potencijalno teških posljedica. *Web* aplikacije posebno su osjetljive na kibernetičke napade jer često zahtijevaju visoku razinu dostupnosti. Budući da te aplikacije moraju biti javno dostupne, ne mogu se zaštititi iza vatrozida. Mnoge aplikacije imaju pristup, bilo izravno ili neizravno, vrlo poželjnim podacima o kupcima. Napadač traži ranjivosti kako bi mogao ukrasti te informacije ili ih proslijediti, [4].



Slika 3. Pojednostavljen prikaz mrežno temeljenih napada i njihovih ishoda

Iako se taktike kibernetičkih napada stalno razvijaju, njihove temeljne strategije napada ostaju relativno slične. U nastavku su navedeni neki od najčešćih.

2.1.1. Napad ubacivanja

U napadu ubacivanja (engl. *Injection Attack*), napadač prisiljava aplikaciju da obrađuje korisničke podatke kao da je riječ o uputama za izvršavanje bilo koje druge naredbe. Napadi ubacivanja su među najstarijim i najopasnijim napadima usmjerenim na *web*-aplikacije i mogu dovesti do krađe podataka, gubitka podataka, gubitka integriteta podataka, uskraćivanja usluge, kao i potpunog kompromisa sustava. Neki od načina na koji napadač može izvršiti napad iznimno su jednostavni, dok drugi zahtijevaju puno vještine i vremena za otkrivanje. Primarni razlog ranjivosti ubacivanja obično je nedovoljna provjera valjanosti korisničkog unosa. Napad ubacivanjem je zlonamjerni kod ubačen u mrežu koji je napadaču donio sve informacije iz baze podataka. Ova vrsta napada smatra se velikim problemom u *web*-sigurnosti i navedena je kao najveći sigurnosni rizik *web*-aplikacije. SQL *Injection* ranjivosti nastaju kada programeri softvera stvaraju dinamične upite baze podataka koji uključuju korisničko isporučeni unos

(engl. *user-supplied input*). Kako bi se izbjegli nedostaci SQL ubacivanja programeri moraju prestati pisati dinamičke upite i/ili spriječiti da korisnički isporučeni unos koji sadrži zlonamjerni SQL utječe na logiku izvršenog upita. Međutim, napadi ubacivanja ne pojavljuju se samo u SQL-u, a metoda ubacivanja ne mora nužno uključivati *web* oblik. Svaka točka u kojoj aplikacija omogućuje unos ili preuzimanje podataka može sadržavati nedostatak koji omogućuje kibernetički napad, [5]. U nastavku su opisane različite vrste napada ubacivanja:

Ubacivanje SQL naredbi je vrsta napada u kojem napadač izvršava zlonamjerne SQL naredbe (engl. *Malicious Payload*) koji kontroliraju poslužitelj baze podataka *web*-aplikacije. Ovo je jedna od najstarijih ranjivosti jer sve *web*-stranice ili *web*-aplikacije koriste SQL baze podataka. Postoji nekoliko vrsta SQL ubacivanja (engl. SQL *Injection*), ali sve su povezane s napadačem koji umetne proizvoljni SQL upit u baze podataka *web*-aplikacije. Koristeći SQL *Injection* ranjivost, s obzirom na prave okolnosti, napadač ga može koristiti za zaobilaženje mehanizama provjere autentičnosti i autorizacije *web*-aplikacije i dohvaćanje sadržaja cijele baze podataka. Ako *web*-aplikacija ne može sanirati korisnički unos, napadač može implementirati SQL naredbu po svom izboru u internu bazu podataka i mijenjati, kopirati ili izbrisati sadržaj bare podataka. Učinci SQL injekcija su zaobilaženje provjere autentičnosti, otkrivanje informacija, gubitak podataka, krađa podataka i gubitak integriteta podataka, uskraćivanje usluge i ponekad kompromis sustava, [5].

Napad skriptama na *web*-aplikaciju (engl. *Cross-Site Scripting* - XSS) je vrsta sigurnosnog napada u kojem napadač ubacuje podatke poput zlonamjerne skripte u sadržaj koji dolazi s drugih, pouzdanih *web*-stranica. XSS napadi događaju se kada je nepouzdanom izvoru dopušteno unositi vlastiti kôd u *web*-aplikaciju, a taj zlonamjerni kôd uključen je u dinamički sadržaj koji se isporučuje pregledniku *web*-stranice. XSS napade generalno dijelimo na Pohranjene XSS napade (engl. *Stored* XSS *Attacks*), Slijepo skriptiranje na više mjesta (engl. *Blind Cross-site Scripting*) i Reflektirani XSS napadi (engl. *Reflected* XSS *Attacks*). Pohranjeni napadi su oni u kojima je ubačena skripta trajno pohranjena na ciljnim poslužiteljima, kao što je forum poruka, zapisnik posjetitelja stranice, baza podataka, polju komentara i slično. Žrtva zatim dohvaća zlonamjernu skriptu s poslužitelja kada zatraži pohranjene informacije. Slijepo skriptiranje na više mjesta oblik je trajnog XSS-a. To se obično događa kada se napadačev paket spremi na poslužitelj i reflektira natrag na žrtvu iz pozadinske aplikacije. *Blind Cross-site Scripting* teško je potvrditi u stvarnom scenariju. Reflektirani napadi su oni u kojima se ubačena skripta reflektira s *web*-poslužitelja, kao što je poruka o pogrešci, rezultat pretraživanja ili bilo koji drugi odgovor koji uključuje dio ili cijeli unos poslan poslužitelju kao dio zahtjeva.

Reflektirani napadi su jedni on najčešćih vrsta XSS napada. Dostavljaju se žrtvama drugom rutom, primjerice u poruci e-pošte ili na nekoj drugoj *web*-lokaciji. Kada korisnik klikne na zlonamjernu vezu, pošalje posebno izrađen obrazac ili čak samo pregledava zlonamjernu stranicu, ubrizgani kôd putuje na ranjivu *web*-stranicu, što se reflektira natrag u korisnikov preglednik. Preglednik zatim izvršava kôd jer je došao s "pouzdanog" poslužitelja, [6].

Slično napadima SQL ubrizgavanja, XPath *Injections* napadaju *web*-stranice koje rade na informacijama koje su dali korisnici kako bi konstruirali XPath upit za XML podatke. To je vrsta napada u kojem zlonamjerni unos može dovesti do neovlaštenog pristupa ili otkrivanja osjetljivih informacija, kao što su sadržaj i struktura XML dokumenta. Velik broj tehnika koje se mogu koristiti u napadu pomoću SQL ubacivanja ovisi o karakteristikama SQL-a koje koristi ciljana baza podataka. Naspram SQL ubacivanja, XPath napadi mogu biti mnogo prilagodljiviji, [5].

Ubacivanje predloška (engl. *Template Injection*) na strani poslužitelja događa se kada napadač može koristiti sintaksu izvornog predloška za ubacivanje zlonamjernog korisnog paketa u predložak, koji se zatim izvršava na strani poslužitelja. Moduli predložaka dizajnirani su za generiranje web-stranica miješanjem fiksnih predložaka s promjenjivim podacima. Napadi ubacivanja predloška na strani poslužitelja mogu se pojaviti kada se korisnički unos pohranjuje izravno u predložak, a ne prosljeđuju kao podaci. To napadačima omogućuje ubacivanje proizvoljnih direktiva o predlošcima kako bi manipulirali modulom predložaka, često im omogućujući da preuzmu potpunu kontrolu nad poslužiteljem. Kao što ime sugerira, korisni paketi za ubacivanje predložaka na strani poslužitelja isporučuju se i procjenjuju na strani poslužitelja, što ih potencijalno čini mnogo opasnijima od tipičnog ubacivanja predloška na strani klijenta, [7].

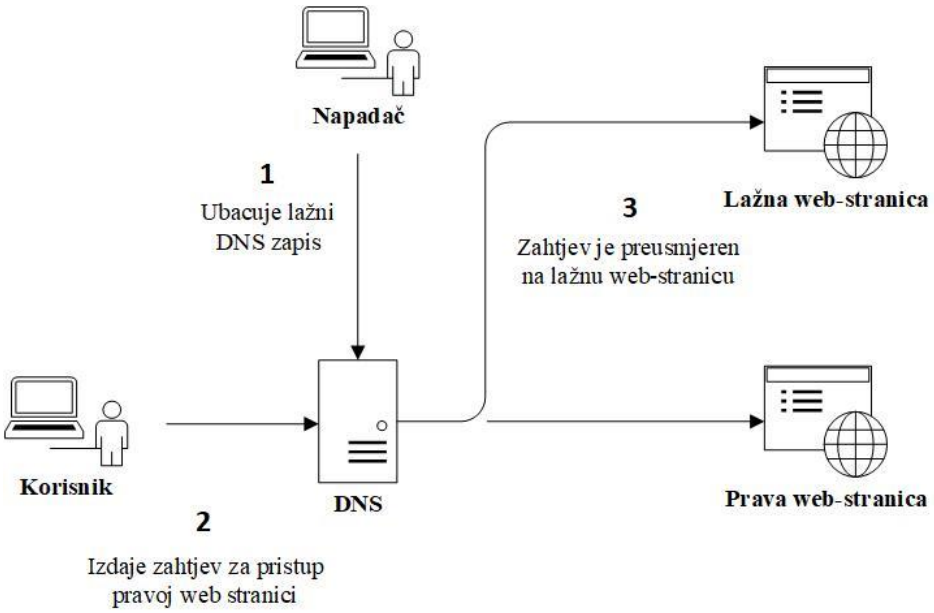
Ubacivanje kôda (engl. *Code Injection*) je opći pojam za vrste napada koji se sastoje od ubacivanja kôda koji se zatim izvršava u aplikaciji. Napad se događa kada napadač koristi pogrešku provjere unosa u softveru kako bi unio i izvršio zlonamjerni kôd. Taj kôd se upisuje u jezik ciljane aplikacije i izvodi na strani poslužitelja. Svaka aplikacija koja izravno upotrebljava neprovjerene unesene podatke ranjiva je na ovu vrstu napada, a *web* aplikacije su glavni cilj napadača, [8].

LDAP (engl. *Lightweight Directory Access Protocol*) je aplikacijski protokol koji se koristi preko IP mreže za upravljanje i pristup distribuiranom informacijskom servisu direktorija. Primarna svrha imeničkog servisa je pružanje sustavnog skupa zapisa, obično organiziranih u hijerarhijsku strukturu. Sličan je telefonskom imeniku koji sadrži popis pretplatnika s njihovim kontakt brojem i adresom. LDAP ubacivanje vrsta je sigurnosnog iskorištavanja koja se koristi za komprimiranje procesa provjere autentičnosti koje koriste neke *web* stranice. LDAP ubacivanje radi na sličan način kao i SQL ubacivanje, tako da napadač šalje SQL kôd u *web*-obrazac. Prvenstveno se događa zbog nedostatka ili slabe provjere valjanosti unosa koja ne odbacuje pogrešno oblikovan unos ili uklanja zlonamjerne LDAP kontrolne znakove prije uključivanja nepouzdanog korisničkog unosa u upit, [9].

Napadi ubacivanjem naredbi, koji se također češće nazivaju napadi ubacivanja naredbi operacijskog sustava (engl. *OS command injection*), iskorištavaju programski propust izvršavanja naredbi sustava bez odgovarajuće provjere valjanosti unosa ili sanitacije, što može dovesti do proizvoljnih naredbi koje izvršava zlonamjerni napadač. To je opasna ranjivost jer se naredbe operativnog sustava obično izvršavaju s ovlastima ranjive aplikacije. Stoga bi napadač mogao steći potpunu kontrolu nad ubrizgavanjem naredbi, ugrožavajući aplikaciju i sve njene podatke. Ranjivost ubacivanja naredbe OS-a može se koristiti u svim programskim jezicima koji mogu pozvati *system shell* naredbu, [10].

2.1.2. DNS trovanje

DNS (engl. *Domain Name Server*) razrješava abecedne nazive domena kao što su www.primjer.com u odgovarajuće IP adrese koje se koriste za pronalaženje i komunikaciju između čvorova na Internetu. Trovanje DNS-a (engl. *DNS Spoofing*) prevarantski je kibernetički napad u kojem napadač preusmjerava *web*-promet prema lažnim *web*-poslužiteljima i *web*-stranicama za krađu identiteta. Te lažne *web*-stranice obično izgledaju identično kao i odredište korisnika, što napadačima olakšava varanje posjetitelja u dijeljenju osjetljivih podataka. Jedan od primjera je kako Kina koristi trovanje DNS-a kako bi blokirali pristup određenim stranicama ili zamijenili originalne stranice vlastitim kopijama koje korisnici neznatno koriste misleći da su na identičnoj stranici kao i korisnici izvan Kine, [11].



Slika 4. Napad DNS trovanja poslužitelja

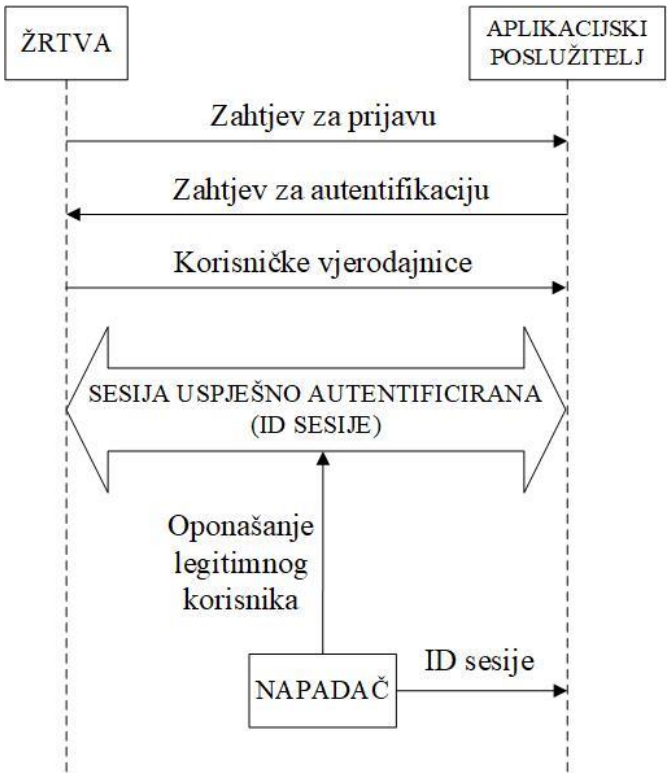
Izvor: [12]

2.1.3. Napad grubom silom

U napadu grube sile (engl. *Brute-force attack*) napadač pokušava dobiti pristup osjetljivim podacima i sustavima metodom pokušaja i pogreške (engl. *trial and error*) sustavnim isprobavanjem što je više moguće kombinacija korisničkih imena i pogađanih lozinki. Ova vrsta napada dobila je ime „Brute-force“ jer koriste pretjerane nasilne pokušaje kako bi prisilili svoj put na privatne račune legitimnih korisnika. Ovo je jedna od najstarijih, ali i dalje popularnih metoda kibernetičkih napada. Ovisno o složenosti i duljini lozinke koja se pokušava probiti, probijanje može potrajati od nekoliko minuta do nekoliko godina, [13].

2.1.4. Otmica sesije

Otmicu sesije (engl. *Session Hijacking*) možemo definirati kao preuzimanje aktivne TCP/IP komunikacijske sesije bez dopuštenja korisnika. Nakon uspješne implementacije, napadač preuzima identitet komprimiranog korisnika, imajući isti pristup resursima kao i legitimni korisnik. Neki od uobičajenih rezultata otmice sesije su krađa informacija, krađa identiteta i krađa osjetljivih podataka. Otmice sesije mogu biti aktivne i pasivne. Kod aktivne metode otmice sesije, napadač će ukloniti jedno od računala i preuzeti njegovu poziciju u razmjeni komunikacije. Aktivni napad omogućuje napadaču izdavanje naredbi na mreži što omogućuje stvaranje novih korisničkih računa na mreži koje kasnije napadač može koristiti kako bi pristupio mreži bez izvođenja napada otmice sesije, [14].

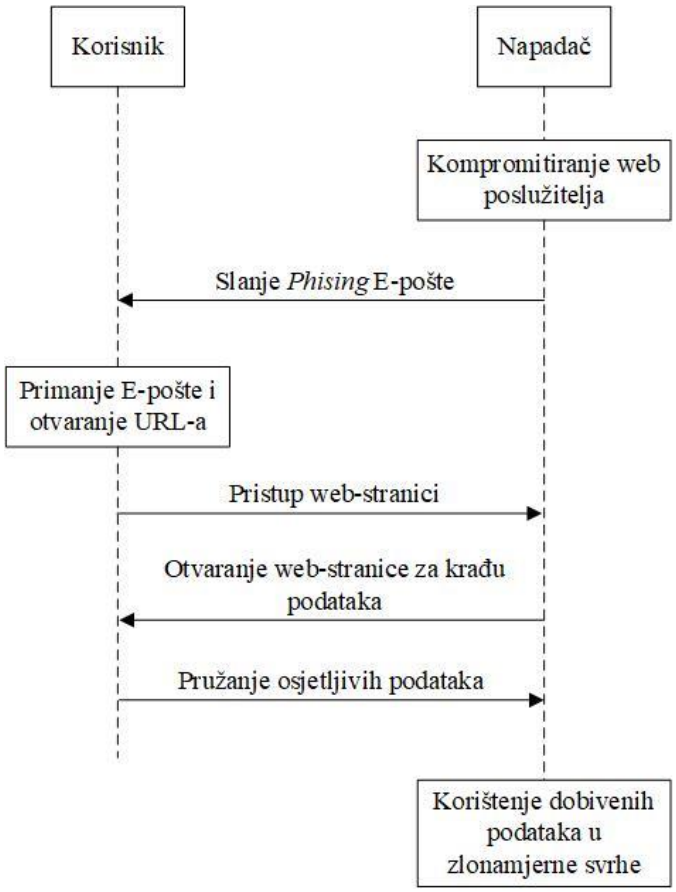


Slika 5. Dijagram toka napada otmice sesije

Izvor: [15]

2.1.5. Napad krađom identiteta

Napadi krađom identiteta (engl. *Phishing)* su vrsta kibernetičkih napada koji najčešće koriste telefon, tekst ili e-poštu kako bi se privukli naivni pojedinci i pružili svoje osjetljive ili osobne podatke, podatke kreditne kartice, lozinki i pojedinosti o osobi. Napadači se predstavljaju kao legitimni predstavnici neke korporacije ili firme, npr. predstavnici Microsoft korisničke službe, koji zatim traže pristup osobnom računalu. Nakon što se osigura pristup osobnom računalu, često dođe do krađe identiteta ili značajnog financijskog gubitka, [16].

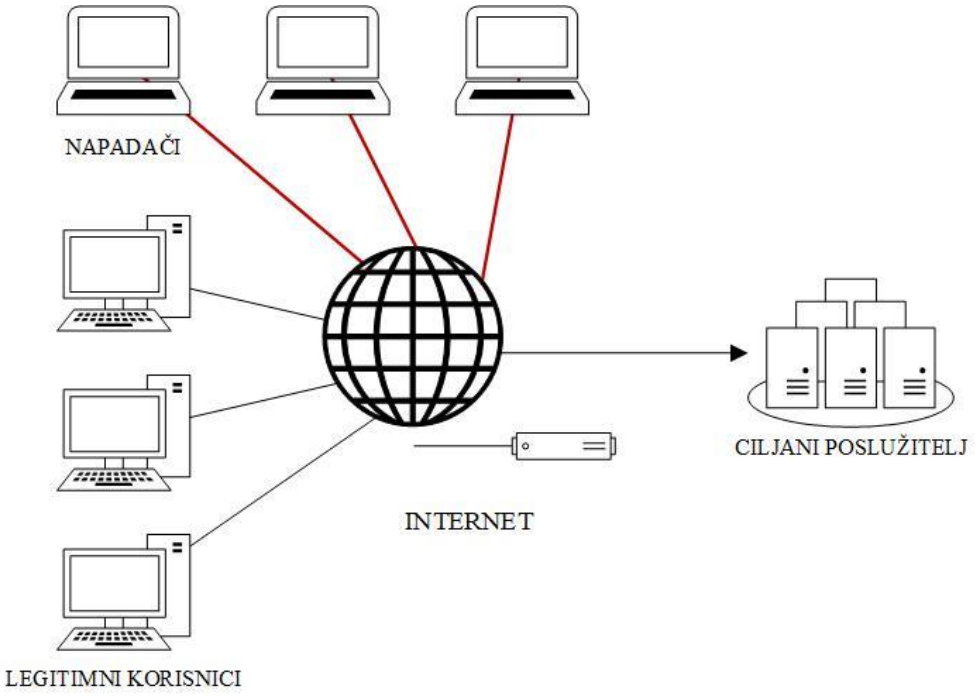


Slika 6. Dijagram toka *phishing* napada

Izvor: [17]

2.1.6. Distribuirano uskraćivanje usluge

Kod napada distribuiranog uskraćivanja usluge (engl. *Distributed Denial of Service* - DDoS) koriste se kompromitirani računalni sustavi kao izvori napadačkog prometa. Cilj može biti poslužitelj, *web*-stranica ili neki drugi mrežni resurs. Poplava dolaznih poruka, zahtjeva za povezivanje ili neispravno oblikovanih paketa prisiljava ciljani sustav na usporavanje ili isključivanje usluge legitimnim korisnicima i sustavima. DDoS napad je poput neočekivane prometne gužve koja začepljuje autocestu, sprječavajući redoviti promet da stigne na svoje odredište, [18]. Ova vrsta prijetnje, zbog jednostavnosti provede predstavlja često istraživani problem što je vidljivo iz brojnih znanstvenih radova poput [19], [20], [21].



Slika 7. Pojednostavljen prikaz DDoS napada

Izvor: [22]

DDoS napade generalno dijelimo u tri kategorije:

1) Napad na temelju volumena - DDoS napadi temeljeni na volumenu (engl. *Volume-Based Attacks*) najčešći su od tri. Da bi se napravio takav napad, napadači koriste mnoga računala i internetske veze (često distribuirane širom svijeta) kako bi poslali veliku količinu prometa ili paketa prema ciljanoj mreži u nastojanju da nadvladaju maksimalnu propusnost *web*-stranice. Kao rezultat toga, legitimni promet ne može proći, a napadači mogu uspješno srušiti *web*-stranicu. Ovaj tip napada prevladava naspram druga dva zbog niže tehničke prepreke za generiranje velikog broj zahtjeva. Uglavnom se koriste jednostavne tehnike pojačanja kako bi se skalirao napad. Napadi na temelju volumena mjere se u bitovima po sekundi (bps), [23].
2) Napadi protokola - Za razliku od napada temeljenih na volumenu i klasičnih DDoS napada, napadi protokola (engl. *Protocol Attacks*) oslanjaju se na slabost u internetskim komunikacijskim protokolima. Budući da su mnogi od tih protokola standardizirani i u globalnoj upotrebi, promjena načina rada tih protokola bila bi komplicirana i spora za uvođenje. Čak i kada bi neki složeni protokol bio ponovno uveden kako bi se ispravili postojeći nedostaci, vjerojatno bi se uvele nove slabosti koje bi omogućile nove vrste protokolarnih napada i mrežnih napada. Napadači preplavljuju *web*-stranice i ove resurse poslužitelja slanjem lažnih zahtjeva za protokol

kako bi potrošili dostupne resurse. Snaga tih napada mjeri se u paketima po sekundi (pps), [23].

3) Napadi sloja aplikacije – Napadi sloja aplikacije (engl. *Application Layer Attacks*) općenito zahtijevaju manje resursa od prijašnje spomenutih napada na temelju volumena i napada protokola. Ova vrsta napada dobila je ime po tome što cilja ranjivosti unutar aplikacija kao što su operativni sistemi ili aplikacije. Kao rezultat napadač dobiva sposobnost zaobilaženja normalne kontrole pristupa, te zatim može:
    - Izmijeniti, čitati, brisati ili dodavati podatke unutar operacijskog sustava
    - Uvesti vrstu virusnog programa kako bi kopirao virus kroz cijelu mrežu
    - Uvesti program za analizu mreže i dobivanje informacija za rušenje ili kvarenje sustava
    - Prekidanje podatkovnih aplikacija ili operativnih sustava
    - Onemogućavanje sigurnosnih kontrola

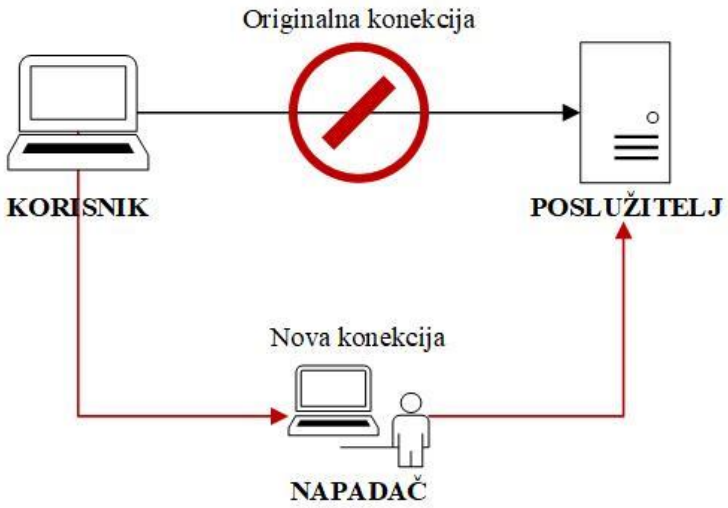
Budući da napadi sloja aplikacije ciljaju samo određene pakete aplikacija, oni mogu proći nezapaženo. Napadi sloja aplikacije žele poremetiti određene funkcije ili značajke *web*-stranica kao što su internetske transakcije. Snaga tih napada mjeri se u zahtjevima u sekundi (rps), [23].

2.1.7. Napad rječnikom

Napad rječnikom (engl. *Dictionary attacks*) je metoda provaljivanja u računalo ili poslužitelj zaštićen lozinkom sustavnom provjerom i pokušajem svim mogućih lozinki i pristupnih izraza dok se ne pronađe ispravna lozinka. Napad rječnikom jedna je od brute-force metoda napada i vrlo je česta kao oblik kibernetičkih napada zbog velikih količina pojedinaca koji koriste uobičajene varijacije riječi kao lozinke. Ovi napadi rijetko su uspješni protiv sustava koji za lozinke koriste više riječi i potpuno su neuspješni protiv sustava koji za lozinke koriste kombinacije velikih i malih slova pomiješanih s brojevima. Klasičan brute-force napad možda može biti uspješan u takvim slučajevima, ali takav pristup može potrajati predugo vremena da bi bio učinkovit, [24].

2.1.8. Napad čovjeka u sredini

Korištenje besplatnog javnog Wi-Fi-a je svakodnevica mnogih ljudi. Dobar je način za uštedu mobilnih podataka. Međutim, jedan prosječan korisnik neće razmišljati o sigurnosti korištenja takvih mreža. Upravo te javne mreže se najčešće koriste za napade čovjeka u sredini (engl. *Man in the middle attack*) jer mogu jednostavno doći do osobnih podataka korisnika. MITM napadi su jedni od najčešćih kibernetičkih napada upravo zato što su jednostavni i potencijalno vrlo unosni. Ne samo da se mogu izložiti financijski detalji, nego čak i svi osobni podaci i vrijedne informacije. MITM napadi su napadi gdje se kriminalac ubaci između komunikacije dva uređaja i čita promet bez da ga itko primijeti. Obično su ta dva uređaja prijenosno računalo i Wi-Fi usmjerivač. Ako se ne koristi šifrirana veza, što se često događa kada se posjećuje nesigurna *web*-stranica, čovjek u sredini može saznati sve osjetljive informacije korisnika. Ukratko, MITM napad može dovesti do krađe identiteta, krađe podataka, te izloženosti bankovnih podataka i svih drugih informacija koje korisnik ne bi inače podijelio s javnošću. Ljudi uvijek imaju mobitel pri sebi, i spajaju se na svakakve Wi-Fi mreže u kafićima, trgovinama itd. kako bi uštedjeli mobilne podatke. Mobilni uređaju su također pogodni za MITM napade, [25].



Slika 8. Napad čovjeka u sredini

Izvor: [26]

2.2. Napadi temeljeni na informacijskom sustavu

Napadi temeljeni na sustavu možemo kategorizirati pod sintaksne napade (engl. *syntactic attacks*) koji koriste softver poput virusa kako bi ometao ili oštetio računalni sustav ili mrežu. Njegov cilj je napasti korisnike uzrokujući proizvodnju grešaka i nepredvidivih rezultata u računalnom sustavu. Sintaksni napadi ponekad se grupiraju pod pojmom zlonamjernih softvera ili *malware*. Ti napadi mogu uključivati viruse, crve (engl. *worms*) i trojanske konje. Jedan od čestih načina prijenosa takvih napada je e-pošta, [27].

2.2.1. Virus

Da bi se razumjelo što je virus, prvo je potrebno objasniti izvorno biološko značenje te riječi. Biološki virusi poput onih koji mogu razboljeti ljude su parazitski. Oni ubrizgavaju vlastiti kôd, u ovom slučaju DNA ili RNA, u stanicu domaćina kao sredstvo replikacije. Ovaj kôd uzrokuje da stanica napravi tonu kopija virusa i na kraju eksplodira, šaljući nove viruse posvuda. Isperite i ponovite. Računalni virusi djeluju po sličnom principu. Za razliku od nekih oblika zlonamjernog softvera koji su u potpunosti izvršni programi, virusi su obično manji dijelovi kôda koji se miješaju s drugim programima ili datotekama i repliciraju se samo kada su uvjeti ispunjeni. Tako ih može pokrenuti određeni datum i vrijeme, otvaranje određenog programa ili čak dostizanje određene količine korištenja diska. Nakon što se virus pokrene, pokušat će se kopirati i širiti, zaraziti druge datoteke i programe na putu, ponekad putem mreže i baš kao i pravi virusi, ove kopije virusa mogu biti malo drugačije od izvornog što antivirusnom softveru otežava njihovo uklanjanje. Slično tome kako mnoge varijante virusa prehlade otežavaju stvaranje cjepiva. Neki čak dolaze šifrirani čineći otkrivanje još kompliciranijim. Naravno da virusi, bili oni biološki ili digitalni, ne bi bili problem ako bi samo kopirali sebe. Ali baš kao što će virus vodenih kozica razboljeti čovjeka, računalni virus može sadržavati nosivu komponentu (engl. *payload*) koji će uzrokovati neku vrstu učinka koji može biti bilo što, od prikazivanja šale do trajnog oštećenja važnih podataka. Ovih dana virusi mogu pokrenuti DDoS napade zarazom puno računala i navođenjem svih njih da napadnu određeni poslužitelj odjednom, [28].

2.2.2. Crvi

Kada crv (engl. *Worm*) zarazi novi sustav, njegov prvi potez je početi tražiti više sustava za zarazu, obično istražujući zaraženi sustav i njegove mrežne veze. Crv normalno koristi obične mrežne protokole kako bi istražio svoju lokalnu mrežu i proširio se nakon što otkrije sustave potencijalnih žrtava. Ranjivi sustavi, sustavi sa starijim softverom koji su osjetljivi na napad, vjerojatno će biti zaraženi. Neće svi sustavi biti ranjivi. Neki crvi ovise o operativnom

sustavu i zarazit će samo Windows ili Apple ili Linux sustave. Crvi se također mogu spriječiti pri pokušaju zaraze sustava koji imaju ažurirani i potpuno zakrpani softver. Crv će se nastaviti pokušavati širiti kada je zaraženi sustav povezan s više od jedne mreže, ili kada se taj sustav poveže s novom mrežom, dodatno šireći infekciju. Nakon povezivanja s drugom mrežom, proces ponovno počinje. Crv se može brzo proširiti na mnoge sustave na mnogim različitim mrežama, pogotovo ako iskorištava široko rasprostranjenu ranjivost. Nakon što se otkrije crv, mora se ukloniti, a u najgorem slučaju, sustav će možda trebati ponovno instalirati. Puno je bolje izbjeći infekciju na prvom mjestu tako da korisnik bude u toku sa softverom sustava i zakrpama, onemogućiti nepotrebne mrežne protokole i učinkovitu higijenu sustava kibernetičke sigurnosti, [29].

2.2.3. Trojanski konj

Napadač skriva zlonamjerni program u e-pošti nevinog izgleda ili datoteci. Klikom ili preuzimanjem datoteke program prenosi zlonamjerni softver na uređaj žrtve, a zlonamjerni kôd može izvršiti bilo koji zadatak koji je napadač namjeravao. Jednom kada je trojanski konj prenesen i aktiviran, može negativno utjecati na performanse i dovesti žrtvu u opasnost na mnoge načine. Trojanci napadaču mogu dati kontrolu stražnjih vrata nad uređajem, snimiti pisanja tipkovnicom ili ukrasti osjetljive korisničke podatke, preuzeti virus crva, šifrirati korisničke podatke i tražiti novac za ključ, aktivirati kameru ili mogućnosti snimanja uređaja ili pretvoriti računalo u takozvano „zombi računalo“ za provođenje prijevare ili nezakonitih radnji. Iako je većina napada trojanskih konja zlonamjerna, policija ih također može koristiti za legalno hvatanje informacija relevantnih za kaznenu istragu. Čak je i naprednim skenerima zlonamjernog softvera teško pronaći i uništiti trojanske konje, ali obično ih prate neobična ponašanja, poput prekomjernih skočnih prozora, gubitka kontrole tipkovnice i miša te neočekivanih promjena razlučivosti, boje i orijentacije radne površine računala, [30].

2.2.4. Stražnja vrata

Prva stvar koju napadač učini prilikom provaljivanja nekog *web*-mjesta ili poslužitelja je instaliranje stražnjih vrata (engl. *Backdoor*). *Backdoor* daje napadaču kompletne mogućnosti daljinskog upravljanja ugrožene *web*-stranice. Može se koristiti za uređivanje *web*-stranice, krađu osjetljivih informacija, pokretanje DDoS napada na drugim *web*-mjestima ili zaražavanje računala korisnika koji posjećuju *web*-mjesto zlonamjernim softverom. Otkrivanje stražnjih vrata na *web*-mjestu i njihovo blokiranje vrlo je kompliciranо. Vrlo se dobro skrivaju među tisućama datoteka nevidljivih vanjskim skenerima *web*-stranica i obično će preživjeti ponovnu instalaciju, [31].

2.2.5. Botovi

Botovi (engl. *Bots*) su softverski programi koji izvode unaprijed definirane, ponavljajuće, automatizirane zadatke. Botovi obično zamjenjuju ili oponašaju ljudsko ponašanje korisnika. Budući da su automatizirani, rade puno brže od ljudskih korisnika. Oni izvršavaju korisne funkcije, poput korisničke usluge ili indeksiranja pretraživača, ali mogu doći i u obliku zlonamjernog softvera koji se koristi za stjecanje potpune kontrole nad računalom. Računalni botovi i internetski botovi u osnovi su digitalni alati i kao bilo koji drugi alat, mogu se koristiti i za dobre i loše svrhe. Dobronamjerni botovi izvršavaju korisne zadatke, međutim zlonamjerni botovi nose kibernetičke prijetnje i mogu se koristiti za napade, neželjenu poštu, špijuniranje, ometanje i kompromitiranje *web*-stranica. Otprilike pola cjelokupnog internetskog prometa danas čine računalni botovi koji izvršavaju određene zadatke, poput automatizacije korisničke službe, simulacije ljudske komunikacije na društvenim mrežama, pomaganja tvrtkama u pretraživanju sadržaja na mreži i pomaganja u optimizaciji tražilice, [32].

2.3. Širenje kibernetičkih prijetnji

Kibernetičke prijetnje razvijaju se kroz vrijeme iskorištavanjem novih pristupa. Često, napadači modificiraju postojeće *malware* postupke kako bi iskoristili nedostatke koji postoje u novim tehnologijama. U drugim slučajevima istražuju jedinstvene karakteristike novih tehnologija kako bi pronašli ranjivost. Iskorištavajući nove internetske tehnologije s milijunima aktivnih korisnika, napadači koriste te nove tehnologije kako bi učinkovito i brzo došli do velikog broja žrtava. Neki od primjera bi bili pametni telefoni i društveni mediji. Danas svaki korisnik interneta ima račun na društvenoj mreži, a broj korisnika eksponencijalno raste iz godine u godinu. Društvene mreže postale su preferirana metoda komunikacije među mlađom generacijom. Na svakoj od tih *web*-stranica korisnici dijele svoje osobne informacije kao što su ime, prezime, spol i datum rođenja, slike itd. Napadači iskorištavaju društvene mreže kao novi medij za pokretanje kibernetičkih napada. Zbog neograničenog pristupa profilu korisnika, napadači mogu dodatno dobiti informacije o poslovnim tajnama i ostalim privatnim informacijama.

Društvene mreže također su povećale napore kako bi zaštitili privatnost, intimnost i dostupnost korisničkih podataka. To ih čini atraktivnim metama za razne organizacije koje mogu objediniti velike količine korisničkih podataka, bile one za legitimne svrhe ili za zlonamjerne. U većini slučajeva izdvajanje podataka krši očekivana prava privatnosti korisnika.

3. Metode zaštite računala od kibernetičkih prijetnji

Održavanjem sigurnosti osobnih računala smanjuje se mogućnost kibernetičkih napada koji mogu doći u obliku raznih zlonamjernih softvera i izravnih pokušaja kibernetičkih napada usmjerenih na krađu osobnih i osjetljivih podataka. U nastavku su navedene preporučene metode zaštite osobnih računala od kibernetičkih prijetnji:

3.1. Sigurnosna kopija podataka

Do gubitka podataka može doći na puno načina, od kvarova tvrdog diska i kibernetičkog napada do fizičke krađe hardvera. Bez obzira na način, sigurnosna kopija podataka osigurat će vraćanje podataka na uređaje korisnika. Preporuka je da se sigurnosna kopija pohranjuje na sigurnom, odvojenom mjestu od izvornog uređaja, a dobar primjer toga je oblak, npr. OneDrive. Glavni razlog za sigurnosno kopiranje podataka je brzo i neprimjetno vraćanje podataka na korisnički uređaj u slučaju gubitka podataka, bili oni povjerljivi poslovni dokumenti ili dragocjene privatne fotografije. Neki od najčešćih načina sigurnosne kopije podataka:

- Prijenosni mediji – Uobičajeno se odnosi na prijenosne uređaje kao što su USB memorijski stick-ovi. Univerzalno su kompatibilni sa svim prijenosnim računalima, stolnim računalima, pa čak i mobilnim uređajima i tabletima ako imaju OTG kabel. Naspram nekih drugih solucija pohrane, prijenosni mediji prosječno imaju jako mali kapacitet za današnje standarde, od nekoliko gigabajta do par stotina gigabajta. Glavna prednost prijenosnih medija je njihova univerzalnost, a glavne mane bi bile loše sigurnosne opcije zaštite podataka i njihova mala fizička veličina, što ih čini pogodnim gubljenju.
- Eksterni tvrdi diskovi – Kao što samo ime govori, radi se o istim tvrdim diskovima koji se koriste u osobnim računalima, samo što se nalaze u vlastitom kućištu, izvan računala. Prednosti eksternih tvrdih diskova je što često imaju opciju enkripcije podataka te puno veći kapacitet naspram standardnih prijenosnih medija, čak do deset terabajta.
- Sigurnosna kopija u oblaku – Danas je pohrana podataka u oblaku jedna od najpopularnijih metoda sigurnosne kopije. Svi mobilni uređaju inherentno dolaze s besplatnim pristupom oblaku između 5 i 50 gigabajta. Osobna računala s Windows 10 sustavom imaju opciju registriranja novog Microsoft računa ili korištenje postojećeg računa kako bi dobili pristup OneDrive oblaku. Alternativno, može se koristiti i bilo koji drugi oblak. Jedna od prednosti sigurnosne kopije u oblaku su promjenjiva veličina, korisnik može birati između

besplatnog ili plaćenog kapaciteta, gdje plaćena opcija može nuditi do nekoliko terabajta memorije u oblaku. Ostale prednosti su različita fizička lokacija naspram korisničkog računala, enkripcija podataka, kompatibilnost između mobilnih uređaja i osobnih računala. Glavna mana ove metode pohrane je povjerenje osobnih podataka samom oblaku, te cijena. Ako korisnik treba veliku količinu kapaciteta za sigurnosnu kopiju, jeftinije je kupiti eksterni tvrdi disk sličnog kapaciteta, [33].

3.2. Osiguranje korisničkih uređaja i mreže

Dobro zaštićena mreža omogućava sigurnije korištenje interneta. Svi umreženi domovi koriste Internet, a to uključuje uređaje kao što su osobna računala, mobilni uređaji, tableti, televizori i ostali uređaji koji se bežično spajaju na mrežu. Kako bi se mreža zaštitila, potrebno je poduzeti nekoliko koraka:

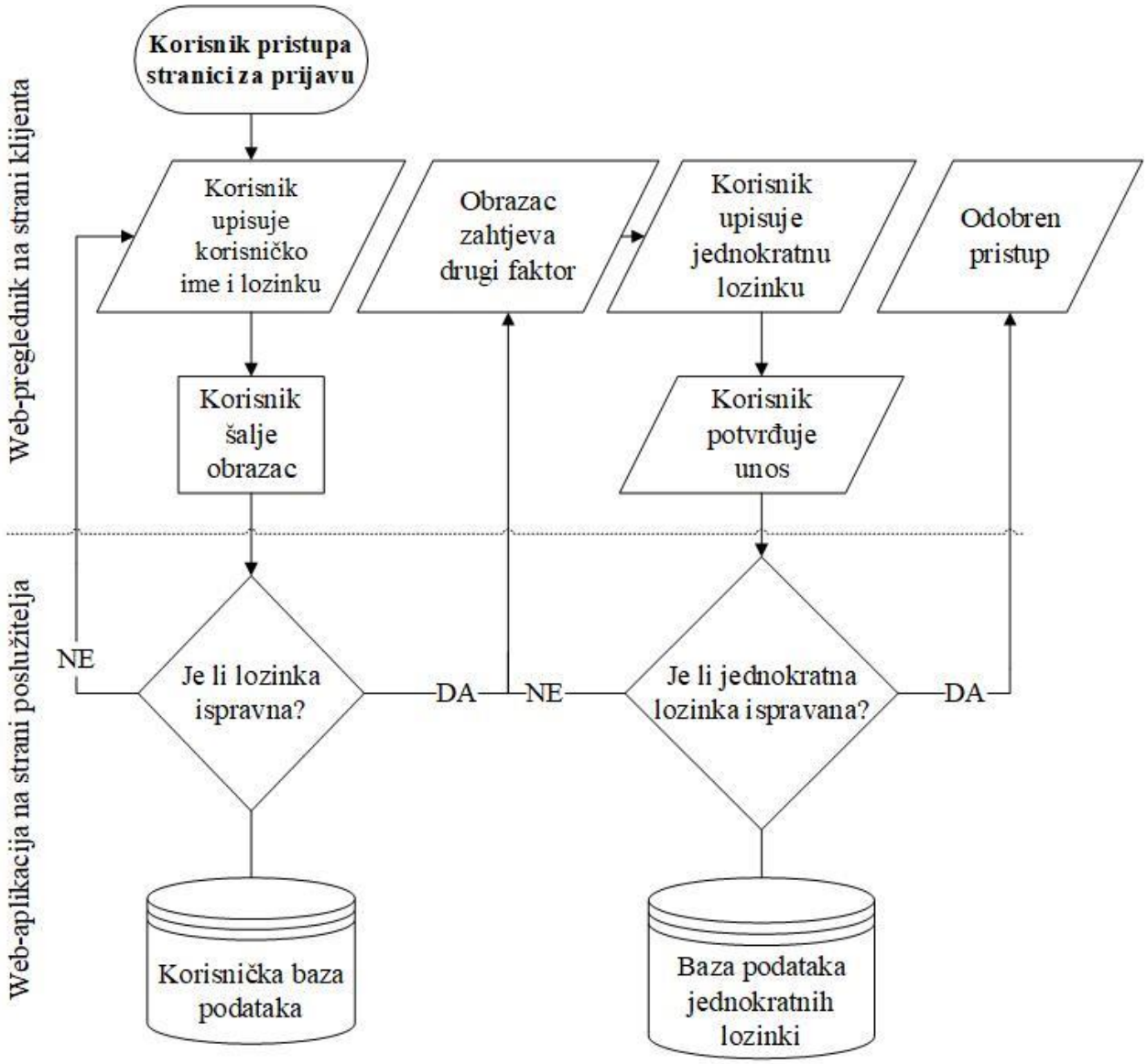
- Ažuriranje softvera – Redovito ažuriranje operativnog sustava i antivirusnih softvera može pomoći pri zaustavljanju novijih vrsta kibernetičkih napada. Većina uređaja dozvoljava ažuriranje nakon radnih sati kako ne bi ometali korisnike u njihovom radu, pa tako korisnik može odabrati vrijeme koje mu odgovara kako bi se izvršilo ažuriranje. Ažuriranje često dolazi sa zakrpama koje popravljaju ozbiljne sigurnosne nedostatke, stoga je izuzetno bitno da se ažuriranja ne ignoriraju.
- Postavljanje vatrozida (engl. *Firewall*) – S obzirom na to da su danas sva računala povezana s internetom, napadači imaju velike mogućnosti za pronalaženje ranjivih računala. Vatrozid može spriječiti napadače ili druge vanjske prijetnje da uopće dobiju pristup osobnom računalu. Vatrozid nadgleda cijeli mrežni promet te prepoznaje i blokira neželjeni promet. Postavljanje vatrozida zaštitit će osobno računalo korisnika, a korisnici također mogu blokirati pristup internetu određenim aplikacijama.
- Sigurnosni softver – Korištenje sigurnosnog softvera kao što su anti-virusi, anti-spyware i anti-spam filteri smanjuje šansu zaraze računala. Njihova učinkovitost ovisi o redovitosti ažuriranja. Stoga je bitno da se sigurnosti softver ažurira svakodnevno. Većina sigurnosnih programa koristi baze podataka ili liste poznatih kibernetičkih prijetnji kako bi ih usporedili s programima na osobnom računalu i ostalim korisničkim uređajima. Njihovo ograničenje je da pružaju zaštitu samo protiv poznatih kibernetičkih prijetnji. Ako postoji kibernetička prijetnja koja nije u bazi podataka sigurnosnog softvera, postoji šansa da ta prijetnja neće biti zaustavljena, [33].

3.3. Enkripcija osjetljivih i privatnih podataka

Enkripcija je postupak korištenja algoritama kako bi podaci bili nečitljivi svima koji ih pokušaju pročitati bez dozvole. Jedan od najboljih načina enkripcije podataka na Internetu je korištenje Virtualne privatne mreže (engl. *Virtual Private Network* - VPN). Međutim, jednako je bitno kriptirati i lokalno spremljene podatke. Enkripcija lokalne pohrane, kao npr. prijenosnog tvrdog diska, dobar je način da se osiguraju osjetljivi podaci u slučaju da se tvrdi disk izgubi. Postoje dva načina enkripcije tvrdih diskova: Enkripcija cijelog diska (engl. *Full-disk encryption* - FDE) i Samokriptirajući diskovi (engl. *Self-encrypting drives* - SED). FDE se koristi kod prijenosnih računala jer su podložni gubljenju ili krađi, međutim nije pogodan za korištenje u podatkovnim centrima i cloud okruženjima, [34].

3.4. Višefaktorska provjera autentičnosti

Višefaktorska provjera autentičnosti (engl. *Multifactor authentication*, MFA) je sigurnosna tehnologija koja zahtjeva nekoliko metoda autentifikacije kako bi se provjerio korisnikov identitet tijekom prijave ili neke druge transakcije. Višefaktorska provjera autentičnosti kombinira 2 ili više vjerodajnice, naprimjer lozinku koju korisnik zna napamet i sigurnosni token kao naprimjer biometrijska verifikacija na mobilnim terminalnih uređajima. Cilj MFA je stvaranje višeslojne zaštite koja će onemogućiti pristup osobnom računalu, mobilnom uređaju ili mreži neautoriziranom korisniku ili napadaču. Ako napadač zna lozinku, i dalje će mu trebati token, koji samo legitimni korisnik može generirati. Najčešće se koristi 2FA (engl. *two-step authentication*) u obliku mobilnih aplikacija, SMS poruka ili glasovnih poruka kako bi se smanjila mogućnost kibernetičkog napada, [35].



Slika 9. Dijagram toka klasične autentifikacije u dva koraka

Izvor: [36]

3.5. Korištenje kompleksnih lozinki

Korištenje kompleksnih lozinki uvijek je bolje od korištenja jednostavnih lozinki. Kompleksne lozinke nastaju korištenjem kombinacije više riječi, velikih i malih slova, brojeva, te znakova. Korištenjem takvih lozinki praktički onemogućuje korištenje brute-force metode napadanja, jer bi vrijeme potrebno za probijanje takve lozinke bilo predugačko da bi bilo isplativo. Također se preporučuje korištenje sugeriranih lozinki, a danas nije ni potrebno pamtiti sve te različite lozinke napamet uporabom *password manager*-a.

3.6. Podukom korisnika umreženih uređaja

Prva linija obrane protiv kibernetičkih napada je poduka korisnika umreženih uređaja. Korisnici mogu naučiti kako upravljati lozinkama, kako identificirati kibernetičke prijetnje, što učiniti ako naiđu na kibernetičku prijetnju i kako ju prijaviti ovlaštenim tijelima. Također bitno je znati koje stranicu su sigurne za koristiti a koje nisu, jer postoji mogućnost kibernetičkog napada i preko reklama koje je prikazuju na stranici, ako se klikne na njih i preuzme sumnjiva datoteka, [33].

4. Programski alati za zaštitu računala od kibernetičkih prijetnji

Izuzetno je bitno zaštititi mrežno okruženje. Svaki pojedinac treba shvatiti kibernetičku sigurnost ozbiljno. Kibernetička sigurnost odnosi se na zaštitu mreža, korisničkih uređaja i njihovih podataka protiv neautoriziranog pristupa. Ne postoji garancija da korisnik Interneta neće postati žrtva kibernetičkog napada čak i ako je dobro upoznat s kibernetičkim prijetnjama. Svrha programskih alata za zaštitu od kibernetičkih prijetnji je da uklone zlonamjerne softvere ili datoteke koje mogu ugroziti sigurnost osobnih računala. Te vrste softvera često su povezane sa softverom za nadzor računala.

4.1. Antivirusni softver

Antivirusni softver vrsta je programa koji je dizajniran za otkrije, prevenira i ukloni različite vrste *malware* zaraza na osobnim računalima i mrežama. Antivirusni softveri originalno su dizajnirani da otkriju i uklone različite vrste virusa s računala, te da spriječe različite vrste napada, kao što su trojanski konji, crvi, *adware*, *bot*-ovi i *keylogger*-i. Mnogi antivirusni softveri rade u pozadini, skeniraju računala u unaprijed određeno dan i vrijeme, te stavljaju sumnjive programe i datoteke u karantenu, pritom informirajući korisnika o pronađenoj kibernetičkoj prijetnji.

Funkcije antivirusnog softvera su:

- Detektiranje, blokiranje i uklanjanje *malware*-a i *ransomware*-a
- Sprječavanje krađe identiteta
- Upozoravanje na sumnjive i opasne *web*-stranice prije ulaska na njih
- Skeniranje *Dark Web*-a za provjeru kompromitiranog e-mail računa
- Zaštita online računa sigurnosnom enkripcijom lozinki
- Dozvoljavanje korisnicima da pokrenu skeniranje računala u bilo kojem trenutku

Da bi antivirusni softver mogao opsežno skenirati sistem, treba imati privilegijski pristup. To ga čini čestom metom napadačima ako nije često ažuriran. Antivirusne aplikacije koriste više slojeva obrane kako bi zaštitile osobna računala od svih štetnih i sumnjivih stvari koje se nalaze na Internetu. Ključni elementi su zaštita u stvarnom vremenu heuristička tehnologija koja bi trebala prepoznati još nepoznate prijetnje, pri tome pomažući da korisnikovo osobno računalo postane sigurnije mjesto. Jedan od najkorištenijih antivirusnih softvera je Windows Security koji Microsoft nudi svojim korisnicima Windows operativnog sustava besplatno od 2004. godine, [37].

4.2. Softver za otkrivanje zlonamjernih programa

Softver za otkrivanje zlonamjernih programa (engl. *Anti-malware*) je vrsta softverskog programa koji je kreiran da zaštiti računalne sustave i osobna računala od kibernetičkih prijetnji poput *malware*-a. Po imenu softvera može se pogoditi da je svrha *Anti-malware*-a prevencija, detekcija i uklanjanje *malware*-a. *Anti-malware* koristi dvije strategije kako bi zaštitio računalo od zlonamjernog softvera:

Otkrivanje zlonamjernog softvera utemeljenog na potpisu – Ako Anti-malverski program koristi otkrivanje na temelju potpisa, njegovo znanje o tome što spada i zlonamjerni softver dolazi iz njegovog repozitorija, koji redovito ažuriraju ljudi identificirajući zlonamjerno ponašanje nekog softvera i izraziti ga u oblik podložan repozitoriju potpisa, te na kraju stroju koji taj repozitorij čita. Drugi unos koji Anti-malverski program mora uzeti u obzir je program koji se pregledava. Nakon što *Anti-malware* prepoznaje što se smatra zlonamjernim ponašanjem i koji program pregledava, može koristiti vlastitu tehniku otkrivanja kako bi odlučio radi li se o zlonamjernom programu ili ne.

Otkrivanje zlonamjernog softvera utemeljenog na ponašanju – Ova metoda otkrivanja procjenjuje promatrani softver prema njegovim namjeravanima radnjama prije nego što zlonamjerni softver može izvršiti planiranu radnju. To se obično postiže slanjem sumnjivog softvera u *sandbox* te potom aktivacijom. Ponašanje sumnjivog softvera analizira se za sumnjive aktivnosti. Svaki njegov pokušaj izvođenja radnji koje su očito abnormalne ili neovlaštene ukazuje na to da je softver sumnjiv ili zlonamjeran. *Sandbox* je sigurnosna značajka koja se često koristi kod anti-malverskih programa za izolaciju potencijalno zlonamjernih datoteka od ostatka sustava i njihovo uklanjanje prije nego što imaju priliku napraviti štetu, [38].

4.3. Protušpijunski softver

Protušpijunski softver (engl. *Anti-spyware*) za cilj ima sprječavanje i otkrivanje neželjenog špijunskog softvera te njegovo uklanjanje. *Anti-spyware* provodi rutinske provjere na osobnom računalu kako bi osigurao da je sustav čist, te također štiti privatnost od mogućih napada. Rizik ovih softvera je lažno predstavljanje na Internetu. Danas je česta pojava lažnog predstavljanja, a *Anti-spyware* je popularna meta takvih napada. Obično je vrlo jednostavno prepoznati razliku između pravog i lažnog *Anti-spyware* softvera, a to je gledanjem recenzija na Internetu, [39].

4.4. Softver protiv napada praćenja unosa tipkovnice

Zadatak softvera protiv napada praćenja unosa tipkovnice (engl. *anti-keylogger*) je detekcija bilo kakvog napada praćenja unosa tipkovnice (engl. *keylogger*) koji se nalazi u sustavu. Njegova je sposobnost da zaustavi *keylogger* prije nego što krene s radom kako bi spriječio napadača u saznavanju korisničkih lozinki. Korištenje *anti-keylogger*-a ključan je način osiguranja privatnosti i osobnih detalja. Slično kao i *Anti-malware, Anti-keylogger* softver koristi dva načina otkrivanja *keylogger* zlonamjernih programa:

Na temelju potpisa – *Anti-keylogger* softver provjerava postoji li prisutnost *keylogger*-a unutar neke datoteke, te ju označava kao zlonamjernu ako rezultat bude pozitivan. Također daju korisniku osobnog računala do znanja zašto softver smatra da je označena datoteka zlonamjerna. Općenit nedostatak svih softvera koji koriste otkrivanje temeljem potpisa je što mogu samo prepoznati *keylogger*-e koji se nalaze na listi zlonamjernih softvera. Ako se radi o najnovijoj vrsti prijetnje, ova vrsta *Anti-keylogger*-a vrlo vjerojatno neće moći označiti datoteku kao prijetnju dok se ne ažurira lista koja uključuje tu prijetnju.

Na temelju ponašanja – također znan kao i heuristički način detekcije. Sadržava značajke pomoću kojih može prepoznati *keylogger* aktivnost koje se smatraju zlonamjernima. Ako napadač koristi *keylogger* kako bi dobio pristup unosa tipkovnice, ova vrsta *Anti-keylogger*-a prepoznati će njegovu aktivnost te ju zaustaviti prije nego što dođe do štete, [40].

4.5. Softver za detekciju napada na uobičajeno ponašanje programa

Postupak koji natjera softver da izvodi nenamjerne radnje bilo neovlaštenim miješanjem programskog kôda ili promjenom ponašanja naziva se napad mijenjanja uobičajenog ponašanja programa. Primjer toga je neovlašteno miješanje kôda za promjenu programskog koda radi učitavanja zlonamjernih pravila. Ubacivanje SQL kôda također je oblik subverzije u svrhu korupcije podataka ili krađe osobnih podataka. Softver za detekciju napada na uobičajeno ponašanje programa (engl. *Anti-subversion)* otkriva pokušaj promjene uobičajenog ponašanja programa i pokušava zaustaviti zlonamjerne učinke. *Anti-subversion* zaštita postiže se statičkim i dinamičkim načinom:

Statička detekcija napada na uobičajeno ponašanje programa – obavlja se tijekom izgradnje kôda. Kôd se statički ispituje i provjerava protiv različitih vrsta napada proučavanjem programskog izvornog kôda. Neki od primjera statičke Anti-subverzije su revizije sigurnosti i verifikacija kôda. Ova vrsta zaštite obično se smatra dobrom praksom u kodiranju i neophodna je u nekim režimima usklađenosti. Međutim, kao i ostala rješenja, ne može spriječiti sve vrste *Subversion* napada

Dinamička detekcija napada na uobičajeno ponašanje programa – za razliku od statičke anti-subverzije, dinamička se obavlja tijekom izvršavanja kôda. Kôd je dinamički zaštićen od *Subversion* napada tako što se ponašanje programa stalno provjerava. Primjeri dinamičke Anti-subverzije su vatrozidi i zaštita ugrađena u softver, [41].

4.6. Softver za zaštitu od neovlaštenog pristupa

Softver za zaštitu neovlaštenog pristupa (engl. *Anti-Tamper*) je program koji otežava izmjenu originalnog softvera. U početku, ovaj naziv se upotrebljavao za postupak osiguranja medija kao što su filmovi i muzika, ali s obzirom na to da danas više nitko ne iznajmljuje filmove u obliku DVD-a, taj naziv je promijenio značenje u Copyright. Međutim, kada se govori o softveru, samo značenje se nije promijenilo. Neke od načina zaštite neovlaštenog pristupa je otežanje takozvane „reverse engineering“ metode koja pokušava rekreirati originalni program, a zatim ga izmijeniti po želji napadača. Česte žrtve ovih napada su skoro svi programi koji su se napravili za operativne sustave, pa i sami operativni sustavi. Nažalost, ne postoji metoda koja može u potpunosti zaustaviti neovlašteno izmjenjivanje kôda neke aplikacije. Stoga se danas ide prema tome da proizvođač aplikacije uvijek održava svoj softver i dodaje nove funkcije, a istovremeno drži kompetitivnu cijenu, kako bi privukao legitimne kupce, [42].

4.7. Vatrozid

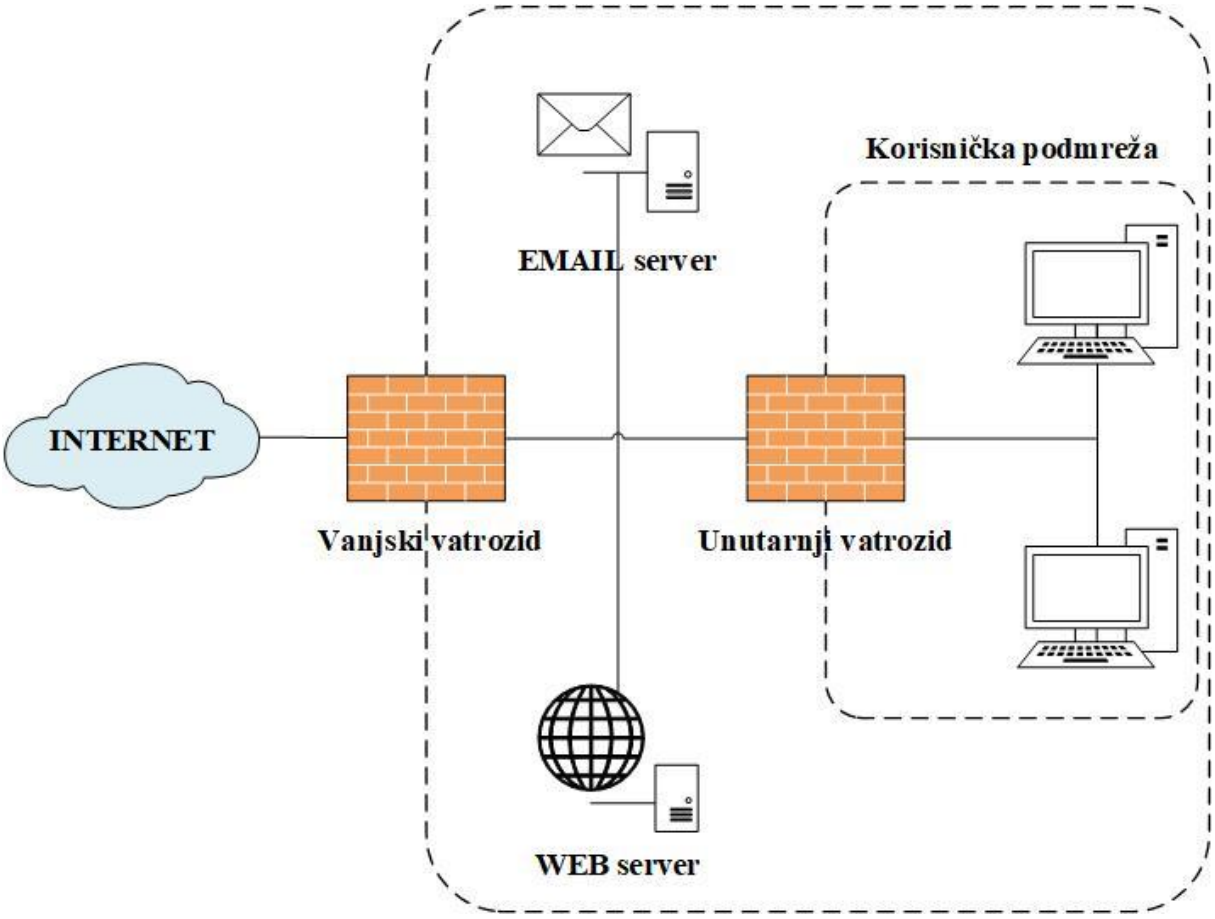
Vatrozid je sustav koji nudi mrežnu sigurnost filtriranjem dolaznog i odlaznog mrežnog prometa na temelju skupa korisničkih pravila. Njegov općenit zadatak je smanjiti ili zaustaviti pojavu neželjenih mrežnih komunikacija. U većini osobnih računala, vatrozid pruža potrebnu razinu sigurnosti koja, zajedno s drugim mjerama, sprječava napadače da pristupe sustavu na zlonamjerni način. Postoje 3 osnovne vrste mrežnog vatrozida:

1. Vatrozid za filtriranje paketa (engl. *Stateless Firewall*)
2. Vatrostalni zid (engl. *Stateful Firewall*)
3. Vatrozid aplikacijskog sloja

Vatrozid za filtriranje paketa djeluje na mrežnom sloju OSI modela i donosi odluke o obradi na temelju mrežnih adresa, portova ili protokola. *Stateless Firewall* vrlo je brz jer nema puno logike koja stoji iza odluka koje se donose. Također se ne pohranjuju nikakvi podaci. Portovi se moraju ručno otvoriti za sav promet koji će teći kroz vatrozid. Vatrozidi za filtriranje paketa smatraju se nesigurnim zato što će proslijediti sav promet koji teče u odabranom portu. Stoga, iako je promet zlonamjeran, sve dok dolazi na prihvaćen port, neće biti blokiran.

Vatrostalni zid nalazi se na mrežnom i transportnom sloju OSI modela. To je vrsta vatrozida koji prati stanje aktivnih mrežnih veza tijekom analiziranja dolaznog prometa tražeći potencijalne kibernetičke prijetnje. Vatrostalni zid mogu otkriti neovlaštene pokušaje pristupanja mreži, te analizirati podatke u paketima kako bi utvrdili sadrže li zlonamjerni kôd.

Vatrozid aplikacijskog sloja filtrira podatke na aplikacijskom sloju. Njegov je posao dopustiti ili zabraniti veze unutar mreže prema Internetu i dopustiti ili zabraniti komunikaciju koja dolazi s Interneta i usmjerava se na lokalnu mrežu korisnika. Filtriranje na aplikacijskom sloju nudi najveću razinu sigurnosti, ali je puno sporiji i više opterećuje procesor računala prilikom pregleda svakog paketa naspram druge dvije vrste vatrozida. Međutim, s razvojem računala, pa tako i njihovih procesora, opterećenje vatrozida ne predstavlja nikakav problem današnjim procesorima s četiri ili više jezgri, [43].



Slika 10. Prikaz vatrozida u Internetskoj mreži

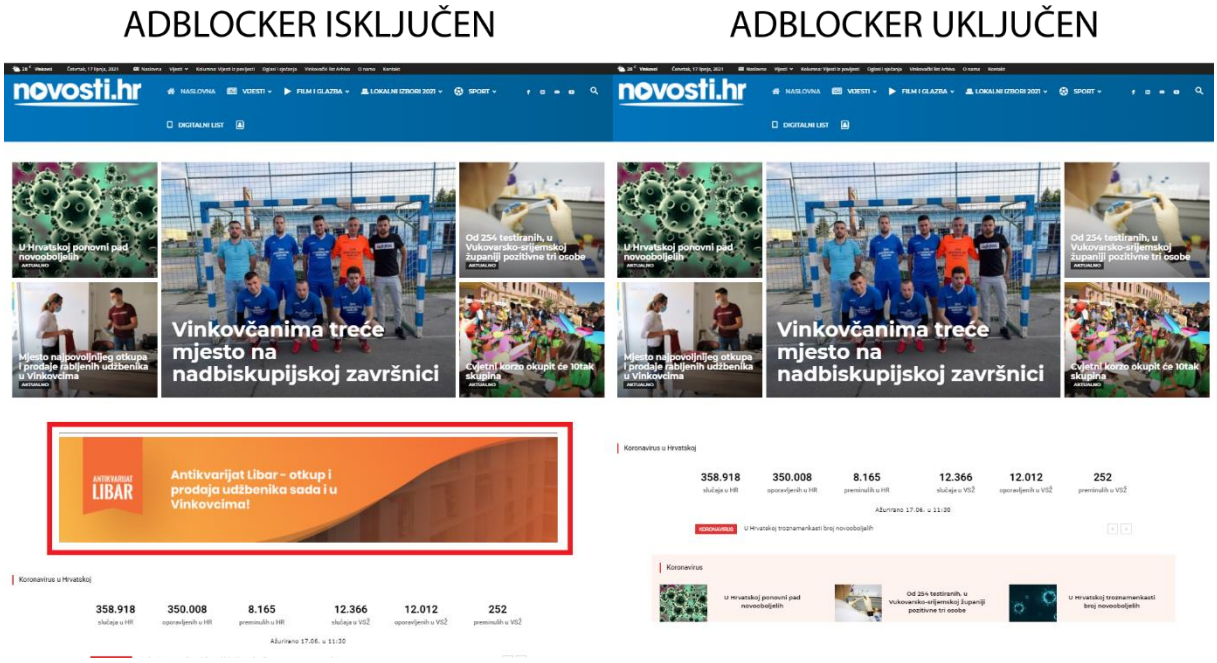
Izvor: [44]

Vatrozidi sljedeće generacije (engl. *Next Generation Firewall*) su naprednija verzija klasičnog vatrozida i nude iste prednosti. Kao i klasični vatrozidi, vatrozidi sljedeće generacije koriste statičko i dinamičko filtriranje paketa i VPN podršku kako bi se osiguralo da sve veze između mreže, Interneta i vatrozida budu sigurne. Najbitnija razlika između klasičnih vatrozida i vatrozida sljedeće generacije je sposobnost filtriranja paketa na temelju aplikacija. Osim toga, vatrozidi sljedeće generacije nude optimiziranu sigurnosnu infrastrukturu koja je jednostavnija i jeftinija za održavanje, ažuriranje i kontrolu, [45].

Jedinstveno upravljanje prijetnjama (engl. *Unified threat management*) opisuje informacijski sigurnosni sustav koji pruža jedinstvenu točku zaštite od kibernetičkih prijetnji. Kombinira produktivne, sigurnosne i upravljačke mogućnosti u jednoj instalaciji, koja olakšava administratorima upravljanje mrežama. Za razliku od antivirusnih alata, UTM ne štiti samo osobna računala i poslužitelje, nego i cijelu mrežu uključujući pojedinačne korisnike skeniranjem i filtriranjem potencijalno opasnog sadržaja i blokiranjem napada, [46].

4.8. Alati za blokiranje oglasa

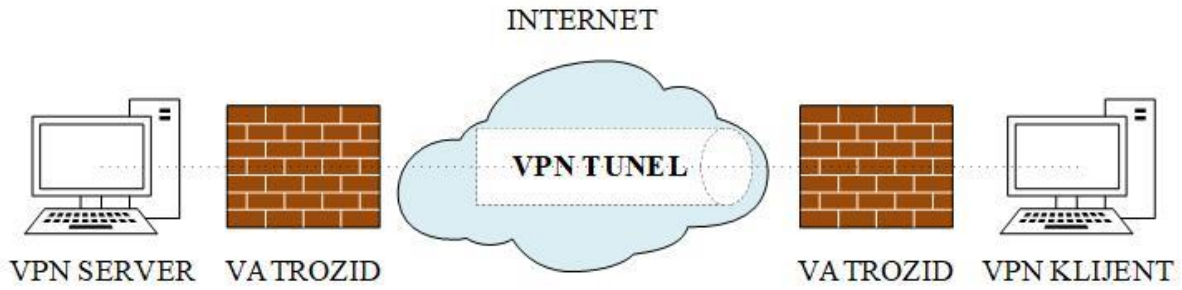
Alati za blokiranje oglasa (engl. *Adblocker)* je softver, najčešće u obliku proširenja *web*-preglednika, koji mijenjaju ili uklanjaju sadržaj oglasa na *web*-stranici. Ovisno o tome koje su liste za blokiranje odabrane, mogu se blokirati različite vrste oglasa, a najčešće su napravljeni da blokiraju iritantne oglas pop skočnih prozora i *banner*-a. Njihov cilj je ukloniti zlonamjerne oglase koji se predstavljaju kao normalni oglasi, ali prilikom klika na njih preuzima se zlonamjerni softver preko kojeg napadač može izvršiti kibernetički napad. Prednosti korištenja ovog softvera je produljivanje životnog vijeka baterije prijenosnog osobnog računala, brže vrijeme učitavanja stranica, uklanjanje dosadnih reklama i zaštita privatnosti.



Slika 11. Usporedba *web*-stranice s ugašenim i upaljenim *adblocker-om*

4.9. Virtualna privatna mreža

Virtualna privatna mreža (engl. *Virtual Private Network*) povezuje osobno računalo, tablet ili pametni telefon s poslužiteljem negdje na *web*-u i omogućuje pregledavanje Interneta preko internetske veze tog poslužitelja. Stoga, ako se poslužitelj nalazi u drugoj zemlji, izgledat će kao da korisnik dolazi iz te zemlje i ovisno o stranici, moći će se pristupiti stvarima koje inače korisnik ne bi mogao vidjeti. VPN je usluga koja stvara sigurnu i kriptiranu mrežnu vezu. Osim toga, osigurava se veća privatnost i anonimnost na Internetu. Korisnik bi tipično želio koristiti VPN na javnoj mreži kako bi izbjegao napade poput MITM i prisluškivanja. VPN koristi protokol tuneliranja koji radi enkripciju podataka koji se šalju s izvorišta i dekriptiraju se tek kada dođu na odredište.



Slika 12. Pojednostavljeni prikaz rada VPN-a

Izvor: [47]

4.10. Testiranje sigurnosti probijanjem sigurnosti

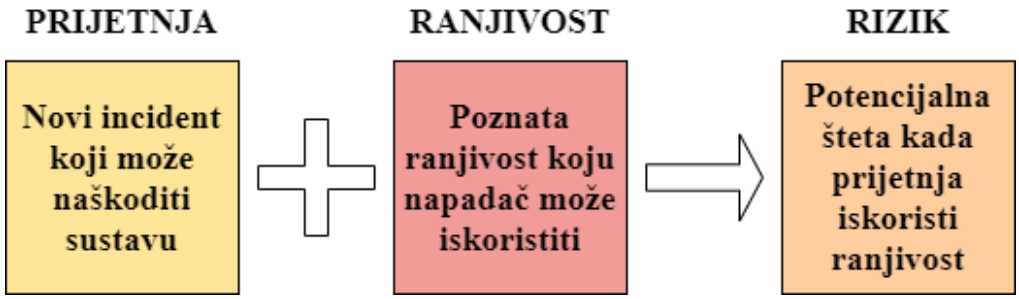
Testiranje sigurnosti probijanjem sigurnosti metoda je testiranja *web*-aplikacije i mreže kako bi se otkrili sigurnosni propusti koje bi napadač mogao iskoristiti. Glavni razlog testiranja sigurnosti probijanjem je učenje osoblja kako se nositi s bilo kojom vrstom kibernetičkog napada. Ovi testovi služe kao način provjere plana odaziva na kibernetičke napade te određivanje njihove učinkovitosti. Različite vrste testova probijanja uključuju fizičko i aplikacijsko probijanje te probijanje mrežnih usluga i bežične povezivosti. Može se izvesti interno ili eksterno kako bi se simulirali različiti kutovi i pristupi napada. Ovisno o ciljevima testa, osoba koja provodi test može ali i ne mora imati prethodno predznanje o sustavu koji pokušava probiti. Tako se testiranje sigurnosti probijanjem sigurnosti može podijeliti na 3 načina testiranja:

1. *Black box*
2. *White box*
3. *Gray box*

Tijekom *Black box* testiranja, osoba koja testira sustav ne prima nikakve informacije o infrastrukturi sustava. Glavna prednost ove metode testiranja je realna simulacija stvarnog kibernetičkog napada u kojem osoba koja testira sustav preuzima ulogu neinformiranog napadača. Tijekom *White box* testiranja, osoba koja testira sustav ima potpun pristup o arhitekturi i *source code*-u sustava, a cilj je provesti dubinsku reviziju sigurnosti sustava, znajući da osoba koja testira sustav zna sve dalje o njemu. Tijekom *Gray box* testiranja, osoba koja testira sustav imat će djelomično znanje ili pristup internoj mreži ili *web*-aplikaciji, a cilj je saznati koji su to pojedini dijelovi sustava u najvećem riziku tijekom kibernetičkog napada, [48].

5. Smjernice prevencije i planiranje odaziva na kibernetičke napade

Kada se pokušava zaštititi osobno računalo na internetu, trebalo bi znati i načine na koje se korisnik može zaštititi kada se dogodi kibernetski napad. Prvi korak za ublažavanje bilo koje vrste napada je identifikacija zlonamjernog softvera ili kibernetičkog napada koji se trenutno događa. Zatim se moraju analizirati i procijeniti sve pogođene strane i datotečni sustavi koji su ugroženi. Na kraju se mora tretirati cijeli sustav kako bi se sustav mogao vratiti u prvobitno radno stanje, bez ikakvih narušavanja sigurnosti. To se uglavnom radi izračunavanjem tri čimbenika: ranjivosti, prijetnje i rizika.



Slika 13. Rizik kao zbroj prijetnje i ranjivosti

Ranjivost se odnosi na poznatu slabost imovine koju može iskoristiti jedan ili više napadača. Drugim riječima, to je poznata slabost koje omogućuje da napad bude uspješan. Na primjer, kada član tima podnese ostavku i zaboravi onemogućiti pristup vanjskim računima, promijeniti podatke za prijavu ili ukloniti imena s kreditnih kartica tvrtke, to ostavlja tvrtku otvorenom za namjerne i nenamjerne prijetnje. Međutim, većinu ranjivosti iskorištavaju automatizirani napadači, a ne ljudi koji tipkaju s druge strane mreže. Zato je testiranje ranjivosti ključno kako bi se osigurala kontinuirana sigurnost vaših sustava prepoznavanjem slabih točaka i pojačanjem strategije za brz odaziv na kibernetičke prijetnje. Postoje pitanja koja se postavljaju prilikom određivanja sigurnosnih ranjivosti kao što su npr. jesu li podaci sigurnosno kopirani i pohranjuju li se na sigurnom mjestu izvan lokacije računala (engl. *offsite backup*)? Postoje li podaci spremljeni u oblaku? Ako da, kako se točno štite ranjivosti oblaka? Kakva vrsta sigurnosti se koristi kako bi se odredilo tko može pristupiti, izmijeniti ili izbrisati podatke s računala? Kakva se antivirusna zaštita koristi? Postoji li plan oporavka podataka? To su pitanja koja se obično postavljaju kada se provjeravaju ranjivosti.

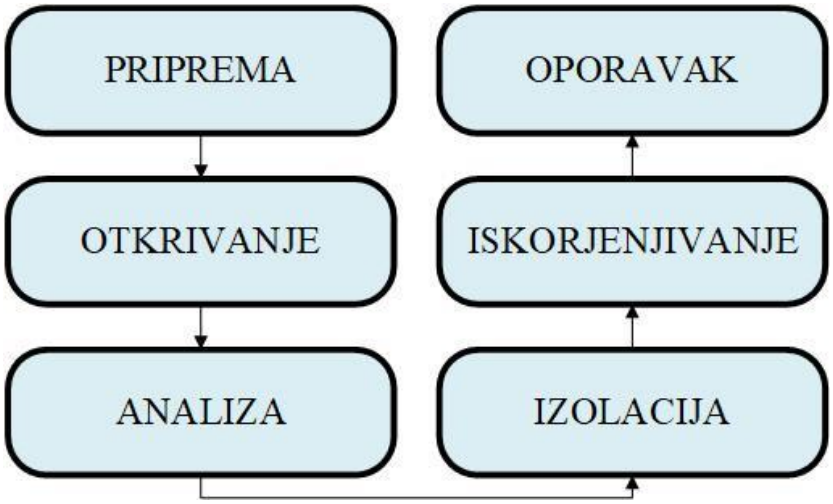
Prijetnja se odnosi na novi ili novootkriveni incident koji potencijalno može naštetiti sustavu. Postoje 3 glavne vrste prijetnji: Nacionalne prijetnje, poput poplava ili tornada. Nenamjerne prijetnje poput radnika koji slučajno pristupi pogrešnim informacijama te namjerne prijetnje, za koje postoji mnogo primjera, uključujući *spyware*, *malware* i *adware*, a

crvi i virusi su kategorizirani kao prijetnje jer mogu potencijalno naštetiti uređajima zbog izloženosti i automatiziranih napada. Iako su ove prijetnje uglavnom izvan kontrole korisnika i teško ih je unaprijed identificirati, neophodno je redovito poduzimati odgovarajuće mjere za procjenu prijetnji.

Rizik se odnosi na potencijal gubitka ili oštećenja kada prijetnja iskoristi ranjivost. Primjer rizika uključuje financijske gubitke, gubitak privatnosti, imovinsku štetu i pravne implikacije. Rizik se također može definirati na sljedeći način: prijetnja pomnožena s ranjivošću. Potencijal rizika može se smanjiti stvaranjem i primjenom plana upravljanja rizikom, a ovdje su ključni aspekti koje treba uzeti u obzir prilikom izrade strategije upravljanja rizikom. Prvo treba procijeniti rizike i odrediti potrebe. Kada je riječ o dizajniranju i provedbi okvira za procjenu rizika, od ključne je važnosti odrediti najvažnije napade koji će se adresirati prvi. Iako se učestalost može razlikovati u svakoj organizaciji, ova se razina ocjenjivanja mora redovito provoditi. Upravljanje rizicima ključ je kibernetičke sigurnosti, [49].

Plan odaziva na kibernetičke napade određuje koje korake treba poduzeti i tko ih treba poduzeti, u trenutku kada dođe do poboja u sigurnosti. Kvalitetno napravljen plan odaziva omogućit će brzo djelovanje i samim time smanjiti količinu učinjene štete. Kada je riječ o kibernetičkim napadima, isplati se biti spreman. Svaka minuta je bitna kada je sigurnost mreže ili osobnog računala kompromitirana, a dodano čekanje dok se shvati što se ustvari događa povećavaju ukupno vrijeme reagiranja na incident.

Plan odaziva na kibernetičke napade (engl. *cybersecurity incident response plan*) set je instrukcija namijenjene pomaganju u pripremi, otkrivanju, odgovoru i oporavku od kibernetičkih napada. Većina tih planova usmjerena je na tehnologiju i rješava probleme poput krađe osobnih i osjetljivih podataka, otkrivanja zlonamjernog softvera i distribuiranih uskraćivanja usluga. Međutim, bilo koji značajan kibernetički napad može utjecati na organizaciju na više načina, tako da bi plan odaziva trebao obuhvaćati područja kao što su financije, služba za korisnike, dobavljači i partneri, lokalne vlasti i korisnike, [50]. Način kreiranja plana odaziva na kibernetičke napade može se svesti na 6 koraka:



Slika 14. Koraci planiranja odaziva na kibernetičke prijetnje

Faza pripreme je prva faza planiranja odaziva na kibernetičke prijetnje te možda i najvažnija u zaštiti osobnih računala i digitalne imovine. Priprema za bilo koji potencijalni sigurnosti incident ključ je uspješnog odaziva. Spremnost uključuje, [51]:

- Dizajniranje, razvoj, obuku i provedbu plana organizacije
- Stvaranje smjernica za komunikaciju kako bi se osigurala dobra komunikacija tijekom i nakon kibernetičkog napada
- Provođenje simulacija kibernetičkih napada za evaluaciju učinkovitosti plana odaziva na kibernetičke prijetnje.

Faza otkrivanja je proces u kojem se određuje ako je sigurnost nekog sustava kompromitirana ili ne. Kibernetički napadi mogu se pojaviti u različitim dijelovima sustava. Cilj ove faze u planiranju je nadziranje mreža i sustava radi otkrivanja, upozoravanja i izvještavanja o potencijalnim sigurnosnim incidentima. Rezultat je utvrđivanje ozbiljnosti, vrste i opasnosti kibernetičkog napada te spremanje tih informacija kao dokaze protiv napadača na sudu, [51].

Faza analize - Kako bi se dobilo pravilno razumijevanje sigurnosnog incidenta, velik dio napora dolazi iz ove faze. To uključuje, [51]:

- Prikupljanje informacija te određivanje prioriteta pojedinih kibernetičkih napada i koraka odaziva
- Forenzičko očuvanje i analiza podataka za određivanje opsega i posljedica kibernetičkog napada

- Tijekom kibernetičkog napada, tim za odaziv treba se usredotočiti na tri područja: Analiza krajnjih točaka, Binarna analiza te takozvani „*Enterprise hunting*“

Analiza krajnjih točaka za zadatak ima određivanje tragova koje je napadač ostavio te analizu kopije sustava kako bi se utvrdilo što se dogodilo na uređaju tijekom kibernetičkog napada. Binarna analiza usredotočuje se na analizu zlonamjernih alata i datoteka koje je napadač koristio te dokumentacija funkcionalnosti tih programa. *Enterprise hunting* odnosi se na analizu postojećih sustava i zapisnika događaja kako bi se odredio opseg kibernetičkog napada te dokumentaciju svih ugroženih sustava, uređaja i računa, [51].

Faza izolacije - Nakon što se opseg kibernetičkog napada uspješno odredi, moguće je započeti proces izolacije. U ovom procesu su svi ugroženi uređaji izolirani od ostatka mreže kako bi se zaustavilo širenje napada. Loša je ideja sigurnosno sve izbrisati jer se istovremeno brišu svi dokazi kojima se može utvrditi gdje je kibernetički napad počeo i na osnovu toga izraditi plan kako bi se spriječilo ponavljanje sličnog napada u budućnosti. Sljedeći korak je određivanje kratkoročnih i dugoročnih strategija izolacije. Kratkoročna izolacija može se koristiti za izolaciju uređaja prema kojem je usmjeren sva promet napada. Dugoročno ograničenje može biti potrebno kada je potrebna *deep-dive* analiza koja je dugog trajanja, a u to spada stvaranje nove preslike uređaja i provođenje pregleda tvrdih diskova. Također, preporučeno je imati sigurnosnu kopiju sustava kako bi se ubrzao oporavak. Pitanja na koja treba odgovoriti kada se provodi faza izolacije, [51]:

- Što treba učiniti kako bi se provela kratkoročna strategija izolacije?
- Što treba učiniti kako bi se provela dugoročna strategija izolacije?
- Postoji li otkriven zlonamjerni softver koji je izoliran od ostatka sustava?
- Postoje li sigurnosne kopije?
- Potrebna li je autentifikacija s više faktora za pristup sustavu?
- Jesu li se sve vjerodajnice provjerile za dostojnost i jesu li promijenjene?
- Jesu li primijenjene najnovije zakrpe i sigurnosna ažuriranja?

Faza iskorjenjivanja - Nakon izolacije kibernetičke prijetnje, potrebno je i ukloniti korijen prijetnje. Svi zlonamjerni softveri moraju se pouzdano ukloniti, a sustavi se moraju ojačati zakrpama i ažuriranjima. Bilo da korisnik to uradi sam, ili zaposli treću stranu za to, izuzetno je bitno biti detaljan. Ako postoje tragovi zlonamjernog softvera ili drugih sigurnosnih problema u osobnom računalu, još uvijek postoji mogućnost gubljenja osobnih i osjetljivih podataka. Pitanja koja moraju biti odgovorena u fazi iskorjenjivanja, [51]:

- Jesu li svi zlonamjerni softveri sigurno uklonjeni?
- Jesu li instalirane najnovije zakrpe i ažuriranja sustava?
- Moguće li je stvoriti novu presliku sustava?

Faza oporavka - Zadnji korak u planiranju odaziva na kibernetičke prijetnje je uklanjanje sigurnosnih prijetnji , analizu i izvješćivanje o incidentu, ažuriranje trenutnog plana odaziva imajući na umu što se dogodilo, te zatim procijeniti sveukupnu štetu i sigurnost sustava, [51].

6. Zaključak

Metode i alati za zaštitu osobnih računala od kibernetičkih prijetnji stalno napreduju, kako napreduju i digitalne tehnologije. Sukladno razvoju tehnologije rastu i vrste kibernetičkih napada, a njihov broj također svakodnevno raste. Kako bi korisnici zaštitili svoja osobna računala, a time i svoje osjetljive podatke potrebno je kontinuirano razvijati metode i alate koji će to omogućiti. Neki od najefektivnijih načina zaštite protiv kibernetičkih napada su sigurnosne kopije podataka, enkripcija osjetljivih podataka, korištenje višestruke provjere autentičnosti te podukom korisnika o kibernetičkim prijetnjama.

Kada se govori o kibernetičkoj sigurnosti, postoje tri glavne aktivnosti od kojih se osobna računala pokušavaju zaštititi, a to su: neovlaštena izmjena, neovlašteno brisanje i neovlašteni pristup. Kibernetičke prijetnje se općenito klasificiraju na mrežno temeljene napade i napade temeljenih na informacijskom sustavu. Kibernetičke prijetnje razvijaju se kroz vrijeme iskorištavanjem novih pristupa, najčešće modificiranjem postojećih zlonamjernih softvera. Održavanjem sigurnosti osobnih računala smanjuje se mogućnost kibernetičkih napada koji mogu doći u obliku raznih zlonamjernih softvera i izravnih pokušaja kibernetičkih napada usmjerenih na krađu osobnih i osjetljivih podataka. Svrha programskih alata za zaštitu od kibernetičkih prijetnji je da uklone zlonamjerne softvere ili datoteke koje mogu ugroziti sigurnost osobnih računala. Te vrste softvera često su povezane sa softverom za nadzor računala. Smjernice prevencije kibernetičkih napada sastoje se od tri čimbenika: prijetnja, ranjivost i rizik. Plan odaziva na kibernetičke napade određuje koje korake treba poduzeti i tko ih treba poduzeti, u trenutku kada dođe do poboja u sigurnosti. Kvalitetno napravljen plan odaziva omogućit će brzo djelovanje i samim time smanjiti količinu učinjene štete.

Literatura

[1] CertMike. Confidentiality, Integrity And Availability – The CIA Triad. Preuzeto sa: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/ [Pristupljeno: svibanj 2021.]

[2] Nacionalni CERT. Godišnji izvještaj rada nacionalnog CERT-a za 2019. godinu, Zagreb, 2020.

[3] Nacionalni CERT. Godišnji izvještaj rada nacionalnog CERT-a za 2020. godinu, Zagreb, 2021.

[4] Acunetix. What Is a Web Application Attack and how to Defend Against It. Preuzeto sa: https://www.acunetix.com/websitesecurity/web-application-attack/ [Pristupljeno: svibanj 2021.]

[5] Lifars. Injection attacks explained. Preuzeto sa: https://lifars.com/2020/04/injection-attacks-explained/ [Pristupljeno: svibanj 2021.]

[6] Nithya V, Pandian Lakshmana S, Malarvizhi C. A Survey on Detection and Prevention of Cross-Site Scripting Attack. Internation Journal of Security and Its Applications. 2015;9(3): 139-152.

[7] PortSwigger. Server-side template injection. Preuzeto sa: https://portswigger.net/web-security/server-side-template-injection [Pristupljeno: svibanj 2021.]

[8] Donald R, Ligatti J. Defining code-injection attacks. ACM SIGPLAN Notices. 2012;47(1): 179-190.

[9] Shahriar H, Haddad H, Bulusu P. LDAP Vulnerability Detection in Web Applications. Marietta: Kennesaw State University; 2017.

[10] Stasinopoulos A, Ntantogian C, Xenakis C. Commix: automating evaluation and exploitation of command injection vulnerabilities in Web applications. International Journal of Information Security. 2019;18(1): 49-72.

[11] The Ecomonic Times. Definition of "DNS Spoofing". Preuzeto sa: https://economictimes.indiatimes.com/definition/dns-spoofing [Pristupljeno: svibanj 2021.]

[12] A. A. Maksutov, I. A. Cherepanov and M. S. Alekseev, "Detection and prevention of DNS spoofing attacks," 2017 Siberian Symposium on Data Science and Engineering (SSDSE), 2017, pp. 84-87, doi: 10.1109/SSDSE.2017.8071970.

[13] Kaspersky. Brute Force Attack: Definition and Examples. Preuzeto sa: https://www.kaspersky.com/resource-center/definitions/brute-force-attack [Pristupljeno: svibanj 2021.]

[14] Owasp. Session hijacking attack. Preuzeto sa: https://owasp.org/www-community/attacks/Session_hijacking_attack [Pristupljeno: svibanj 2021.]
[15] An effective method for preventing SQL injection attack and session hijacking. Preuzeto sa: https://www.semanticscholar.org/paper/An-effective-method-for-preventing-SQL-injection-D'silva-Vanajakshi/4594dddef4184b4cfd81ed4f6979760cb71fcebd [Pristupljeno: svibanj 2021.]
[16] Cisco. What is Phishing?. Preuzeto sa: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works [Pristupljeno: svibanj 2021.]
[17] ResearchGate. Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages. Preuzeto sa: https://www.researchgate.net/publication/325568402_Prevention_of_Phishing_Attacks_Based_on_Discriminative_Key_Point_Features_of_WebPages [Pristupljeno: svibanj 2021.]
[18] Cloudflare. What is a DDoS attack?. Preuzeto sa: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [Pristupljeno: svibanj 2021.]
[19] Cvitic, I., Perakovic, D., Gupta, B., & Choo, K.-K. R. (2021), Boosting-based DDoS Detection in Internet of Things Systems. IEEE Internet of Things Journal, 4662(c), 1-1. https://doi.org/10.1109/JIOT.2021.3090909
[20] Cvitic, I., Perkovic, D., Periša, M., & Husnjak, S. (2019). An Overview of Distributed Denial of Service Traffic Detection Approaches. PROMET . Traffic&Transportation, 31(4), 453-464. https://doi.org/10.7307/ptt.v41i4.3082
[21] Perakovic, D., Perisa, M., Cvitic, I., & Husnjak, S. (2017). Artificial neuron network implementation in detection and classification of DDoS traffic. TELFOR Journal, 9(1), 26-31. https://doi.org/10.1109/TELEFOR.2016.7818791
[22] OperaVPS. How To Detect And Prevent DDoS Attacks?. Preuzeto sa: https://operavps.com/detect-and-prevent-ddos-attacks/ [Pristupljeno: svibanj 2021.]
[23] PentaSecurity. Types of DDoS Attacks: General Breakdown. Preuzeto sa: https://www.pentasecurity.com/blog/ddos-attacks-types-explanation/ [Pristupljeno: svibanj 2021.]
[24] TechTarget. Dictionary Attack. Preuzeto sa: https://searchsecurity.techtarget.com/definition/dictionary-attack [Pristupljeno: svibanj 2021.]
[25] Mallik A (2019). Man In The Middle Attack: Understanding in simple words. Jurnal pendidikan teknologi informasi, 2(2). http://dx.doi.org/10.22373/cj.v2i2.3453

[26] WallStreet. A Complete Guide to Man in The Middle Attack (MitM). Preuzeto sa: https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/ [Pristupljeno: svibanj 2021.]
[27] M. Bhardwaj, G.P. Singh. Types of Hacking Attack and their Counter Measure. 2011;1(1): 43-53
[28] The Economic Times. Definition of "Computer Virus". Preuzeto sa: https://economictimes.indiatimes.com/definition/computer-virus [Pristupljeno: svibanj 2021.]
[29] Norton. What is a computer worm, and how does it work?. Preuzeto sa: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html [Pristupljeno: svibanj 2021.]
[30] Hasan M. Z, Hussain M. Z, Ullah Z. Computer Viruses, Attacks, and Security Methods. Lahore: Lahore Garrison University; 2019.
[31] Imperva. Backdoor Attack. Preuzeto sa: https://www.imperva.com/learn/application-security/backdoor-shell-attack/ [Pristupljeno: svibanj 2021.]
[32] Gupta, B. B., Tewari, A., Cvitić, I., Peraković, D., & Chang, X. (2021). Artificial intelligence empowered emails classifier for Internet of Things based system sin industry 4.0. Wireless Networks.
[33] Australian Government. How to protect your business from cyber threats. Preuzeto sa: https://business.gov.au/online/cyber-security/how-to-protect-your-business-from-cyber-threats [Pristupljeno: lipanj 2021.]
[34] L. Hars, "Discryption: Internal Hard-Disk Encryption for Secure Storage," in Computer, vol. 40, no. 6, pp. 103-105, June 2007, doi: 10.1109/MC.2007.202.
[35] TechTarget. Multifactor authentication (MFA). Preuzeto sa: https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA [Pristupljeno: lipanj 2021.]
[36] ResearchGate. WiFiOTP: Pervasive two-factor authentication using Wi-Fi SSID broadcasts. Preuzeto sa: https://www.researchgate.net/publication/283489178_WiFiOTP_Pervasive_two-factor_authentication_using_Wi-Fi_SSID_broadcasts [Pristupljeno: lipanj 2021.]
[37] Webroot. What is Antivirus Software?. Preuzeto sa: https://www.webroot.com/us/en/resources/tips-articles/what-is-anti-virus-software [Pristupljeno: lipanj 2021.]
[38] TechTarget. Antimalware (anti-malware). Preuzeto sa: https://searchsecurity.techtarget.com/definition/antimalware [Pristupljeno: lipanj 2021.]

[39] Study. What Is Anti-Spyware? - Definition & Programs. Preuzeto sa: https://study.com/academy/lesson/what-is-anti-spyware-definition-programs.html [Pristupljeno: lipanj 2021.]
[40] GeeksforGeeks. Anti-keylogger. Preuzeto sa: https://www.geeksforgeeks.org/anti-keylogger/ [Pristupljeno: lipanj 2021.]
[41] Freejournal Organization. Anti-subversion software. Preuzeto sa: https://amp.ww.en.freejournal.org/35683261/1/anti-subversion-software.html [Pristupljeno: lipanj 2021.]
[42] Whitehawk. What is software tamper-proofing?. Preuzeto sa: http://www.whitehawksoftware.com/white-hawk-technology/what-is-software-tamper-proofing/ [Pristupljeno: lipanj 2021.]
[43] PaceTechnical. Netowrk Firewalls Explained. Preuzeto sa : https://pacetechnical.com/2013/04/30/network-firewalls-explained/ [Pristupljeno: lipanj 2021.]
[44] D. Soper. Firewalls and Network Security. Preuzeto sa: https://www.youtube.com/watch?v=XEqnE_sDzSk [Pristupljeno: lipanj 2021.]
[45] Cisco. What Is a Next-Generation Firewall?. Preuzeto sa: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html [Pristupljeno: lipanj 2021.]
[46] Kaspersky. What is Unified Threat Management (UTM)?. Preuzeto sa: https://usa.kaspersky.com/resource-center/definitions/utm [Pristupljeno: lipanj 2021.]
[47] VPNMentor. The Ultimate Guide to VPN Tunneling & How To Use It In 2021. Preuzeto sa: https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/ [Pristupljeno: lipanj 2021.]
[48] V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart and S. Chotivatunyu, "PENTOS: Penetration testing tool for Internet of Thing devices," TENCON 2017 - 2017 IEEE Region 10 Conference, 2017, pp. 2279-2284, doi: 10.1109/TENCON.2017.8228241.
[49] Umberger H., Gheorghe A. (2011) Cyber Security: Threat Identification, Risk and Vulnerability Assessment. In: Gheorghe A., Muresan L. (eds) Energy Security. NATO Science for Peace and Security Series C: Environmental Security. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-0719-1_13
[50] Cisco. What Is an Incident Response Plan for IT?. Preuzeto sa: https://www.cisco.com/c/en/us/products/security/incident-response-plan.html [Pristupljeno: lipanj 2021.]

[51] SecurityMetrics. The Six Steps to Build an Effective Cyber Incident Response Plan. Preuzeto sa: https://www.stealthlabs.com/blog/the-six-steps-to-build-an-effective-cyber-incident-response-plan/ [Pristupljeno: lipanj 2021.]

Popis kratica

2FA	Two-factor Authentication
CIA	Central Intelligence Agency
CRLF	Carriage Return Line Feed
DDOS	Distributed Denial of Service
DNA	Deoxyribonucleic acid
DNS	Domain Name System
DVD	Digital Versatile Disc
FDE	Full-disk encryption
HTTP	Hypertext Transfer Protocol
ID	Identity document
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MFA	Multifactor Authentication
MITM	Man In The Middle
NGFW	Next Generation Firewall
OS	Operating System
OSI	Open Systems Interconnection
OTG	On The Go
RNA	Ribonucleic Acid
SED	Self-encrypting drives
SMS	Short Message Service
SQL	Structured Query Language
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
UTM	Unified Threat Management
VPN	Virtual Private Network
XSS	Cross-Site Scripting

Popis slika

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Pregled metoda i alata zaštite osobnih računala od kibernetičkih prijetnji**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 02/07/2021

Student/ica:

Luka Pavić

(potpis)