Pregled metoda i alata primjenjivih u zaštiti mrežne komunikacije

Zdrilić, Luka

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Luka Zdrilić

PREGLED METODA I ALATA PRIMJENJIVIH U ZAŠTITI MREŽNE KOMUNIKACIJE

ZAVRŠNI RAD

Zagreb, 2022.

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. 6254

Pristupnik: **Luka Zdrilić (0135248050)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Pregled metoda i alata primjenjivih u zaštiti mrežne komunikacije**

Opis zadatka:

U okviru završnog rada potrebno je pružiti osvrt na sigurnosne aspekte mrežne komunikacije, te pružiti pregled potencijalnih prijetnji mrežne komunikacije. Na temelju prethodnih osvrta potrebno je analizirati dostupna programska rješenja te druge primjenjive metode dostupne u povećanju razine sigurnosti mrežne komunikacije.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

PREGLED METODA I ALATA PRIMJENJIVIH U ZAŠTITI MREŽNE KOMUNIKACIJE

OVERVIEW OF METHODS AND TOOLS APPLICABLE IN THE PROTECTION OF NETWORK COMMUNICATION

Mentor: dr. sc. Ivan Cvitić

Student: Luka Zdrilić

JMBAG: 0135248050

Zagreb, rujan 2022.

PREGLED METODA I ALATA PRIMJENJIVIH U ZAŠTITI MREŽNE KOMUNIKACIJE

SAŽETAK

Korisnici danas provode veliki dio svog dana na internetu, a taj trend raste iz godine u godinu. Iako takav ubrzani razvoj interneta i mrežne komunikacije ima veliki broj prednosti, on ima i neke nedostatke. Glavni nedostatak je pitanje sigurnosti. Zlonamjerni korisnici na internetu sa trendom rasta popularnosti mrežne komunikacije pronalaze sve veći broj načina kako bi ostvarili svoju korist putem raznih tipova prevara na internetu. S obzirom na velik broj zlonamjernih korisnika koji prevare čine u svrhu ostvarivanja financijske koristi ili krađe osobnih podataka, potrebno je pronaći sve bolje vrste rješenja koja će korisnike zaštititi od zlonamjernih sadržaja i koja će im pružiti mogućnost korištenja interneta za zabavu, edukaciju i komunikaciju.

KLJUČNE RIJEČI: *Internet; sigurnost; mrežna komunikacija; zlonamjerni sadržaji*

OVERVIEW OF METHODS AND TOOLS APPLICABLE IN THE PROTECTION OF NETWORK COMMUNICATION

SUMMARY

Users today spend much of their day online, and this trend is growing every year. Although such an accelerated development of the Internet and network communication has a number of advantages, it also has some disadvantages. The main drawback is the issue of security. Malicious users on the Internet with the growing trend of popularity of network communication are finding an increasing number of ways to gain their benefit through various types of fraud on the Internet. Given the large number of malicious users who commit fraud for the purpose of financial gain or theft of personal data, it is necessary to find better solutions that will protect users from malicious content and that will give them the opportunity to use the Internet for entertainment, education and communication.

KEYWORDS: *Internet; security; network communication; malicious content*

SADRŽAJ

1. UVOD

Globalizacija je donijela ubrzani razvoj interneta i otvaranje svijeta i mogućnosti za svakoga. Ljudi danas provode veliki dio svog dana na internetu, a taj trend raste iz godine u godinu. Iako takav ubrzani razvoj interneta i mrežne komunikacije ima veliki broj prednosti, on ima i neke nedostatke. Glavni nedostatak je pitanje sigurnosti. Zlonamjerni korisnici na internetu sa trendom rasta popularnosti mrežne komunikacije pronalaze sve veći broj načina kako bi ostvarili svoju korist putem raznih tipova prevara na internetu.

S obzirom na velik broj zlonamjernih korisnika koji prevare čine u svrhu ostvarivanja financijske koristi ili krađe osobnih podataka, potrebno je pronaći sve bolje vrste rješenja koja će korisnike zaštititi od zlonamjernih sadržaja i koja će im pružiti mogućnost korištenja interneta za zabavu, edukaciju i komunikaciju.

U ovom završnom radu raspravljati će se o pitanju sigurnosti mrežne komunikacije. Cilj rada je objasniti sigurnosne aspekte mrežne komunikacije i dati uvid čitateljima u mogućnosti koje se pružaju kada je riječ o zaštiti podataka na internetu.

Rad je podijeljen u pet poglavlja:

1. Uvod
2. Sigurnosni aspekti mrežne komunikacije
3. Pregled prijetnji mrežnoj komunikaciji
4. Metode zaštite mrežne komunikacije
5. Zaključak

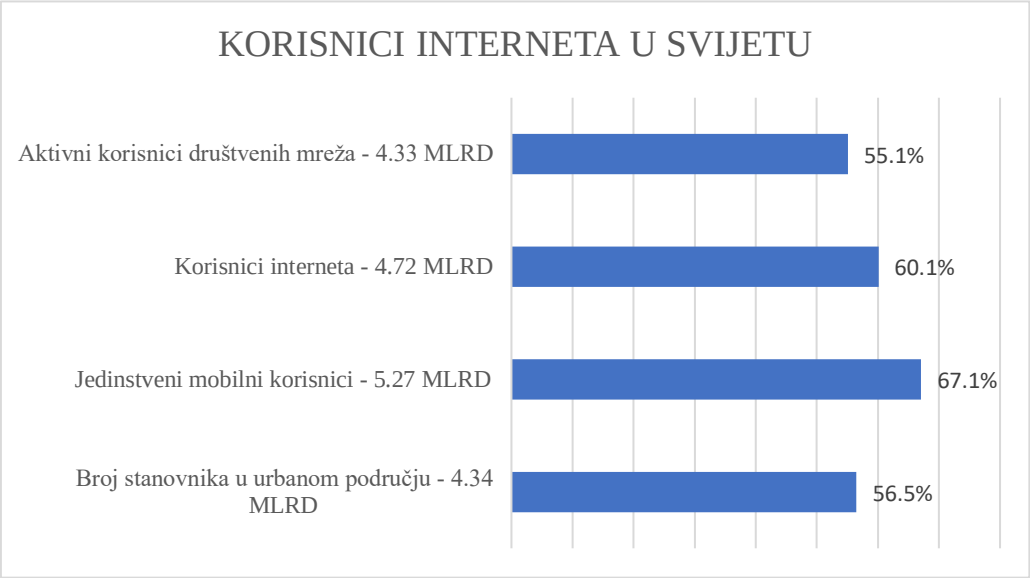
Nakon uvodnog dijela u drugom poglavlju analizira se sigurnost korištenja digitalne tehnologije. Također prikazuju se podaci o broju korisnika interneta u svijetu, broju korisnika koji koriste društvene mreže te o aktivnosti korisnika na e-trgovini. Opisuju se i tri važna aspekta informacijske sigurnosti, koja uvelike doprinose sigurnosti bilo kojeg oblika mrežne komunikacije.

U trećem poglavlju prikazane su razne sigurnosne prijetnje koje se mogu pojaviti u mrežnoj komunikaciji. Nabrojane su i opisane vrste zlonamjernih programa čija je svrha nezakonito prikupljanje informacija i dokumentacija od raznih korisnika.

U četvrtom poglavlju prikazane su vrste i način rada pojedinih programskih rješenja koja nude zaštitu mrežne komunikacije.

2. SIGURNOSNI ASPEKTI MREŽNE KOMUNIKACIJE

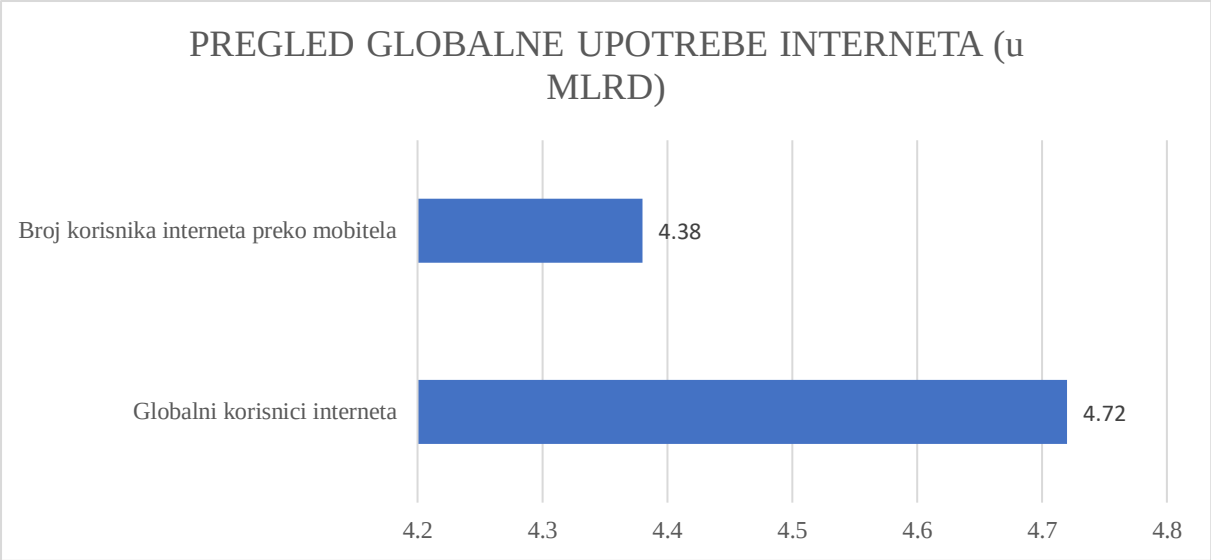
Globalizacija je uvelike utjecala na razvoj novih tehnologija i na prelazak korisnika diljem svijeta na digitalne tehnologije. Razlog tome leži u činjenici kako nove tehnologije omogućuju pristupačnost i nova rješenja za korisničke probleme i izazove. Grafikon 1 prikazuje globalne statistike o korištenju interneta [1].



Grafikon 1 Korisnici interneta u svijetu, [1]

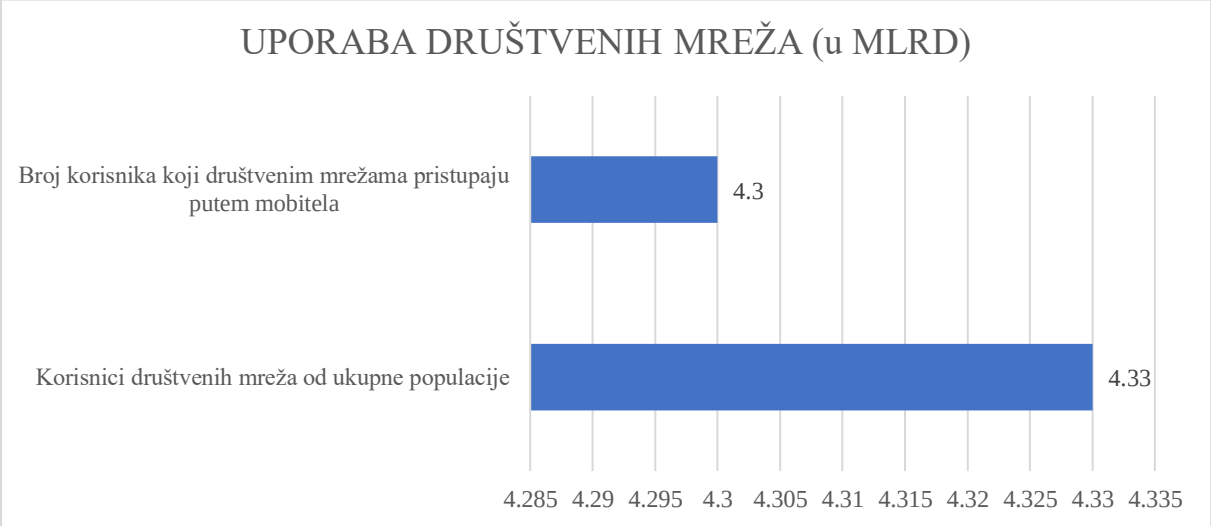
Prema podacima za travanj 2021. godine, svjetska populacija broji 7,85 milijardi stanovnika, od čega 56,5% stanovništva živi u urbanom području. U svijetu ima 5,27 milijardi korisnika mobilnih telefona što čini 67,1% populacije. Također, 60,1% populacije koristi Internet, odnosno 4,72 milijarde ljudi. Društvene mreže koristi 4,33 milijarde ljudi, odnosno 55,1% populacije [1].

Na Grafikon 2 prikazana je godišnja promjena broja internetskih korisnika u svijetu koja je u povećanju za 7,6%. Korisnici dnevno u prosjeku provode na internetu 6 sati i 56 minuta, a zanimljivo je kako čak 92,8% korisnika internetu pristupa putem mobilnih uređaja [1].



Grafikon 2 Pregled globalne upotrebe interneta, [1]

Grafikon 3 prikazuje broj korisnika društvenih mreža koji je u konstantnom porastu i trenutno broji 4,33 milijarde korisnika. Postotak populacije koja koristi društvene mreže je 55,1%. Godišnja promjena u broju korisnika društvenih mreža bilježi povećanje od 13,7%. Postotak korisnika društvenih mreža koji im pristupaju putem mobilnog uređaja je 99%. Prosječno dnevno korisnici na društvenim mrežama provedu 2 sata i 22 minute [1].



Grafikon 3 Uporaba društvenih mreža, [1]

Grafikon 4 prikazuje aktivnost svjetske populacije na internetskim trgovinama. Od ukupnog broja korisnika, 81,8% je pretraživalo Internet zbog proizvoda ili usluge koju su željeli kupiti, 92,2% njih je posjetilo neku *web* trgovinu, 44,0% je posjetilo neku od *online* stranica za aukcije, 78,6% je onih koji su kupili neki proizvod *online*, a 40,1% korisnika je prodalo proizvod *online* [1].

Grafikon 4 Aktivnost na e-trgovini, [1]

S obzirom na trendove razvoja i korištenja Internet mreže i usluga prikazanih na prethodnim grafovima, posljedično se ističe sve veći broj izazova sigurnosti korisnika. Sigurnost čini prihvatljivu razinu nekog rizika i proces održavanja te razine. Informacijska sigurnost predstavlja disciplinu koja ima za cilj osigurati zaštitu informacijskih sustava i informacija od neovlaštenog pristupanja, primjene, korištenja i/ili uništavanja [2].

Svaki informacijski sustav ima za cilj zaštititi informacije od izmjena koje se rade na neovlašten način. To znači da se mora osigurati integritet i pristup informacijama ovlaštenim korisnicima te zaštititi informacije od neovlaštenog preuzimanja i objavljivanja [3].

Postoje tri aspekta informacijske sigurnosti, a to su [3]:

- Povjerljivost,
- Integritet,
- Dostupnost.

Prvi aspekt informacijske sigurnosti odnosi se na povjerljivost podataka. Povjerljivost podataka podrazumijeva tajnost podataka. To znači da pristup podacima ili informacijskim sustavima trebaju imati samo ovlaštene osobe. Kod aspekta povjerljivosti podataka najveća pažnja je usmjerena na autentifikaciju i identifikaciju korisnika [3].

Drugi aspekt se odnosi na integritet. Integritet predstavlja činjenicu da informacije i podaci ne mogu biti izmijenjeni bez ovlaštenja korisnika, odnosno da se neovlaštenim osobama ne dozvoljavaju neovlaštene promjene informacija i podataka [3].

Cilj integriteta kao sigurnosnog aspekta je spriječiti neovlaštene korisnike da naprave modifikaciju podataka ili programa i spriječiti ovlaštene korisnike da naprave modifikaciju podataka ili programa na način koji nije propisan i ovlašten. Cilj je također i održati konzistentnost podataka i programa [3].

Treći aspekt sigurnosti informacijskih sustava je dostupnost. Taj aspekt predstavlja dostupnost informacija i podataka, a njegov najviši cilj je postići osiguranje pravovremene

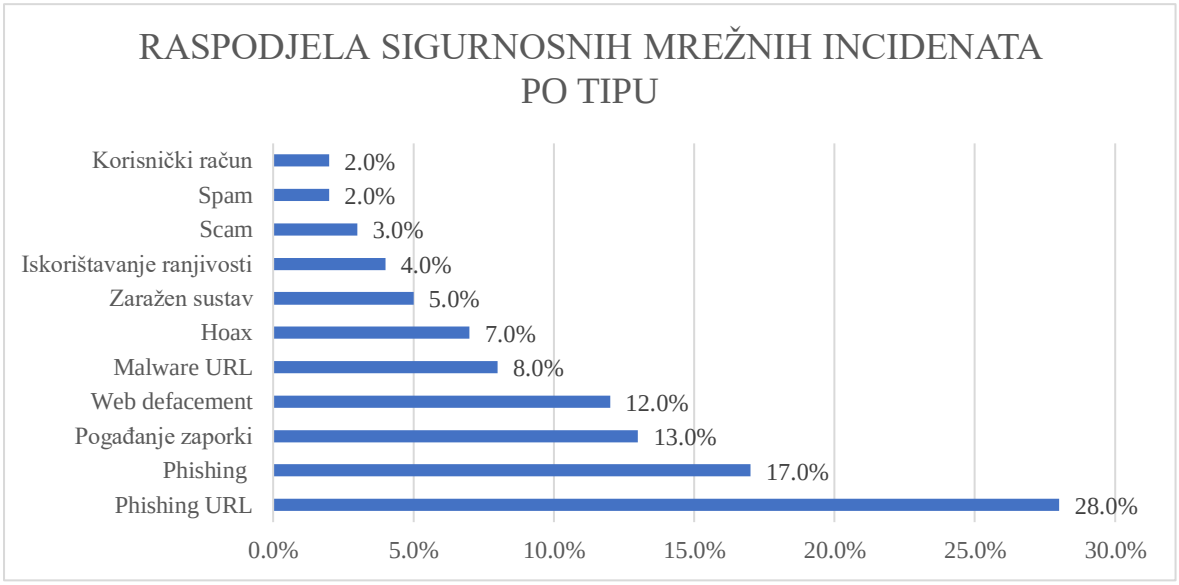
dostupnosti podataka korisnicima. Održavanje *hardwera*, nadogradnja *softwera* i optimizacija mreže osiguravaju dostupnost [3].

Osim navedena tri aspekta u novije vrijeme postoje razmišljanja kako bi u sigurnosni trokut trebalo ubaciti još neke aspekte, a to su dokazivost, autentičnost i neporecivost, no postoje i protivnici ove teze jer smatraju da su ova tri aspekta već uključena u osnovni sigurnosni trokut [2].

Što se tiče zakonskog sustava koji štiti informacije na mreži, u Republici Hrvatskoj se može izdvojiti nekoliko glavnih institucija i zakona. Institucije koje se brinu o informacijskoj sigurnosti su [2]:

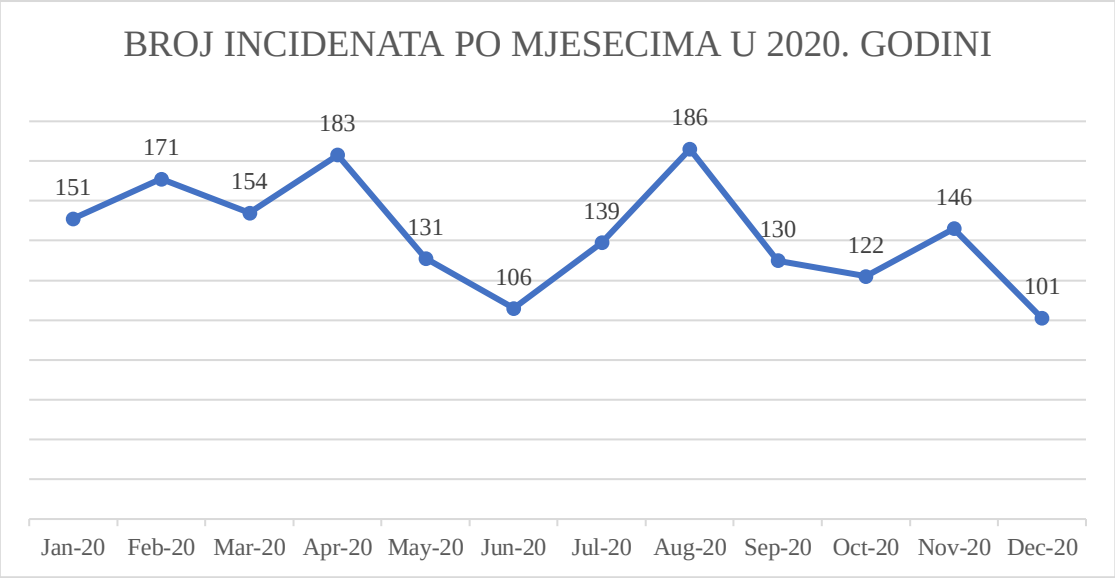
- Nacionalni CERT (engl. *Computer Emergency Response Team*),
- CARNet,
- Zavod za sigurnost informacijskih sustava ZSIS,
- Ured vijeća za nacionalnu sigurnost,
- Agencije za podršku informacijskim sustavima i informacijskim tehnologijama,
- Agencija za zaštitu osobnih podataka,
- Središnji državni ured za e-Hrvatsku.

Nacionalni CERT redovno objavljuje izvješća o sigurnosti interneta i informacijskih sustava.



Grafikon 5 Raspodjela sigurnosnih mrežnih incidenata po tipu, [4]

Grafikon 5 prikazuje raspodjelu incidenata po tipu u 2020. godini. Može se iščitati kako je spektar incidenata raznolik, ali i kako više od četvrtine mrežnih incidenata čini *Phishing* URL.



Grafikon 6 Broj incidenata po mjesecima u 2020. godini, [21]

Grafikon 6 prikazuje krivulju rasta i pada sigurnosnih incidenata po mjesecima u 2020. godini. Godina je započela sa 151 incidentom u siječnju. U veljači je zabilježen porast, a dogodio se 171 incident. U ožujku je ponovno zabilježen pad sa 154 incidenta, međutim u travnju se događa nagli porast sa 183 incidenta što predstavlja jednu od dvije najviše točke krivulje. Svibanj bilježi pad incidenata na 131 slučaj, a pad se nastavlja i u lipnju kada je zabilježeno 106 slučajeva. Nakon toga krivulja ponovo počinje naglo rasti, pa se u srpnju bilježi 139 incidenata, a u kolovozu čak 186 što čini drugu najvišu točku krivulje. Nakon kolovoza ponovno počinje pad u rujnu sa 130 incidenata. Pad se nastavlja do listopada kada je zabilježeno 122 incidenta. Nakon toga se ponovo događa rast u studenom sa 146 incidenata, pa pad u prosincu sa 101 incidentom [21].

Razlog povećanja broja incidenata u kolovozu je korištenje inteligencije otvorenog koda OSINT (engl. *Open source intelligence*) metoda kojom je otkriven veći broj zlonamjernih stranica i kompromitiranih *web* sjedišta s izmijenjenim izgledom i sadržajem *web* stranica. Nacionalni CERT je poslao prijave svim nadležnim pružateljima usluga udomljavanja Internet stranica [21].

3. PREGLED PRIJETNJI MREŽNOJ KOMUNIKACIJI

S obzirom na razvoj interneta i mrežne komunikacije, podrazumijeva se da od tolikog broja korisnika, nemaju svi dobre namjere. Neki korisnici koriste internetske mogućnosti kako bi prevarili druge korisnike. CERT navodi da je kibernetička sigurnost zapravo glavni temelj sigurnog poslovanja i djelovanja u današnjem dobu koje je nadasve informacijsko i digitalno [5]. Važni pojmovi za ovo područje su hakeri financijske koristi (engl. *black hat*), hakeri koji poštuju zakon (engl. *white hat*) i hakeri dobrih i loših namjera (engl. *grey hat*).

Black hat je pojam koji se odnosi na pojedince koji svoje znanje o komunikacijskim i informacijskim sustavima koriste u zlonamjerne svrhe. Ovakvi pojedinci su često tvorci nekih zlonamjernih sadržaja pomoću kojih pokušavaju ukrasti podatke od drugih korisnika. Mnogi ovakvi pojedinci dobivaju financijsku korist od svojih zlonamjernih radnji [5].

White hat je pojam koji se odnosi na etičke hakere koji svoje znanje o komunikacijskim i informacijskim sustavima koriste kako bi povećali razinu sigurnosti. Ovakvi pojedinci imaju dobronamjerne razloge i koriste hakerske sposobnosti kako bi uočili i prijavili problem sigurnosti nekog sustava. Često sudjeluju u inovativnim rješenjima [5].

Grey hat je pojam koji se odnosi na pojedince koji imaju i svojstva *black hat* i svojstva *white hat* pojedinaca. Oni svoja znanja i vještine u komunikacijskim i informacijskim sustavima mogu koristiti i za dobre i za loše namjere, no najčešće ne koriste ova znanja za osobni dobitak [5].

3.1. Vrste napada krađe identiteta

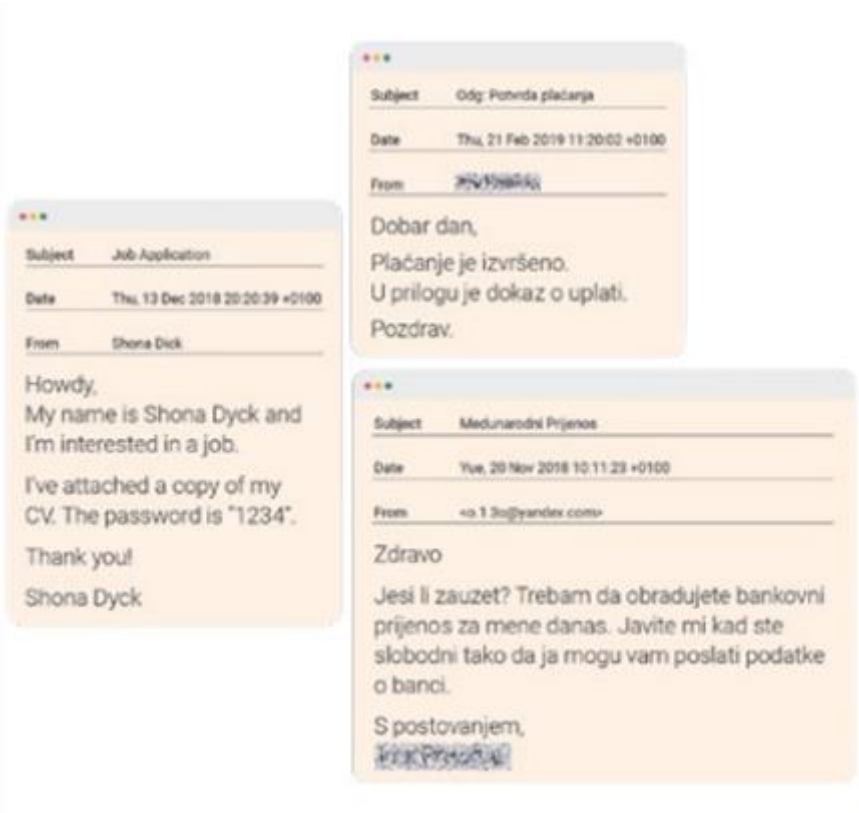
Sve transakcije se danas mogu obaviti na način da se koriste neke određene osobne informacije. Upravo takve informacije su vrlo zanimljive zlonamjernim korisnicima i cilj velikog broja kibernetičkih napada je upravo takve informacije i prikupiti. Zlonamjerni korisnici dobivaju vrlo važne i velike povlastice ako uspiju uzeti takve informacije. Pomoću njih oni mogu upravljati tuđim bankovnim računom, obavljati kupovine i druge transakcije, ugovarati usluge i koristiti iste te informacije za daljnje napade. Ovakvi napadi se najčešće događaju napadom krađe identiteta (engl. *Phishing*) [5].

Postoji nekoliko tipova *phishinga* [5]:

- Krađa identiteta preko telefonskih poziva (engl. *Vishing*),
- Napad preko SMS (engl. *Short Message Service*) poruke (engl. *Smishing*),
- Prevara korisnika (engl. *Catphishing*),
- Ciljani napad (engl. *Spear phishing*),
- Napad na metu visokog profila (engl. *Whaling*).

Krađa identiteta preko telefonskih poziva predstavlja pojam (engl. *Vishing)*. Naziv je došao zapravo od opisa prijetnje, odnosno od toga što se za krađu identiteta koristi glas, pa je naziv *vishing* nastao od riječi *voice* i *phishing* [5].

Napad *phishinga* preko SMS poruke predstavlja pojam (engl. *Smishing*). Ova vrsta napada je jedna od najlakših za izvedbu. Korisnik se cilja putem SMS poruke, odnosno obavijesti u kojoj je sadržana izravna poruka ili neki detalj iz lažne narudžbe. Lažna narudžba sadrži i lažnu opciju za otkazivanje, pa ukoliko korisnik klikne na poveznicu, to ga vodi na stranicu koja je lažno dizajnirana kao stranica za otkazivanje narudžbe, no zapravo mu krade osobne podatke. Slika 1 prikazuje primjer *smishinga* [5].



Slika 1 Primjer *smishinga*
Izvor: [5]

Prevara korisnika (engl. *Catphishing*) je pojam koji se odnosi na vrstu *online* obmane. U ovoj vrsti prevare zlonamjerni korisnik stvara lažni profil na društvenim mrežama. On izmišlja nepostojeću osobu i pretvara se da je ta osoba kako bi namamio stvarnu osobu u neku vrstu veze. To su najčešće romantične veze u kojima zlonamjerni korisnik često uspije izmamiti novac, poklone ili samo pažnju. Međutim, ova vrsta prijetnje sigurnosti može biti i lažni odnos u svrhu dobivanja i otkrivanja nekih informacija koje zlonamjerni korisnik može dobiti od svoje žrtve [5].

Ciljani napad (engl. *Spear phishing*) nije isto što i klasični *phishing*. U klasičnom *phishingu* se jedna *e-mail* poruka šalje na adrese milijuna korisnika. *Spear phishing* je specifičan po tome što se za svakog od korisnika pažljivo osmisli određena poruka. Zbog toga je *spear phishing* i opasniji jer se prije napada pažljivo istražuje korisnik, odnosno sve informacije koje su o njemu dostupne putem podataka, društvenih mreža i njegovih *web* stranica. *Spear phishing* se najviše koristi kod napada na organizacije ili pojedince [5].

Napad na metu visokog profila (engl. *Whaling*) je pojam koji se odnosi na sličnu situaciju kao i *spear phishing*, no on cilja specifičnu skupinu. Najčešća skupina koja je žrtva *whalinga* je neka od upravljačkih poslovnih pozicija, primjerice financijski direktor ili izvršni direktor. *Whalingom* se najčešće napadaju sektori poput zdravstva, bankarstva, tehnologije i sličnog, jer takvi sektori i informacijski sustavi imaju velik broj korisnika i isto tako veliku ovisnost o podacima [5].

Korisnici interneta svakog dana primaju *phishing* poruke. Najčešće vrste ovakvih poruka govore kako je korisnik osvojio veliki dobitak na lutriji, a postoje i drugi klasični oblici napada kao primjerice poruka od nekog afričkog princa koji traži pomoć koju će zatim velikodušno nagraditi. Klasičan primjer je i poruka u kojoj se napadač predstavlja kao djelatnik banke ili suradnik u poslovanju. Drugim riječima, cilj *phishinga* je dobiti povjerenje od napadnute osobe [5].

3.2. Vrste zlonamjernih programa

Zlonamjerni programi (engl. *Malware*) su programi koji mogu prouzročiti štetu te onemogućiti rad informacijskih sustava. Računalni programi koji se pokreću na računalu bez pristanka korisnika i sadrže neku vrstu nepoželjnog rezultata (oštećenje programa i podataka sa sustava, širenje na druga računala, krađa podataka – povjerljivih informacija, lozinki i brojeva kreditnih kartica, omogućavanje neovlaštenog udaljenog pristupa na računalo, prikaz neželjenih ili zlonamjernih reklamnih poruka, učestalo slanje neželjene elektoničke pošte – *spama*, sudjelovanje u napadima na druga računala) [6].

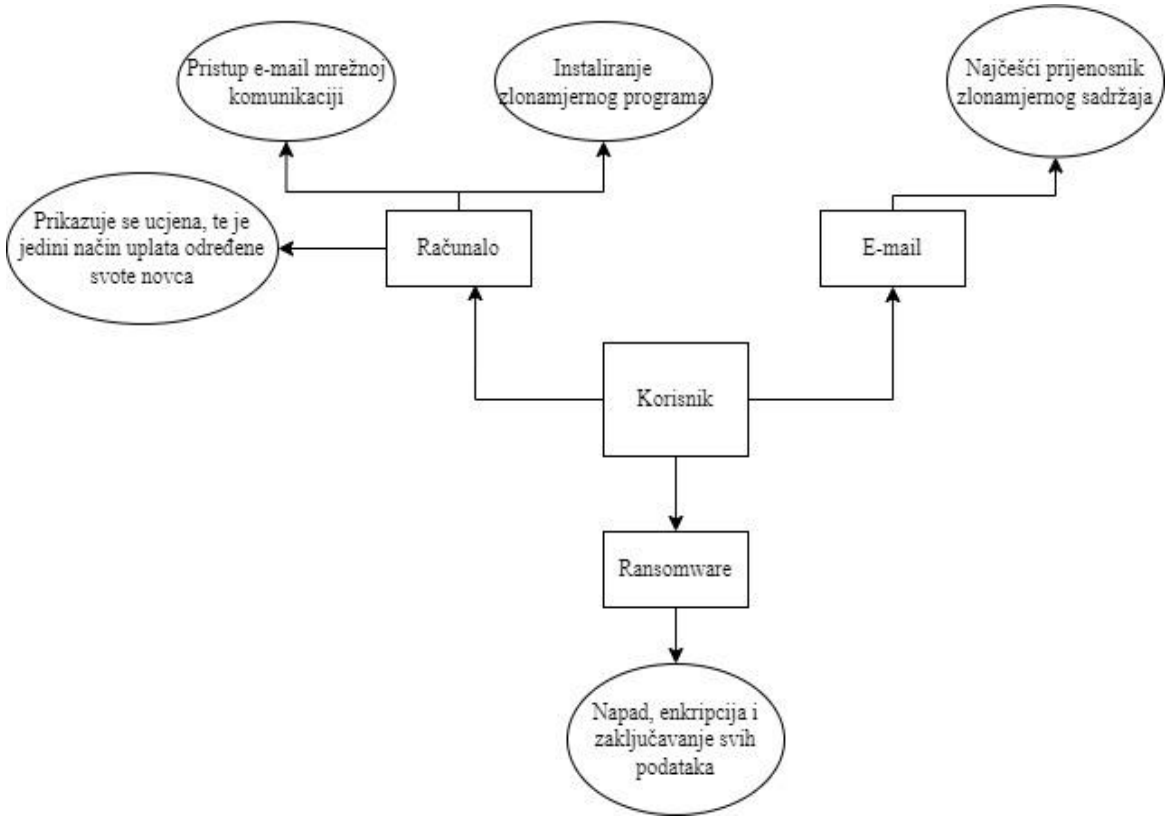
Zlonamjerni programi najčešće funkcioniraju tako da se koriste kao trikovi koji ometaju normalno korištenje uređaja. Svatko može postati žrtvom napada, iako neke osobe možda znaju kako uočiti određene načine na koje napadači pokušavaju naštetiti žrtvama zlonamjernim softverom. Najčešći oblici zlonamjernog sadržaja su [5]:

- Zlonamjerni ucjenjivački softver (engl. *Ransomware*),
- Rudarenje kriptovaluta (engl. *Cryptominer*),
- Zlonamjerni *wiper* sadržaj,
- Trojanski konj.

3.2.1. Zlonamjerni ucjenjivački program

Zlonamjerni ucjenjivački sadržaj (engl. *Ransomware*) prikazan je na Slika 2, a odnosi se na skupinu zlonamjernih programa kojima je cilj korisniku onemogućiti upotrebu računala. Kada se računalo zarazi zlonamjernim sadržajem, on šifrira datoteke i korisniku na ekranu ispisuje poruku koju nije moguće maknuti. Također, od korisnika računala traži otkupninu da bi mogao dalje nastaviti koristiti svoje računalo [5] . Računalni program pristupa datotekama

na računalu, kriptira ih, te ih čini neupotrebljivima bez ključa za dekripciju. Isti sustav može ukrasti osobne podatke te ih poslati bez ikakva znanja korisnika [7].



Slika 2 Način rada *ransomware* programa
Izvor: [7]

3.2.2. Rudarenje kriptovaluta

Rudarenje kriptovaluta (engl. *Cryptominer*) predstavlja zlonamjerni sadržaj koji služi neovlaštenom rudarenju eletroničkih kriptovaluta. Ovo je relativno nova vrsta zlonamjernog sadržaja s obzirom na to da je i kriptovaluta relativno nova vrsta digitalnog novca. Glavni zadatak ovog zlonamjernog sadržaja je preuzeti resurse sa računala žrtve i trošiti iste te resurse na rudarenje bez dozvole vlasnika. S obzirom na to da se ovom vrstom zlonamjernog sadržaja dobiva izravna novčana korist, on je veoma popularan među zlonamjernim napadačima [5].

3.2.3. Napad brisanja ili uklanjanja podataka

Napad brisanja ili uklanjanja podataka (engl. *Wiper*) je vrsta zlonamjernog sadržaja kojoj je glavni zadatak uništiti sustav i podatke. Zbog toga se oni nazivaju i brisači. Ovakve

vrste napada uzrokuju velike štete poslovnim sustavima koji su u najvećoj mjeri financijske prirode. Motiv za ove vrste napada su uglavnom političke poruke ili sabotiranje, odnosno prikrivanje tragova napada [5].

Cyber kriminalci koriste različite tehnike za postavljanje i aktiviranje programa za brisanje i uklanjanje podataka. Neki koriste e-poštu i političke postove, dok drugi koriste korisne poveznice i poruke. Analiza načina rada *wiper* programa otkriva da cilja na tri glavna elementa svoje mete [8]:

- Sve datoteke ili podatke koje sustav ima,
- Sektor za pokretanje operacijskog sustava i mehanizmi sigurnosne kopije,
- Privremene datoteke sustava povezane s podacima.

Zlonamjerni *softver,* ne pobriše cijeli disk jer je to vremenski intenzivan posao već cilja zapravo određene datoteke za oštećenje ili šifriranje. Enkripcija koju stvara *wiper* program je bez ključa, što znači da ne postoji ključ za dešifriranje poništavanja programa [8].

Kada počne brisanje podataka, *wiper* izričito cilja na datoteke za oporavak sustava kako bi ih trajno uništio, te uskraćuje korisnicima bilo kakvu priliku za oporavak svojih podataka. Budući da je gubitak podataka mjerljiv, stručnjaci za sigurnost mogu lako otkriti prisutnost *wiper-a* u slučaju bilo kakvog neobjašnjenog gubitka podataka [8].

3.2.4. Trojanski konj

Trojanski konj predstavlja vrstu zlonamjernog sadržaja kojem je cilj lažno se predstaviti kao koristan program kako bi ga korisnik instalirao na svoje računalo. Trojanski konj ima mogućnost izmjene operacijskog sustava na zaraženom računalu u svrhu prikazivanja oglasa ili skočnih prozora kojima će se ostvariti izravna novčana korist. Postoji i opasniji slučaj trojanskog konja, a to je preuzimanje potpune kontrole nad cijelim zaraženim računalom [5].

Virus trojanskog konja često može ostati na uređaju mjesecima, a da korisnik ne zna da mu je uređaj zaražen. Prepoznavanje znakova prisutnosti trojanca uključuje iznenadnu promjenu postavki računala, gubitak performansi računala ili neku neobičnu aktivnost. Najbolji način za prepoznavanje trojanskog konja je pretraživanje uređaja pomoću skenera ili raznih softvera koji uklanjaju virus [9].

Postoje razne vrste prijetnji trojanskog konja [9]:

- Neovlašteni ulazak u sustav (engl. *Backdoor trojan*) omogućuje napadaču daljinski pristup računalu i preuzimanje kontrole nad njim. Zlonamjernom akteru omogućuje da radi što želi na uređaju kao što je brisanje datoteka, ponovno pokretanje računala i krađa podataka.
- Bankarski trojanac dizajniran je za ciljanje bankovnih računa i financijskih podataka korisnika. Pokušava ukrasti podatke o računu za kreditne i debitne kartice, sustave e-plaćanja i sustave internetskog bankarstva.

- Distribuirani trojanac uskraćivanja usluge izvodi napad kada se mreža preoptereti prometom. Poslat će više zahtjeva s računala ili grupe računala kako bi preplavio ciljnu *web* adresu i uzrokovao uskraćivanje usluge.

3.3. Napad čovjeka u sredini

MITM napad (engl. *Man-in-the-middle*) je vrsta napada u kojem napadač upada u komunikaciju između klijenta i servera tako da ih uvjeri da klijent i server komuniciraju direktno dok napadač u stvari preuzima cijelu komunikaciju bez znanja ostalih sudionika komunikacije. Napad može jedino biti uspješan ako napadač uvjeri obje strane komunikacije da je druga strana upravo ona s kojom ta strana želi pričati. Većina sigurnosnih protokola koristi neku vrstu provjere autentičnosti na rubovima komunikacije kako bi spriječila MITM napade. SSL (engl. *Secure Sockets Layer*) protokol se koristi upravo kako bi obje strane komunikacije mogle provjeriti autentičnost tako da obje strane budu provjerene od pouzdane treće koja ih ovjeri certifikatom, što je prikazano na **Slika 3** [10].

Postoji više vrsta tipova MITM napada [10]:

- RAP *(*engl. *Rouge access point)* → to su uređaji koji se spajaju preko bežične veze te se automatski spajaju na pristupnu točku koja ima najjači signal što znači da ukoliko napadač postavi svoju pristupnu točku, koja ima signal jači od prave pristupne točke, može prevariti ostale uređaje da se spoje na tu pristupnu točku nakon čega sav promet koji ide preko te lažne pristupne točke može biti izmijenjen ili pročitan od strane napadača,

- ARP *(*engl. *Address Resolution Protocol)* → on se koristi unutar lokalne mreže kako bi pristupna točka znala kome poslati promet koji dolazi u lokalnu mrežu. Prilikom slanja podataka preko mreže klijent tada putem ARP može pogledati IP adresu servera kojem želi poslati podatke. Napadač koji želi presresti podatke ovdje se predstavlja kao drugi klijent i odgovara sa svojom MAC (engl. *Media Access Control*) adresom na podatke koji nisu bili za njega. U slučaju da uspije poslati podatke u pravo vrijeme, napadač dobiva pristup svim podatcima koji se razmjenjuju između legitimnog servera i klijenta te tako može doći i do tokena te sesije i dobiti potpuni pristup aplikaciji klijenta.

- mDNS (engl. *Multicast Domain Name System*) *spoofing* → mDNS je sličan kao dns ali se izvodi na pouzdanim mrežama kao na lokalnim mrežama. Na takvim mrežama najčešće se nalaze printeri i televizori. Napadač u tom slučaju odgovara sa lažnim podatcima na taj *multicast* i pri tome napadač postaje pouzdan dok god se nalazi u lokalnoj memoriji od pouzdanih adresa.

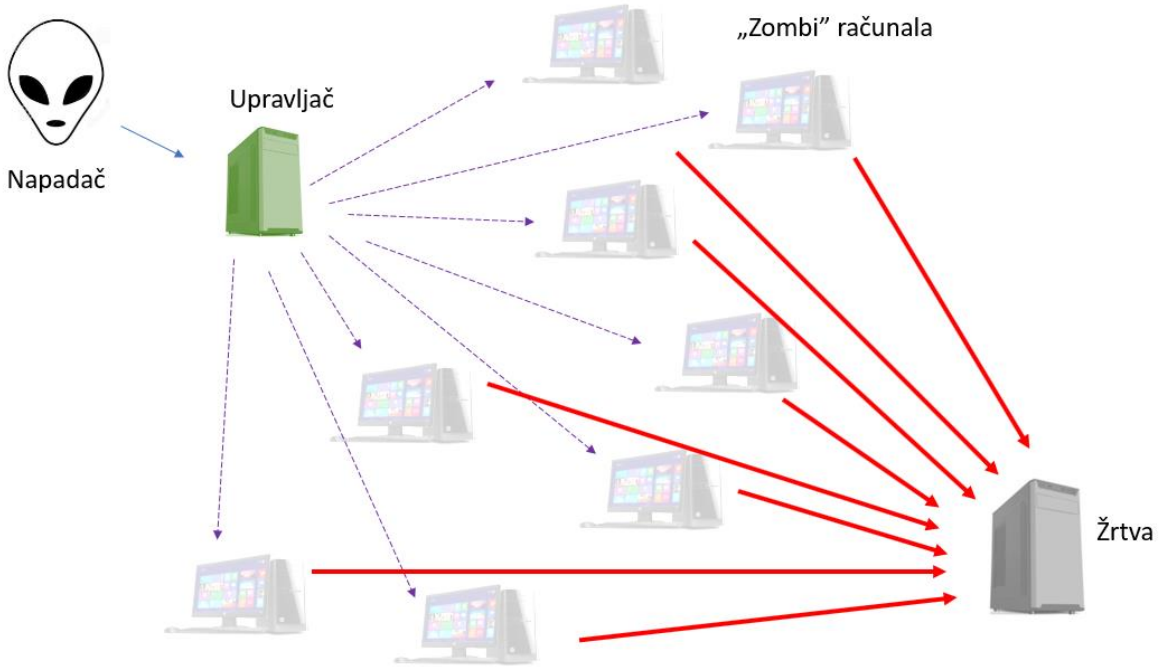
Slika 3 MITM napad
Izvor: [10]

Tehnike MITM napada [11]:

- Njuškanje (engl. *Sniffing*) – napadač koristi alate za hvatanje paketa koji se šalju unutar mreže i pregledava iste na niskom nivou. Koristeći specifične bežične uređaje napadač može vidjeti pakete koji nisu bili namijenjeni njemu.
- Ubacivanje paketa (engl. *Packet injection*) – napadač koristeći uređaj koji može osluškivati pakete koji se šalju unutar mreže osluškuje promet u koji se želi ubaciti. Pokušava odrediti koliko često i kada se paketi šalju te ubacuje svoj maliciozni paket u legitiman tok podataka. Nakon toga dobiva pristup komunikaciji i mogućnost izmjene ili čitanja poruka.
- Preuzimanje sesije (engl. *Session hijacking*) – Napadač dolazi do tokena sesije od legitimnog korisnika i na taj način dobiva pristup web aplikaciji kao da je taj korisnik. Najčešće do tokena sesije dolazi metodom ubacivanja paketa.
- Skidanje enkripcije (engl. *SSL stripping*) – napadač se ubacuje u sigurnu vezu i preuzima pakete koji dolaze sa HTTPS protokolom te ih mijenja u HTTP protokol tako da korisnik šalje svoje podatke sada nezaštićenom vezom u tekstualnom obliku bez ikakve enkripcije koje je lako čitati.

3.4. Napad uskraćivanja usluga

DoS napad ili napad uskraćivanja usluga je napad kojim se korisnicima onemogući njihovo korištenje. Takav napad je teoretski moguće izvesti i s jednog računala, no on ne bi bio naročito učinkovit jer ne bi mogao poslati dovoljno zahtjeva da zaguši na primjer *web* stranicu. No, ako se takav napad izvede s većeg broja računala, onda se on zove DDoS (engl. *Distributed Denial of Service*) napad i puno je učinkovitiji [12].



Slika 4 DDoS napad
Izvor: [12]

DDoS napad, prikazan na **Slika 4**, događa se kada haker pošalje ogromnu količinu prometa na mrežu ili poslužitelju kako bi preopteretio sustav i poremetio njegovu sposobnost za rad. Kada se radi o distribuiranim napadima koji za cilj imaju uskraćivanje mrežnih usluga, nelegitimni promet može dolaziti sa stotina, tisuća ili čak milijun drugih računala. Takvi "distribuirani napadi" mogu trajati danima ili čak i duže [12].

Postoje tri primarne vrste DDoS napada [12]:

1. koriste se ogromne količine prometa prema napadnutim računalima ili sustavima kako bi "zagušili" server zahtjevima te pri tome se najčešće koriste ICMP, UDP, TCP SYN, "*reflection*" metode i drugi mehanizmi napada,
2. DDoS napadi su oni koji koriste mrežne pakete kako bi napali određenu mrežnu infrastrukturu i alate za upravljanje infrastrukturom,
3. Ciljaju organizacijski aplikacijski sloj čiji cilj napada je isti – onemogućiti servis ili određene mrežne resurse, samo im je način onesposobljavanja drugačiji.

Tipični ciljevi za DDoS napade uključuju [13]:

- Internetska mjesta za kupovinu,
- *Online* kasina,
- Svaka tvrtka ili organizacija koja ovisi o pružanju *online* usluga.

Neke od najčešće korištenih vrsta DDoS napada uključuju [13]:

- UDP (engl. *User Data Protocol*) poplava – UDP *flood*, po definiciji, je bilo koji DDoS napad koji preplavljuje metu paketima *User Datagram Protocol* (UDP). Cilj napada je preplaviti nasumične portove na udaljenom hostu. To uzrokuje da

glavno računalo opetovano provjerava ima li aplikacija koja sluša na tom priključku i (kada nije pronađena nijedna aplikacija) odgovara ICMP paketom „*Destination Unreachable*“. Ovaj proces crpi resurse glavnog računala, što u konačnici može dovesti do nedostupnosti.

- ICMP (engl. *Internet Control Message Protocol*) poplava – Slično u načelu UDP *flood* napadu, ICMP *flood* preplavljuje ciljni resurs s ICMP *Echo Request* (ping) paketima, općenito šaljući pakete što je brže moguće bez čekanja na odgovore. Ova vrsta napada može potrošiti i odlaznu i dolaznu propusnost, budući da će poslužitelji žrtve često pokušati odgovoriti s ICMP *Echo Reply* paketima, što će rezultirati značajnim ukupnim usporavanjem sustava.
- SYN (engl. *synchronize*) Poplava – SYN *flood* DDoS napad iskorištava poznatu slabost u nizu TCP (engl. *Transfer Control Protocol*) veze „trosmjerno rukovanje“, pri čemu se na SYN zahtjev za pokretanje TCP veze s *hostom* mora odgovoriti SYN-ACK (engl. *Synchronize-acknowledge*) odgovorom s tog *hosta*, i zatim potvrđenim ACK odgovorom od podnositelja zahtjeva. U scenariju SYN poplave, podnositelj zahtjeva šalje više SYN zahtjeva, ali ili ne odgovara na SYN-ACK odgovor glavnog računala ili šalje SYN zahtjeve s lažirane IP adrese. U svakom slučaju, glavni sustav nastavlja čekati potvrdu za svaki od zahtjeva, obvezujući resurse dok se ne uspostave nove veze, što u konačnici rezultira uskraćivanjem usluge.
- Ping smrti – Napad ping smrti POD (engl. *Ping of Death*) uključuje napadača koji šalje višestruke neispravne ili zlonamjerne pingove računalu. Maksimalna duljina IP paketa (uključujući zaglavlje) je 65.535 bajtova. Međutim, sloj podatkovne veze obično postavlja ograničenja za maksimalnu veličinu okvira – na primjer 1500 bajtova preko *Ethernet* mreže. U ovom slučaju, veliki IP paket je podijeljen na više IP paketa (poznatih kao fragmenti), a *host* primatelj ponovno sastavlja IP fragmente u cijeli paket. U scenariju *Ping of Death*, nakon zlonamjerne manipulacije sadržajem fragmenta, primatelj završava s IP paketom koji je veći od 65.535 bajtova kada se ponovno sastavi. To može prepuniti memorijske međuspremnike dodijeljene za paket, uzrokujući uskraćivanje usluge za legitimne pakete.

3.5. Napredna trajna prijetnja

Napredna trajna prijetnja APT (engl. *Advanced Persistent Threat*) je sofisticirani, kontinuirani kibernetički napad u kojem uljez uspostavlja neotkrivenu prisutnost u mreži kako bi ukrao osjetljive podatke tijekom duljeg vremenskog razdoblja. APT napad pažljivo je planiran i osmišljen kako bi se infiltrirao u određenu organizaciju, izbjegao postojeće sigurnosne mjere i prošao ispod radara [14].

Izvršenje APT napada zahtijeva viši stupanj prilagodbe i sofisticiranosti od tradicionalnog napada. Protivnici su obično dobro financirani, iskusni timovi kibernetičkih kriminalaca koji ciljaju organizacije visoke vrijednosti, te potroše značajno vrijeme i resurse istražujući i identificirajući ranjivosti unutar organizacije. Ciljevi APT-a spadaju u četiri opće kategorije [14]:

- *Cyber* špijunaža, uključujući krađu intelektualnog vlasništva ili državnih tajni,
- e-kriminal radi financijske dobiti,
- haktivizam,
- uništenje.

Postoje tri faze napada kod APT-a [14]:

- Infiltracija – u prvoj fazi, napredne trajne prijetnje često dobivaju pristup putem tehnike društvenog inženjeringa. Jedan od pokazatelja APT-a je *phishing* e-pošta koja selektivno cilja pojedince na visokoj razini poput viših rukovoditelja ili tehnoloških vođa, često koristeći podatke dobivene od drugih članova tima koji su već bili ugroženi. Napadi e-poštom koji ciljaju određene pojedince nazivaju se "krađa identiteta". Može se činiti da e-pošta dolazi od članova tima i uključuje referencu na projekt koji je u tijeku. Ako nekoliko rukovoditelja prijavi da ih je prevario *spear-phishing* napad, počnite tražiti druge znakove APT-a.
- Eskalacija i bočno kretanje – nakon što se dobije početni pristup, napadači ubacuju zlonamjerni softver u mrežu organizacije kako bi prešli na drugu fazu, proširenje. Pomiču se bočno kako bi mapirali mrežu i prikupili vjerodajnice kao što su imena računa i lozinke kako bi pristupili kritičnim poslovnim informacijama. Oni također mogu uspostaviti "stražnja vrata" - shemu koja im omogućuje da se kasnije ušuljaju u mrežu kako bi izveli tajne operacije. Često se uspostavljaju dodatne ulazne točke kako bi se osiguralo da se napad može nastaviti ako se kompromitirana točka otkrije i zatvori.
- Eksfiltracija – kako bi se pripremili za treću fazu, kibernetički kriminalci obično čuvaju ukradene informacije na sigurnom mjestu unutar mreže dok se ne prikupi dovoljno podataka. Zatim ga ekstrahiraju ili "ekfiltriraju" bez otkrivanja. Mogu koristiti taktike poput napada uskraćivanjem usluga (DoS) kako bi odvratili pozornost sigurnosnog tima i vezali mrežno osoblje dok se podaci eksfiltriraju. Mreža može ostati ugrožena, čekajući da se lopovi vrate bilo kada.

3.6. Unutarnja prijetnja

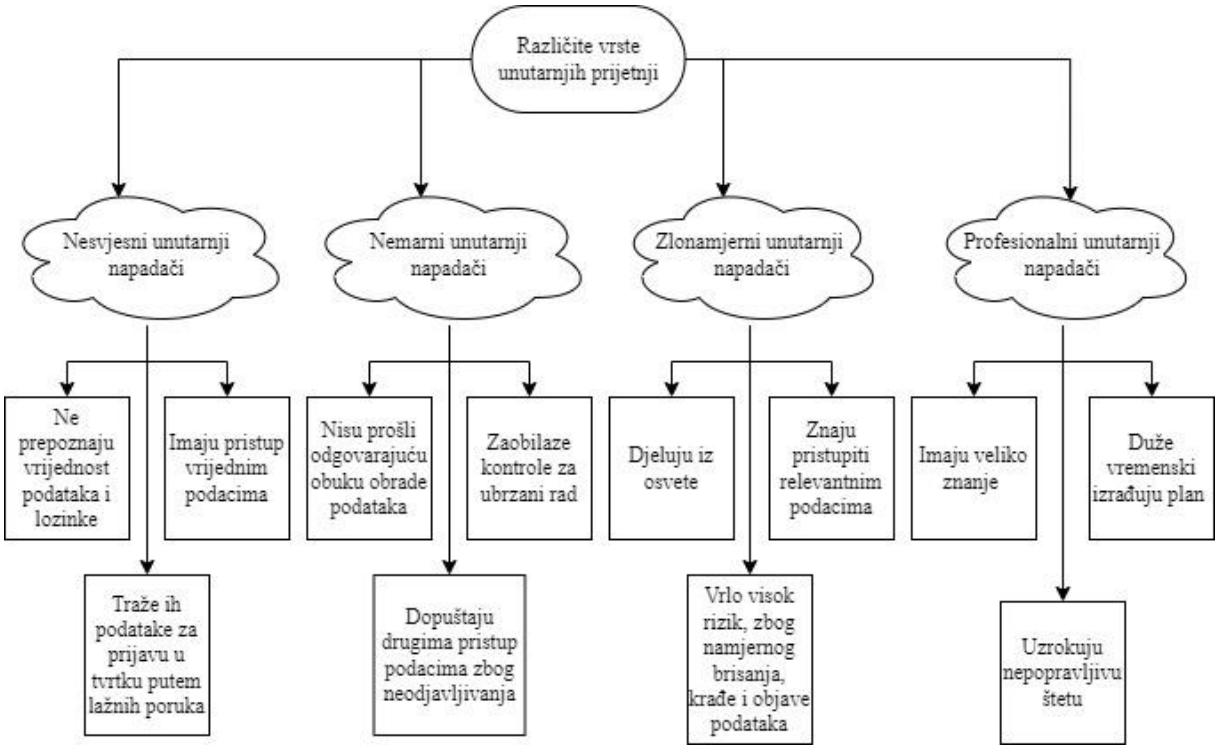
Mreža je posebno ranjiva na zlonamjerne interne korisnike, koji već imaju privilegirani pristup organizacijskim sustavima. Prijetnje internih korisnika može biti teško otkriti i zaštiti se od njih, jer takvi korisnici ne moraju probijati u mrežu da bi joj naštetili [15].

Interni korisnik je svaka osoba koja ima ili je imala ovlašteni pristup ili znanje o resursima organizacije, uključujući osoblje, objekte, informacije, opremu, mreže i sustave. Primjeri internih korisnika mogu uključivati [16]:

- Osobe kojima organizacije vjeruju, uključujući zaposlenike, članove organizacije i one kojima je organizacija dala osjetljive informacije i pristup,
- Osoba koja je dobila značku ili pristupni uređaj koji ju identificira kao nekoga s redovitim ili stalnim pristupom (npr. zaposlenik, serviser, dobavljač),
- Osoba kojoj je organizacija osigurala računala ili pristup mreži,

- Osoba koja razvija proizvode i usluge organizacije, a to je skupina koja uključuje one koji znaju tajne proizvoda koji daju vrijednost organizaciji,
- Osoba koja je upoznata s osnovama organizacije, uključujući cijene, troškove te organizacijske snage i slabosti.

Unutarnje prijetnje se dijele na razne vrste kao što prikazuje Slika 5.



Slika 5 Prikaz unutarnjih prijetnji
Izvor: [17]

3.7. Napad ubrizgavanja koda SQL-a

Kod napada ubrizgavanja koda SQLi (engl. *Structured Query Language Injection*) mnoga *web* mjesta prihvaćaju korisničke unose i ne provjeravaju te unose. Napadači tada mogu ispuniti obrazac ili uputiti API (engl. *Application Programming Interface*) poziv, prosljeđujući zlonamjerni kod umjesto očekivanih vrijednosti podataka. Kod se izvršava na poslužitelju i omogućuje napadačima da ga kompromitiraju [15].

SQL *injection* sigurnosna je ranjivost na *webu* koja napadaču omogućuje miješanje u upite koje aplikacija postavlja svojoj bazi podataka. Općenito omogućuje napadaču pregled podataka koje inače ne može dohvatiti. To može uključivati podatke koji pripadaju drugim korisnicima ili bilo koje druge podatke kojima sama aplikacija može pristupiti. U mnogim slučajevima, napadač može modificirati ili izbrisati te podatke, uzrokujući stalne promjene sadržaja ili ponašanja aplikacije. U nekim situacijama napadač može izbjeći napad SQLi kako

bi ugrozio temeljnog poslužitelja ili drugu pozadinsku infrastrukturu ili izvršio DDoS napad [18].

Uspješan napad SQLi može rezultirati neovlaštenim pristupom osjetljivim podacima, kao što su lozinke, podaci o kreditnoj kartici ili osobni podaci o korisniku. Mnoga kršenja podataka visokog profila posljednjih godina bila su rezultat napada SQLi, što je dovelo do oštećenja ugleda i regulatornih kazni. U nekim slučajevima, napadač može dobiti stalan *backdoor* u sustave organizacije, što dovodi do dugoročnog ugrožavanja koje može proći nezapaženo dulje vrijeme [18].

Postoji širok izbor ranjivosti, napada i tehnika SQLi ubacivanja koji se pojavljuju u različitim situacijama, neki uobičajeni primjeri SQLi ubacivanja uključuju [18]:

- Dohvaćanje skrivenih podataka, gdje možete izmijeniti SQL upit kako biste pružili dodatne rezultate,
- Podmetanje logike aplikacije, gdje možete promijeniti upit da ometa logiku aplikacije,
- UNION napadi, gdje možete dohvatiti podatke iz različitih tablica baze podataka,
- Ispitivanje baze podataka, gdje možete izdvojiti informacije o verziji i strukturi baze podataka,
- Slijepo SQL ubacivanje, gdje se rezultati upita koji kontrolirate ne vraćaju u odgovorima aplikacije.

4. METODE ZAŠTITE MREŽNE KOMUNIKACIJE

Razvojem kriptografije i tehnologije otkriveni su kvalitetni načini kriptiranja i zaštite dokumenata što je u današnje doba iznimno važno. Kriptiranjem se sprječava ulazak neovlaštene osobe u razne osjetljive, povjerljive i tajne dokumente. Ukoliko se dokument dekriptira tajnim ključem, ovlaštena osoba loših namjera može spremiti, kopirati, ispisati ili proslijediti dokument. Ograničavanje pristupa dokumentu nekolicini pojedinaca jedan je od pristupa zaštite dokumenta. U današnje doba zaštita osjetljivih informacija i dokumenata ne može ovisiti o samo jednoj vrsti tehnologije. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, upotrebljavaju se za zaštitu dokumenata. Efikasna zaštita dokumenata ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite. [19]

Najčešća rješenja za zaštitu mrežne komunikacije su [19]:

- antivirusna zaštita,
- vatrozid,
- sustavi za otkrivanje napada IDS (engl. *Intrusion detection systems*),
- sustavi za sprječavanje napada IPS (engl. *Intrusion prevention systems*),
- kriptiranje,
- virtualna privatna mreža VPN (engl. *Virtual Private Network*),
- sigurnosni protokoli.

4.1. Antivirusna zaštita

Antivirusna zaštita se odnosi na antivirusne programe koji imaju za cilj identificirati, neutralizirati i ukloniti zlonamjerne sadržaje i programe. Moderni antivirusni programi sada imaju sposobnost boriti se protiv većine zlonamjernih sadržaja, no njihovo ime je ostalo zadržano iz povijesti interneta, kada su jedini zlonamjerni sadržaji bili virusi [20].

Antivirusni programi su u današnje vrijeme široko zastupljeni i gotovo da ne postoji osoba koja nikada nije instalirala antivirusnu zaštitu. Zaštita računala u obliku antivirusne zaštite je široko rasprostranjena upravo zato što su korisnici svjesni da postoji veliki broj zlonamjernih korisnika koji bi im mogli ukrasti podatke [21].

Antivirusni program je napravljen na način da detektira, zaustavi i ukloni virusne, odnosno zlonamjerne sadržaje i kodove sa zaraženog računala. Ukoliko se dogodi da je neka datoteka zaražena, antivirusni program na vrijeme prepoznaje dio koda i uspijeva zaustaviti izvršavanje tog koda na računalu, te datoteku sprema u karantenu. Antivirusni programi danas imaju zaštitu u realnom vremenu. To znači da oni mogu pratiti dolazak i pojavu svake nove datoteke koja se pojavljuje na računalu. Na taj način oni skeniraju i po potrebi djeluju i prije nego što korisnik računala otvori zaraženu datoteku [20].

Nakon što detektira virusnu sekvencu u nekoj datoteci, antivirusni program će [20]:

- pokušati popraviti datoteku brišući iz nje sam virus,
- staviti datoteku u karantenu tako da toj datoteci više ne može pristupiti nijedan program, pa se samim tim ni virus više ne može širiti,
- izbrisati inficiranu datoteku.

Neki od najpoznatijih antivirusnih programa su [20]:

- *AdAware* Antivirus,
- *Amiti* Antivirus,
- *AVG* Antivirus,
- *Avira* Antivirus.

Slika 6 AdAware antivirusni program
Izvor: [20]

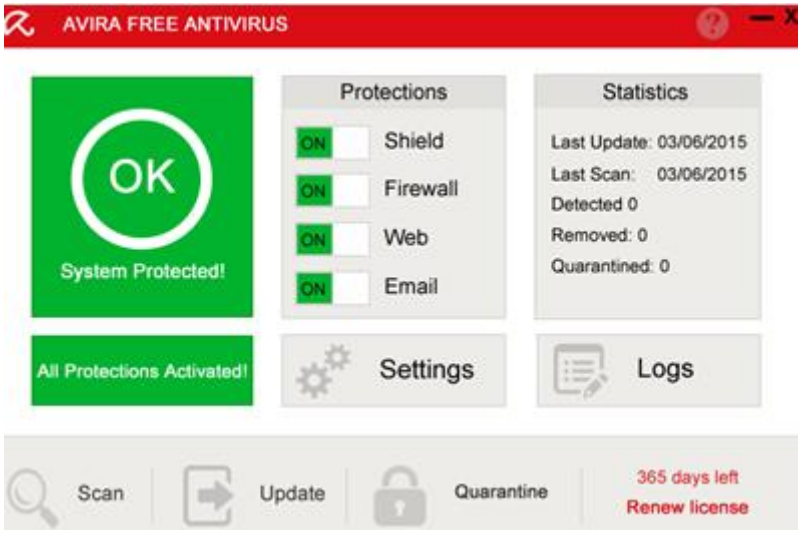
AdAware antivirusni program je vrlo popularan program jer je uvijek aktivan, a korisnici ga vole i jer je besplatan, prikazan je **Slika 6**. To su dovoljne prednosti za korisnike koji ga odluče koristiti, međutim, nedostatak mu je to što ne postoji skeniranje za elektroničku poštu [20].

Slika 7 Amiti antivirusni program
Izvor: [20]

Amiti antivirusni program je također vrlo popularan program među korisnicima, a sučelje programa je prikazano **Slika 7**. Osim što je besplatan, sadrži i heurističko skeniranje i ima podršku za četiri različite vrste skeniranja računala. Također, opcije u njemu su organizirane i jednostavan je za korištenje, pa predstavlja idealan program za korisnike koji žele imati dobar antivirusni program [20].

Slika 8 AVG antivirusni program
Izvor: [20]

AVG antivirusni program je idealan za korisnike jer osim antivirusnog alata ima i mnoge druge značajke kao što su *antispyware*, skener e-pošte, mogućnost planiranog skeniranja, automatski način nadogradnje i slično. Sustav je prikazan na **Slika 8** [20].

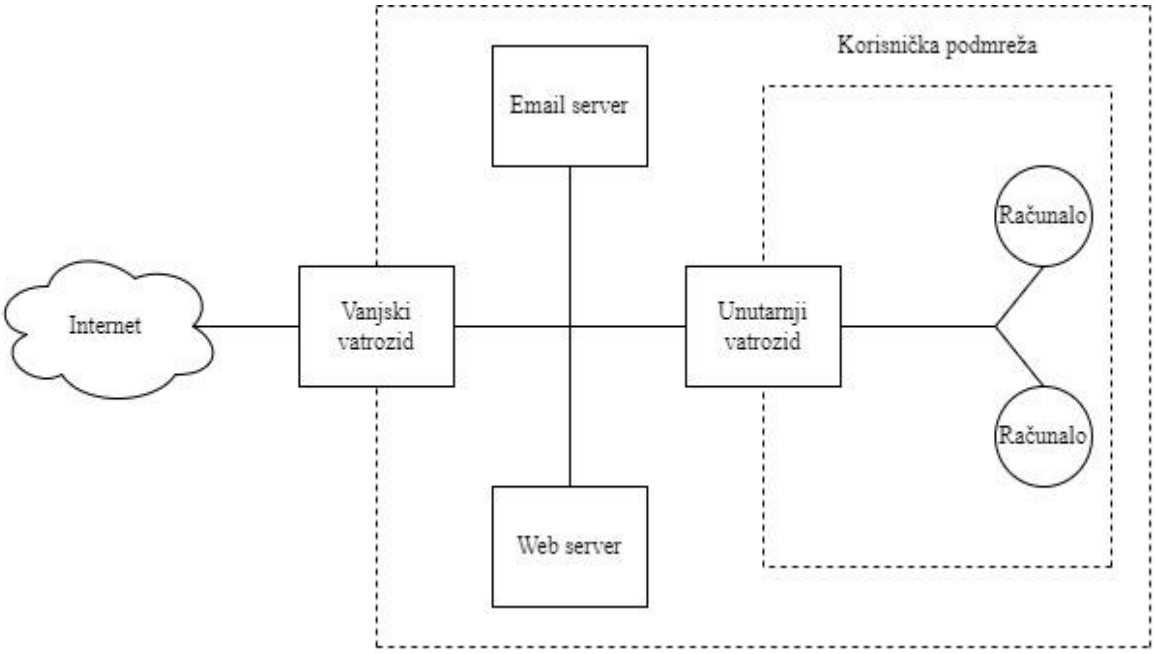


Slika 9 Avira antivirusni program
Izvor: [20]

Avira antivirusni program pruža korisnicima zaštitu od trojanskih konja, raznoraznih crva, *spywarea*, *adwarea* itd. Popularan je među korisnicima jer je besplatan program koji nudi mnoge opcije i mogućnosti, a prikazan je na **Slika 9** [20].

4.2. Vatrozid

Vatrozid kao opći pojam (eng. *Firewall*) odnosi se na uređaj koji nadzire i na osnovu zadanih pravila propušta ili odbacuje mrežni promet. Vatrozid predstavlja softverski program ili *hardwerski* uređaj. On služi za filtriranje i provjeru informacija koje putuju internetskom vezom. Zapravo su prva crta obrane računala jer mogu zaustaviti napadače i zlonamjerne programe prije nego što oni uspiju napraviti štetu za korisnika ili njegovo računalo. Prikaz rada Vatrozida vidljiv je na Slika 10 [22].



Slika 10 Prikaz rada Vatrozida
Izvor: [23]

Vatrozidi se dijele na [22]:

- poslovne – podrazumijevaju sklopovsko ili programsko rješenje (kombinaciju) koje od potencijalno štetnog prometa štiti cijelu poslovnu mrežu na način da se sav promet mreže preusmjerava kroz poseban uređaj namijenjen samo toj svrsi i
- osobne – u pravilu programsko rješenje koje štiti korisničko računalo na kojem se nalazi.

Vatrozid inače filtrira promet koji se nalazi na više slojeva, ovisno o namjeni i potrebi. Najčešće filtriranje se odvija na mrežnom i transportnom sloju te je moguće definirati pravila i za niže slojeve, kao što je sloj podatkovne veze i za više slojeve u koje spada aplikacijski sloj. Kompleksnost samog filtriranja ovisi o sloju filtriranja, pa tako filtriranje na višim slojevima omogućuje pametnije filtriranje (viši slojevi imaju više podataka kod kojih se koristi selektivno filtriranje), međutim proces filtriranja na nižim slojevima se odvija brže [22].

Glavne mogućnosti vatrozida su [22]:

- prijaviti neovlaštene pokušaje za spajanje na računalo korisnika,
- odrediti lokalne mrežne servise kojima je dopuštena interakcija putem mreže,
- spriječiti detektiranje otvorenih mrežnih priključaka koji su nastali od strane udaljenih potencijalnih napadača,
- nadzirati lokalne mrežne servise,
- zaustaviti neovlašten odlazni promet lokalnih mrežnih servisa,
- pružiti informacije o aplikaciji koja traži mrežnu komunikaciju.

Kada govorimo o tipovima vatrozida oni se najčešće kategoriziraju u tri kategorije. To su [19]:

- vatrozid za filtriranje paketa (engl. *Stateless Firewall*),
- vatrozid prema stanju (engl. *Stateful Firewall*),
- vatrozid aplikacijskog sloja (engl. *Application Firewall*).

4.2.1. Vatrozid za filtriranje paketa

Ovaj se vatrozid nalazi na slojevima mrežnog i transportnog modela međusobnog povezivanja otvorenih sustava OSI. Kao što naziv sugerira, vatrozid s praćenjem stanja uvijek prati stanje mrežnih veza. Nakon što vatrozid s praćenjem stanja odobri određenu vrstu prometa i dodaje se u tablicu stanja. Unosi tablice stanja kreirani su za TCP (engl. *Transmission Control Protocol*) tokove ili UDP (engl. *User Datagram Protocol*) datagrame kojima je dopuštena komunikacija kroz vatrozid u skladu s konfiguriranom sigurnosnom politikom. Ako se promet ne vidi određeno vrijeme (ovisno o implementaciji), veza se uklanja iz tablice stanja [24].

4.2.2. Vatrozid prema stanju

Također je poznat kao popis kontrole pristupa ACL (engl. *Access Control List*), ne pohranjuje podatke o stanju veze. ACL-ovi bez stanja primjenjivi su na mrežni i fizički sloj, a ponekad i na transportni sloj kako bi se saznali izvorni i odredišni brojevi *portova*. Kada pošiljatelj pošalje paket i bude filtriran kroz vatrozid, uređaj provjerava podudara li se s bilo kojim od ACL pravila koja su konfigurirana u vatrozidu i zatim ispušta ili odbija paket u skladu s tim [24].

4.2.3. Vatrozid aplikacijskog sloja

Aplikacijski vatrozid prvenstveno se koristi kao poboljšanje standardnog vatrozidnog programa pružanjem usluga vatrozida do aplikacijskog sloja. Neke od usluga koje obavlja aplikacijski vatrozid uključuju kontrolu izvršavanja aplikacija, rukovanje podacima, blokiranje izvođenja zlonamjernog koda i više [25]. Postoje dvije vrste vatrozid aplikacija [25]:

- Aplikacijski vatrozidi temeljeni na mreži: skeniraju i nadziru promet temeljen na mreži namijenjen aplikacijskom sloju ili bilo kojoj specifičnoj aplikaciji.
- Aplikacijski vatrozidi temeljeni na glavnom računalu: Nadziru sav dolazni i odlazni promet koji pokreće aplikacija ili usluga na lokalnom računalu, sustavu ili glavnom računalu.

Vatrozid najčešće predstavlja temeljnu i prvu metodu za povećavanje sigurnosti računalnog sustava. No, iako ovaj sustav izgleda kao sasvim dovoljan sustav za zaštitu, važno je napomenuti da svakako ne bi trebao biti jedini sustav zaštite [22].

4.3. Sustavi za otkrivanje napada

Otkrivanje napada odnosi se na detektiranje bilo koje vrste akcija koje imaju za cilj narušiti ili ugroziti računalni sustav i njegovu sigurnost. Proces kojim se nadzire i analizira akcija u mreži i kojim se mogu detektirati opasne akcije, može biti izveden ručno ili automatski. Prije velikog napretka tehnologije koristilo se ručno otkrivanje napada koje je podrazumijevalo da osoba prati podatke koji prolaze kroz mrežu. Ovakav način rada mogao je biti prihvatljiv do određenog razdoblja kad je kroz mrežu počelo prolaziti puno više podataka nego što ih čovjek može pročitati i analizirati. Početkom 20. stoljeća počeli su se razvijati automatski sustavi za otkrivanje napada [26].

Sustavi za otkrivanje napada predstavljaju programske sustave ili sklopovske uređaje koji se temelje na mogućnosti da otkriju zlonamjeran sadržaj, odnosno napad u realnom vremenu. Sustav funkcioniranja im radi tako da svaki paket koji prolazi kroz mrežu koju ovakva vrsta sustava nadzire, postane analizirani paket u kojem se traže neki određeni znakovi koji bi mogli predstavljati indikator za neželjeno ponašanje, tj. napad u mrežnoj infrastrukturi [26].

Traženje uzoraka i znakova napada se radi na način da se pretražuje baza podataka koja je unaprijed definirana i koja u sebi sadrži detalje o napadima koji su već poznati. Pomoću takve baze podataka može se identificirati napad koji je već započeo, odnosno napad koji je u tijeku [26].

Sustavi za otkrivanje napada se općenito mogu podijeliti na tri vrste: mrežno zasnovane sustave za otkrivanje napada (engl. NIDS - *Network Intrusion Detection System*), računalno zasnovane (engl. HIDS - *Host Intrusion Detection System*) i mješovite sustave za otkrivanje napada koji su kombinacija mrežnih i računalnih sustava [27].

4.3.1. Mrežno zasnovani sustav za otkrivanje napada

Mrežno zasnovani sustav za otkrivanje napada NIDS (engl. *Network Intrusion Detection System*) je mrežni IDS sustav koji ima sposobnost analiziranja mrežnog prometa radi usporedbe baze u datoteci u kojoj je zabilježen potpis napada. NIDS se koristi tehnikom „njuškanja paketa“ odnosno prima sve pakete koji su poslani putem mreže, a ne samo adresirane za korisnikovo računalo, tako da može pohvatati i one mrežne pakete koji nisu namijenjeni korisnikovu računalu već nekim drugim računalima na mreži. Ovakva vrsta sustava ima zadaću javljati korisniku da je došlo do zlonamjerne radnje, te ga upozoriti i zabilježiti taj događaj putem analize napada [26].

4.3.2. Računalno zasnovani sustav za otkrivanje napada

Zadatak računalno zasnovanog sustava za otkrivanje napada (HIDS) je analiza bilježaka sustava i programa koji se nalaze u datotekama, kako bi mogao otkriti nesvakodnevne radnje koje upućuju na potencijalni upad u sustav. Primjer neobičnog ponašanja na mreži je višestruki

pokušaj nepravilne prijave u neki sustav. HIDS sustav isto tako provjerava i datoteke koje se nalaze u sustavu, te prati je li došlo do nekakvih promjena u njima i jesu li stvorene ili možda izbrisane [26].

4.4. Sustavi za sprječavanje napada

Tretiranje malicioznog mrežnog prometa, uskraćivanjem komunikacije izvora napada već na točki izvan štićenog informacijskog sustava, predstavlja efektivnu i popularnu metodu borbe protiv malicioznog koda jer štedi procesno vrijeme informacijskog sustava. U prvom redu je cilj rasterećenje procesnog vremena i resursa sigurnosnih komponenata samog sustava [22].

Sustavi za sprječavanje napada predstavljaju tehnološki naprednije sustave koji služe za otkrivanje napada. Od njih se razliku po tome što osim otkrivanja, služe i za to da otklone napad, odnosno da ga spriječe. Blokiranje napada se može provesti na dva načina [26]:

- prvi način je da se promijeni sadržaj paketa koji je uzrokovao da se napad otkrije,
- drugi način je ubacivanje reset paketa u TCP vezu pomoću koje se provodi napad. Na taj način se veza nasilno prekida i tako zaustavi napad koji je započeo.

Postoje tri metode koje IPS (engl. *Intrusion Prevention Systems*) koristi za detekciju upada u sustav [26]:

- Otkrivanje upada temeljeno na potpisu – ova metoda se koristi potpisima koji su potvrda da se napad dogodio i uspoređuje ih sa mrežnim prometom. Kada se dogodi poklapanje sustav pokreće određene aktivnosti,
- Otkrivanje upada temeljeno na anomalijama – metoda radi na način da stvara osnovu koju sustav uspoređuje sa mrežnim prometom. Ova metoda putem statističke analize provjerava promet, a ako se aktivnosti u mrežnom prometu razlikuju od osnove, sustav pokreće određena rješenja,
- Otkrivanje upada inteligentnom analizom protokola – ova metoda otkriva upade putem identifikacije odstupanja od protokola. Usporedbom nepravilnih događaja sa već definiranim profilima općeprihvaćenih definicija.

4.5. Kriptografske metode u svrhu povećanja sigurnosti mrežne komunikacije

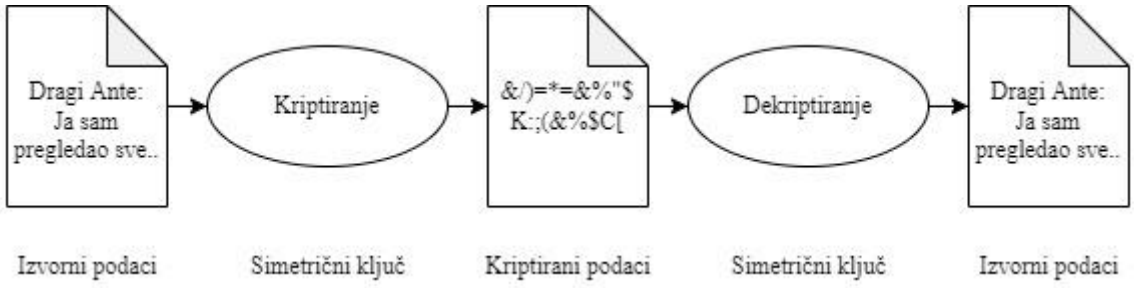
Enkripcija predstavlja važnu metodu zaštite dokumenata koji su pohranjeni na tvrdom disku računala, a posebno onih prijenosnih. U slučaju gubitka prijenosnog računala, ovom metodom je moguće lako izbjeći da se povjerljive informacije otkriju i da ih iskoriste zlonamjerni korisnici u svrhu napada. Kod većine modernih operacijskih sustava omogućeno je i kriptiranje podataka koji su pohranjeni na disku [28], [29].

Postupak kriptiranja uključuje preoblikovanje otvorenog ili jasnog teksta u tekst nerazumljiv osobama kojima nije namijenjen. Osobe kojima je dokument namijenjen i koje ga

smiju pročitati moraju posjedovati poseban ključ za pretvaranje dokumenta u jasan tekst, odnosno dekriptiranje. Postoje simetrični i asimetrični kriptosustavi te kvantna komunikacija odnosno šifriranje audio i video komunikacije [30].

4.5.1. Simetrično kriptiranje

Simetrična enkripcija je vrsta šifriranja gdje se samo jedan ključ (tajni ključ) koristi za šifriranje i dešifriranje elektroničkih podataka, a način rada prikazan je Slika 11. Entiteti koji komuniciraju putem simetrične enkripcije moraju razmjeniti ključ kako bi se mogao koristiti u procesu dešifriranja [31].



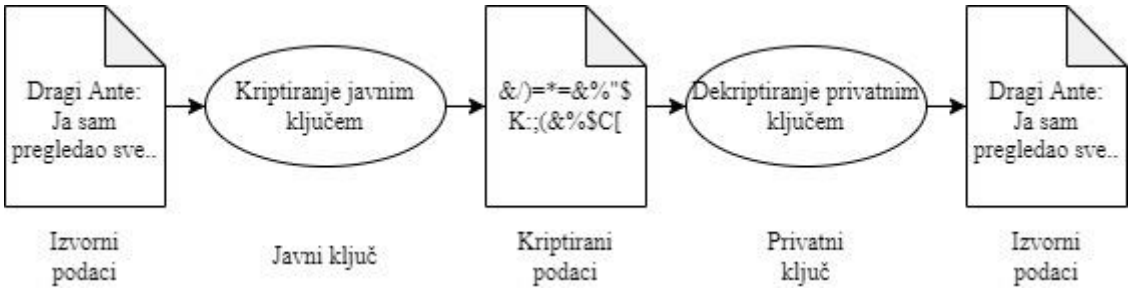
Slika 11 Prikaz rada simetričnog kriptiranja
Izvor: [32]

Korištenjem algoritama simetrične enkripcije podaci se šifriraju tako da ih ne može razumjeti nitko tko ne posjeduje tajni ključ za dešifriranje. Nakon što namjeravani primatelj koji posjeduje ključ dobije poruku, algoritam poništava svoju radnju tako da se poruka vraća u izvorni čitljiv oblik. Tajni ključ koji koriste pošiljatelj i primatelj može biti određena lozinka ili kod te može biti nasumični niz slova ili brojeva koje je generirao sigurni generator slučajnih brojeva (engl. *Random number generator*). Za enkripciju bankarske razine, simetrični ključevi moraju biti kreirani pomoću generatora slučajnih brojeva, koji je certificiran prema industrijskim standardima [31].

Zbog boljih performansi i veće brzine simetrične enkripcije (u usporedbi s asimetričnom), ta kriptografija se koristi za kriptiranje velikih količina podataka, npr. za enkripciju baze podataka [31].

4.5.2. Asimetrično kriptiranje

Asimetrična enkripcija vrsta je enkripcije koja koristi dva odvojena, ali matematički povezana ključa za šifriranje i dešifriranje podataka. Način rada prikazan je Slika 12. Javni ključ kriptira podatke dok ih odgovarajući privatni ključ dekriptrira. Zbog toga je također poznat kao enkripcija s javnim ključem [33].



Slika 12 Način rada asimetričnog kriptiranja
Izvor: [33]

Javni ključ je otvoren svima. Svatko mu može pristupiti i njime šifrirati podatke. Kada su podaci jednom šifrirani, ti se podaci mogu otključati samo korištenjem odgovarajućeg privatnog ključa. Privatni ključ mora biti tajan kako ne bi bio ugrožen. Istom tom privatnom ključu pristup imaju samo ovlaštene osobe, poslužitelj, stroj ili instrument [33].

Zbog odvojena dva ključa enkripcija s javnim ključem smatra se kritičnim elementom u temeljima internetske sigurnosti. Infrastruktura javnih ključeva, okvir politika, procesa i tehnologija koje omogućuju sigurnu komunikaciju trećih strana putem interneta se oslanja na asimetričnu i simetričnu enkripciju [33].

Metode asimetrične enkripcije se koriste za [33]:

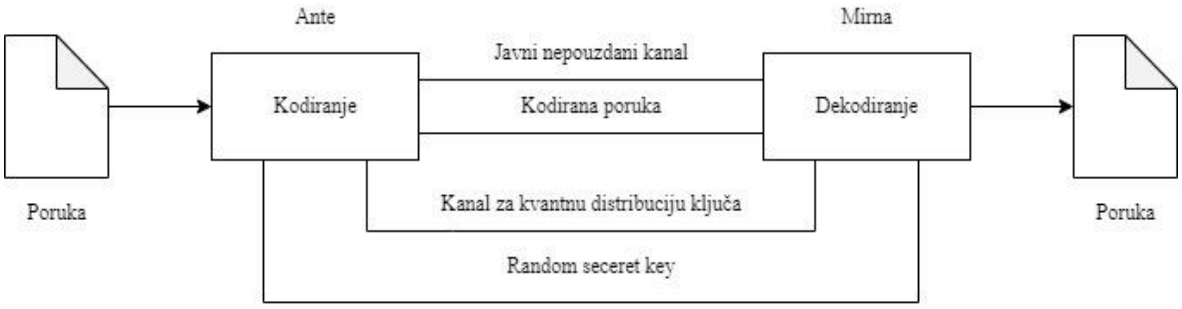
- autentificiranje stranki,
- provjeru integriteta podataka,
- razmjenu simetričnih ključeva.

4.5.3. Kvantna komunikacija

Kvantna kriptografija koristi načela kvantne mehanike za šifriranje podataka i njihov prijenos na način koji se ne može hakirati. Definicija je možda jednostavna, međutim složenost je u principima kvantne mehanike. Kvantna enkripcija ima principe na kojima ona općenito funkcionira [34]:

- čestice koje čine svemir same po sebi su neizvjesne i mogu istovremeno postojati na više od jednog mjesta ili u više od jednog stanja postojanja,
- fotoni se generiraju nasumično u jednom od dva kvantna stanja,
- ne može se izmjeriti kvantno svojstvo bez da se promijeni ili poremeti,
- mogu se klonirati neka kvantna svojstva čestice, ali ne i cijela čestica.

Kvantna distribucija ključeva (engl. *Quantum key distribution*) koristi seriju fotona (svjetlosnih čestica) za prijenos podataka s jedne lokacije na drugu preko optičkog kabela. Uspoređujući mjerenja svojstava izdvajanja tih fotona, dvije krajnje točke mogu odrediti koji je ključ i je li siguran za upotrebu. Način radi prikazan je na Slika 13 [34].

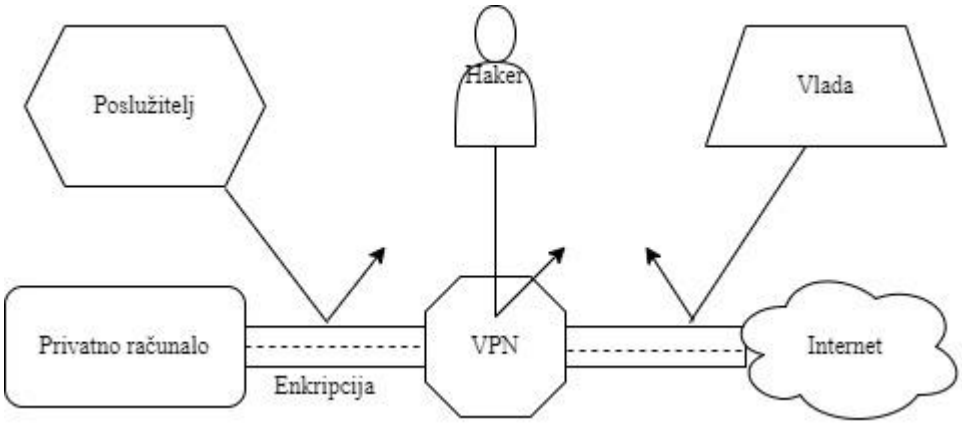


Slika 13 Način rada kvantne kriptografije
Izvor: [35]

Pošiljatelj šalje fotone kroz filter ili polarizator koji im nasumično daje jednu od četiri moguće polarizacije i oznake bita. Fotoni putuju do prijemnika, koji koristi dva razdjelnika snopa (horizontalni ili vertikalni i dijagonalni) za očitavanje polarizacije svakog fotona. Prijemnik ne zna koji razdjelnik snopa koristiti za svaki foton, te mora pogoditi koji će koristiti. Nakon što je tok fotona poslan, primatelj javlja pošiljatelju koji je razdjelnik snopa korišten za svaki od fotona u slijedu kojim su poslani, a pošiljatelj uspoređuje tu informaciju sa slijedom polarizatora korištenih za slanje ključa. Fotoni koji su očitani pomoću pogrešnog razdjelnika snopa se odbacuju, a rezultat od niza bitova postaje ključ. U slučaju ako prisluškivač pročita ili na bilo koji način kopira foton, stanje fotona će se promijeniti. Promjenu će otkriti krajnje točke. To znači da se ne može pročitati foton i proslijediti ga dalje ili napraviti njegovu kopiju, a da se ne otkrije [34].

4.6. Virtualna privatna mreža

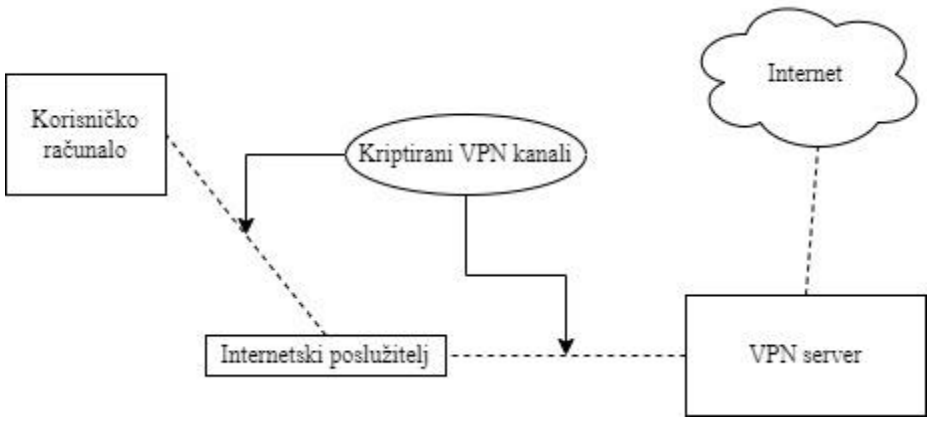
VPN (engl. *Virtual Private Network*) predstavlja kraticu koja označava virtualnu privatnu mrežu. VPN se odnosi na tehnologiju koja se temelji na sigurnom povezivanju računala ili privatnih mreža u jednu zajedničku mrežu koja se koristi kroz privatnu ili javnu mrežnu infrastrukturu. **Slika 14** prikazuje način rada VPN-a.



Slika 14 Prikaz rada VPN-a
Izvor: [36]

Funkcioniranje VPN-a događa se na sljedeći način [36]:

1. VPN softver na računalu korisnika kriptira njegov podatkovni promet i zatim ga šalje VPN serveru putem sigurne veze.
2. Kriptirani podaci sa računala korisnika su nakon toga dekriptirani uz pomoć VPN servera.
3. VPN server zatim odlazi na internet s takvim dešifriranim podacima i prima sav promet kojeg korisnik traži.
4. VPN nakon toga ponovo kriptira podatke i šalje ih natrag korisniku.
5. VPN softver na računalu korisnika dekriptira dobivene podatke kako bi ih korisnik mogao razumjeti i koristiti.



Slika 15 Funkcioniranje VPN-a
Izvor: [36]

Slika 15 prikazuje način funkcioniranja VPN-a.

4.7. Tijela za sigurnost i zaštitu komunikacije

Razvojem i globalizacijom društva, informacije i informacijski sustavi moraju biti zaštićeni i sigurni u državnim sektorima. Sigurnosna politika kod mrežne komunikacije se temelji na organizacijskom i upravljačkom skladu, odnosno tko je za što odgovoran. Politiku izvode stručna tijela za upravljanje sigurnošću kao što su u Hrvatskoj [37]:

- Odjel CERT.
- Zavod za sigurnost informacijskih sustava (ZSIS).

4.7.1. Odjel CERT

CERT predstavlja odjel CARNET-a (Hrvatske akademske i istraživačke mreže). Osnovan je 30. listopada 2007. godine i bavi se prevencijom i zaštitom od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj [37].

CERT se bavi incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru, osim tijela državne uprave za koje je nadležan Zavod za sigurnost informacijskih sustava (ZSIS). Osim toga, Nacionalni CERT se bavi incidentima sa znatnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga [37].

CERT surađuje u području kibernetičke sigurnosti u Hrvatskoj s nacionalnim relevantnim tijelima te sudjeluje u radu tijela proizašlih iz Nacionalne strategije kibernetičke sigurnosti: Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost [37].

Metode CERT-a su [5]:

1. Redovito ažuriranje operacijskog sustava i svih aplikacija koje dolaze u kontakt sa sadržajima na internetu.
2. Korištenje dobre enkripcije na kućnoj bežičnoj mreži i javnoj bežičnoj mreži.
3. Korištenje kompleksne lozinke za pristup javnim servisima (društvenim mrežama, elektroničkoj pošti i sl.).
4. Kod poslovanja s karticama ili korištenja servisa koji mogu obavljati transakcije, treba provjeravati ispravnost certifikata servisnih stranica.
5. Kod novčanih transakcija, a posebno rada s elektroničkim bankarstvom, potrebno je obaviti s računala koji su najmanje izloženi riziku zaraze.
6. Kod poslovanja novcem na internetskom pregledniku potrebno je osobno upisivanje adrese, ne korištenje poveznice iz primljenih poruka.
7. Kod primanja poruka u kojoj se nudi ili se traži nešto neočekivano, potrebna je provjera ako je prijevara.

8. Čuvanje sigurnosne kopije najvažnijih podataka potrebno je provjeriti sadržaj antivirusnim alatom.
9. Da se ne ugrađuje u računalo aplikacije iz nepoznatih i neprovjerenih izvora, posebno ako se radi o sigurnosnim alatima.
10. Da se ne isključuje vatrozid i antivirusni alati i ne ignoriraju njihova upozorenja.

4.7.2 Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava [38].

Djelokrug i zadaće Zavoda za sigurnost informacijskih sustava utvrđeni su Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakonom o informacijskoj sigurnosti te Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti [38].

U skladu sa zakonskom regulativom, pored poslova sigurnosne akreditacije informacijskih sustava, Zavod za sigurnost informacijskih sustava nadležan je i za provedbu aktivnosti u svezi s upravljanjem kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između državnih tijela i stranih država i organizacija kao i poslove istraživanja, razvoja i ispitivanja tehnologija namijenjenih zaštiti klasificiranih podataka te izdavanja uvjerenja za njihovu uporabu [38].

Osim poslova prevencije i odgovora na računalne ugroze informacijskih sustava, Zavod za sigurnost informacijskih sustava zadužen je za reguliranje standarda tehničkih područja sigurnosti informacijskih sustava pravilnicima i njihovo trajno usklađivanje s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava [38].

4.8. Sigurnosni protokoli na OSI razinama

Kao što se navelo u radu, u svijetu se podaci prenose na masovnoj razini, a sigurnost tih podataka je izuzetno važna, stoga internetska sigurnost pruža tu značajku, tj. zaštitu podataka. Postoje različite vrste protokola poput protokola za usmjeravanje, prijenos pošte i protokola za udaljenu komunikaciju. Iznimno važni protokoli su internetski sigurnosni protokoli koji pomažu u sigurnosti i cjelovitosti podataka na internetu. Postoje mnogi protokoli za sigurnost podataka, kao što su protokol za prijenos zaštitno kodiranih podataka SSL (engl. *Secure Socket Layer*), sigurnosni Internet protokol IPsec (engl. *Internet Protocol Security*), sigurnosni protokol transportnog sloja TLS (engl. *Transport Layer Security*) [39].

4.8.1. Sigurnost internetskog protokola IPsec

IPsec (engl. *Internet Protocol Security*) je standard i skup protokola (opcionalan za IPv4, a obavezan za IPv6) koji obuhvaća mehanizme za zaštitu prometa na razini trećeg sloja OSI modela - kriptiranjem i/ili autentifikacijom IP paketa [40].

IPsec osigurava ispunjenje sljedećih sigurnosnih zahtjeva [40]:

- tajnost (engl. *confidentiality*) - isključivo ovlaštena osoba može pristupiti podacima,
- besprijekornost (engl. *integrity*) - nemogućnost promjene podataka od strane neovlaštene osobe.
- autentičnost (engl. *authentication*) - verifikacija identiteta pošiljaoca,
- raspoloživost (engl. *availability*) - dostupnost podacima unatoč neočekivanim događajima, npr. DOS napad i sl.

IPSec nadalje koristi dva načina kada se koristi sama [41]:

- Tunel,
- Transport.

IPSec funkcionira unutar mrežnog sloja te osigurava tajnost, besprijekornost, autentičnost i raspoloživost. Pošto IP protokol osigurava uslugu komunikacijskog kanala od kraja do kraja (eng. *end-to-end*), zaštita kanala na istoj razini korištenjem IPSec-a omogućava mu neovisnost obzirom na niže slojeve. To znači da komunikacijski uređaji na putu između dvaju entiteta ne moraju podržavati IPSec, što omogućava korištenje IPSec-a bez obzira na način implementacije fizičkog sloja i sloja prijenosa podataka. S druge strane, ukoliko dva krajnja entiteta podržavaju IPSec, njegova uporaba je transparentna obzirom na više slojeve protokolnog stoga. Aplikacije mogu koristiti sigurnu komunikaciju koju pruža IPSec, bez obzira na vlastitu funkcionalnost. Isto se odnosi i na protokole koji su implementirani u transportnom sloju, što znači da svi podaci koji se prenose korištenjem TCP i UDP protokola, isto kao i ICMP poruke, mogu koristiti sigurni komunikacijski kanal koji pruža IPSec [19].

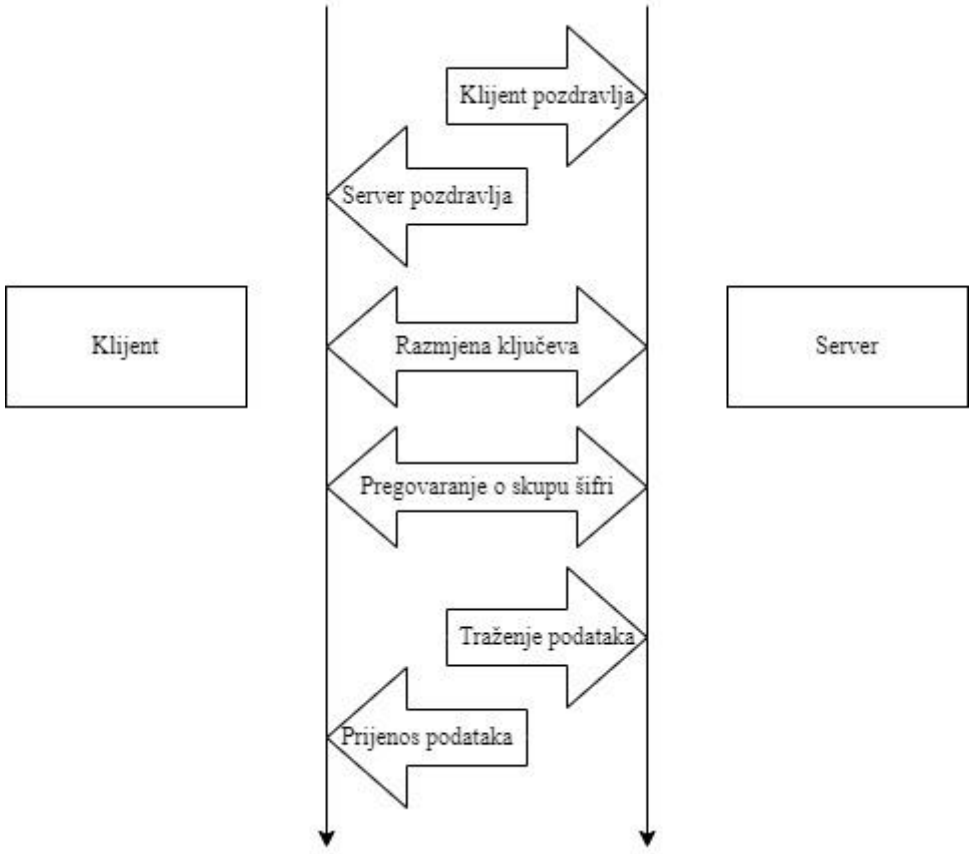
4.8.2. Protokol za prijenos zaštitno kodiranih podataka SSL

SSL (engl. *Secure Sockets Layer*) je internetski sigurnosni protokol koji se temelji na enkripciji. Prvi ga je razvio *Netscape* 1995. godine u svrhu osiguranja privatnosti, provjere autentičnosti i integriteta podataka u internetskoj komunikaciji. SSL je prethodnik moderne TLS enkripcije koja se danas koristi [42].

Kako bi se osigurao visok stupanj privatnosti, SSL šifrira podatke koji se prenose preko *weba*. To znači da će svatko tko pokuša presresti te podatke vidjeti samo iskrivljenu mješavinu znakova koju je gotovo nemoguće dešifrirati [42].

SSL pokreće postupak provjere autentičnosti koji se naziva rukovanje između dva uređaja, koji komuniciraju kako bi se osiguralo da su oba uređaja stvarno ono za što se predstavljaju [42].

SSL također digitalno potpisuje podatke kako bi se osigurao integritet podataka, provjeravajući da podaci nisu neovlašteno mijenjani prije nego što dođu do ciljanog primatelja. Princip rada SSL-a prikazan je na Slika 16 [42].



Slika 16 SSL princip rada
Izvor: [43]

4.8.3. Protokol za zaštitu transportnog sloja TLS

Sigurnost transportnog sloja ili TLS (engl. *Transport Layer Secure*) široko je prihvaćen sigurnosni protokol osmišljen kako bi omogućio privatnost i sigurnost podataka za komunikaciju putem Interneta. Primarni slučaj upotrebe TLS-a je šifriranje komunikacije između *web* aplikacija i poslužitelja, kao što su *web* preglednici koji učitavaju *web* mjesto. TLS se također može koristiti za šifriranje drugih komunikacija kao što su e-pošta, slanje poruka i glas preko IP-a (VoIP engl. *Voice over Internet Protocol*) [42].

Za implementaciju TLS-a, *web* mjesto ili aplikacija mora imati TLS certifikat preuzet na svom izvornom poslužitelju ili SSL certifikat. Tijelo za izdavanje certifikata izdaje ovaj

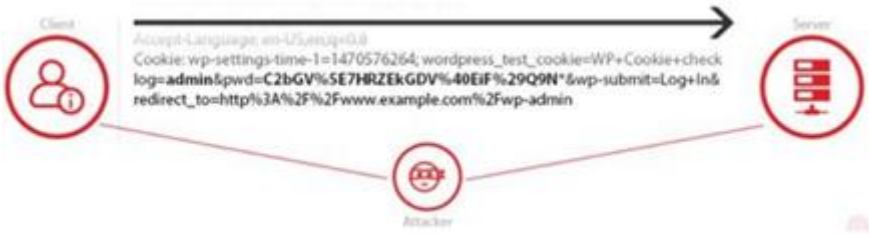
certifikat pojedincu ili tvrtki koja posjeduje određenu domenu stranice. TLS certifikat uključuje vitalne detalje o tome tko je vlasnik domene i javni ključ poslužitelja, koji su potrebni za autentifikaciju identiteta poslužitelja [44].

Nakon provjere autentičnosti, TLS veza se pokreće putem TLS sekvence rukovanja. Kada krajnji korisnik posjeti *web* stranicu koristeći TLS, TLS rukovanje se pokreće između korisničkog uređaja (klijentskog uređaja) i *web* poslužitelja [44].

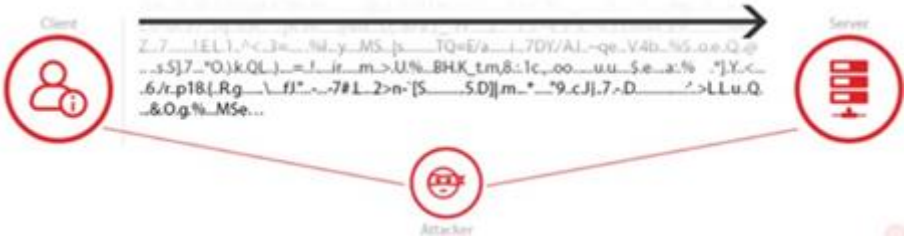
4.8.4. HTTPS protokol

HTTPS(engl. Hypertext Transfer Protocol Secure) je nadogradnja HTTP protokola kako bi se ostvarila sigurna komunikacija preko računalne mreže, najčešće Interneta. HTTPS protokol korištenjem SSL ili TLS protokola postiže očuvanost integriteta i privatnost poruka poslanih između klijenta i servera tako da sve poruke budu šifrirane. Takav način slanja poruka je najbolji način za sprječavanja MITM napada zbog toga što i u slučaju da napadač presretne komunikaciju i dalje ne može vidjeti tekst poruke ili mijenjati poruku. SSL i TLS protokoli koriste enkripciju javnim ključem. Poruke se šifriraju javnim ključevima sudionika u komunikaciji, a mogu se pročitati samo ako su dešifrirane korištenjem privatnog ključa osobe za koju je poruka namijenjena što je prikazano **Slika 17** i **Slika 18**. Na ovaj način riješen je problem poruke u prijenosu [10].

Mora se napomenuti kako su stranice koje koriste HTTPS sporije, jer se u odnosu na HTTP ipak šalje količinski više podataka u svakom zahtjevu i odgovoru (zbog enkripcijskih ključeva i *cipher* sadržaja). Uz današnje brzine interneta i drugih pratećih terminalnih oprema, to ne predstavlja veliki problem, ali činjenica jest da se u milisekundama HTTP brže "vrti" kroz mrežu nego HTTPS [45].



Slika 17 Poruka bez HTTPS enkripcije čitljiva napadaču
Izvor: [10]



Slika 18 Poruka sa HTTPS enkripcijom vidljiva napadaču
Izvor: [10]

5. ZAKLJUČAK

Sigurnost mreže obuhvaća mnoge korake koji se poduzimaju za zaštitu integriteta računalne mreže i podataka unutar nje. Mrežna sigurnost je važna jer štiti vrlo osjetljive podatke od *cyber* napada, zlonamjernih programa, unutarnjih prijetnji unutar sustava, MITM napada i ostalih te osigurava da je mreža upotrebljiva i pouzdana. Mnoge prijetnje vidljivo utječu na sigurnost, integritet i povjerljivost podataka unutar mrežne komunikacije.

Analizom trenutno dostupnih trendova i statističkih pokazatelja prikazano je da velika većina populacije koristi uvelike informacijske i komunikacijske sustave te da je njihova intima sve više ugrožena bilo u privatne ili poslovne svrhe. Napadi se isključivo provode nad osobama unutar važnih tvrtki ili ustanova, koji svoje podatke nenamjerno ili namjerno ustupaju akterima prijetnje. Namjerno zbog toga da bi osigurali što bolju poziciju unutar neke tvrtke, jer su maliciozno izdali prijetnju. Najčešće se koriste razne vrste platformi i sustava za prijetnju. Koliko te vrste prijetnji rastu, toliko treba razvijati metode koje suzbijaju iste.

Razvijeni su razni primjeri načina sprječavanja ugrožavanja bilo kakve vrste mrežne komunikacije. Pokazatelji toga su vatrozid koji je jedan od najupotrebljivijih i najučinkovitijih primjera. Zaštita osjetljivih informacija i podataka očituje se u mnogim drugim mehanizmima kao što su sustavi za otkrivanje napada, sustavi za sprječavanje napada, razne vrste kriptiranja i sigurnosnih protokola. Primarni cilj mrežne sigurnosti je spriječiti neovlašteno pristupanje, u ili između dijelova mreže pomoću mehanizama koji se upotrebljavaju u kombinaciji, ali ne zasebno.

Sukladno pokušaju kibernetičkih kriminalaca da dobiju pristup podacima, ukradu nečiji identitet ili naruše ugled, tvrtke ili ustanove stvaraju potrebu za osobljem koje će spriječiti takve namjere pomoću raznih sigurnosnih metoda i alata u mrežnoj komunikaciji.

Metode u zaštiti mrežne komunikacije koje su prikazane u radu uvelike pomažu spriječiti razne napade, ali napadi postaju sve više sofisticirani, što dovodi do potrebe za razvojem novih metoda zaštite, kao što je kvantna kriptografija. Prednost kvantne komunikacije leži u prisluškivanju, sigurnijoj komunikaciju te nudi više metoda za sigurnost pomoću brojnih protokola.

LITERATURA

[1] Digital around the world. Preuzeto sa: https://datareportal.com/global-digital-overview. [Pristupljeno: travanj 2021].

[2] Antoliš, Krunoslav; Ždrnja, Bojan; Pakšić, Ivan; Vugrek, Alen; Pavliček, Josip; Marijenović, Ivana; Šegudović, Hrvoje; Jušić, Saša. Sigurnost informacijskih sustava. Zagreb. 2010.

[3] Cia Triad of Information Security. Preuzeto sa: https://www.techopedia.com/definition/25830/cia-triad-of-information-security. [Pristupljeno: travanj 2021].

[4] Carnet Cert godisnji izvjestaj. Preuzeto sa: https://www.cert.hr/wp-content/uploads/2021/02/Carnet_Cert_godisnji_izvjestaj_2020_0402-3.pdf. [Pristupljeno: rujan 2022].

[5] Cert naivci brosura web. Preuzeto sa: https://www.cert.hr/wp-content/uploads/2019/03/cert_naivci_brosura_web-1.pdf. [Pristupljeno: svibanj 2021].

[6] Zlonamjerni sadrzaj. Preuzeto sa: https://gov.hr/hr/zlonamjerni-sadrzaj/1232. [Pristupljeno: rujan 2020].

[7] Ransomeware. Preuzeto sa: http://apps.jutarnji.hr/ransomware/. [Pristupljeno: rujan 2022].

[8] How does wiper malware work. Preuzeto sa: https://www.packetlabs.net/posts/how-does-wiper-malware-work/. [Pristupljeno: siječanj 2023].

[9] TrojanHorseVirus.Preuzeto sa: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus. [Pristupljeno: siječanj 2023].

[10] D.Varelija. Napadi tipa Man-in-the-middle na HTTPS i njihovo prepoznavanje. Sveučilište u Rijeci, Završni rad 2018.

[11] Sta je man in the middle napad. Preuzeto sa: https://www.it-klinika.rs/blog/sta-je-man-in-the-middle-napad. [Pristupljeno: siječanj 2023].

[12] Sto su ddos napadi i mozemo li se zastititi od njih. Preuzeto sa: https://www.pro-ping.hr/blog?sto-su-ddos-napadi-i-mozemo-li-se-zastititi-od-njih. [Pristupljeno: rujan 2022].

[13] DDoS attacks. Preuzeto sa: https://www.imperva.com/learn/ddos/ddos-attacks/. [Pristupljeno: rujan 2022].

[14] Advanced persistent threat apt. Preuzeto sa: https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/. [Pristupljeno: rujan 2022].

[15] Network attacks and network security threats. Preuzeto sa : https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/. [Pristupljeno: veljača 2023].

[16] Defining insider threats. Preuzeto sa: https://www.cisa.gov/defining-insider-threats. [Pristupljeno: veljača 2023].

[17] Internal attack 4 employee identikits that could prove to be a threat to your company. Preuzeto sa: https://deltalogix.blog/en/2021/07/07/internal-attack-4-employee-identikits-that-could-prove-to-be-a-threat-to-your-company/. [Pristupljeno: veljača 2023].

[18] SQL-injection. Preuzeto sa: https://portswigger.net/web-security/sql-injection. [Pristupljeno: veljača 2023].

[19] T. Šoštarić. Sigurnost i zaštita računalnih mreža. Sveučilište u Zagrebu, Završni rad 2016.

[20] Najbolji besplatni antivirusni programi za 2019. godinu. Preuzeto sa: https://pcchip.hr/softver/sigurnost/najbolji-besplatni-antivirusni-programi-za-2019-godinu/. [Pristupljeno: lipanj 2021].

[21] Što je antivirusni program. Preuzeto sa: https://geek.hr/pojmovnik/sto-je-antivirusni-program/. [Pristupljeno: lipanj 2021].

[22] Zaštita mreže vatrozid. Preuzeto sa: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html. [Pristupljeno: lipanj 2021].

[23] Firewall penetration testing. Preuzeto sa: https://purplesec.us/firewall-penetration-testing/. [Pristupljeno: rujan 2022].

[24] Stateless vs stateful packet filtering firewalls. Preuzeto sa: https://www.geeksforgeeks.org/stateless-vs-stateful-packet-filtering-firewalls/. [Pristupljeno: rujan 2022].

[25] Application firewall. Preuzeto sa: https://www.techopedia.com/definition/13566/application-firewall. [Pristupljeno: rujan 2022].

[26] A. Alilović. Sustavi za otkrivanje i sprječavanje napada. Sveučilište u Zagrebu, Završni rad 2019.

[27] E. Modrić. Sigurnosni sustavi za otkrivanje napada. Sveučilište u Zagrebu, Diplomski rad 2008.

[28] G. Gledec, M. Mikuc i M. Kos, Sigurnost u privatnim komunikacijskim mrežama. Sveučilište u Zagrebu, Fakultet elektronike i računarstva, 2008.

[29] N. Ružić. Zaštita djece na internetu. Nova prisutnost: časopis za intelektualna i duhovna pitanja. 2011;Vol. IX No.1. Preuzeto sa: https://hrcak.srce.hr/72422. [Pristupljeno: rujan 2022].

[30] CERT, LSS. Metode zaštite dokumenata. Sveučilište u Zagrebu, Fakultet elektronike i računarstva, 2010.

[31] Symmetric key encryption why where and how its used in banking. Preuzeto sa: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking. [Pristupljeno: rujan 2022].

[32] Concepts symmetric cryptography. Preuzeto sa: https://www.ibm.com/docs/en/ztpf/2020?topic=concepts-symmetric-cryptography. [Pristupljeno: rujan 2022].

[33] What is asymmetric encryption how does it work. Preuzeto sa: https://sectigostore.com/blog/what-is-asymmetric-encryption-how-does-it-work/. [Pristupljeno: rujan 2022].

[34] Quantum cryptography explained. Preuzeto sa: https://quantumxc.com/blog/quantum-cryptography-explained/. [Pristupljeno: rujan 2022].

[35] Quantum key distribution. Preuzeto sa: https://www.drishtiias.com/daily-news-analysis/quantum-key-distribution. [Pristupljeno: rujan 2022].

[36] Što je VPN i zašto vam je potreban?. Preuzeto sa: https://marketingorbis.com/2020/03/02/sto-je-vpn-i-zasto-vam-je-potreban/. [Pristupljeno: lipanj 2021].

[37] Nacionalni CERT. Preuzeto sa: https://gov.hr/hr/nacionalni-cert/1230. gov.hr. [Pokušaj pristupa 06 09 2022].

[38] Republika Hrvatska. Zavod za sigurnost informacijskih sustava. Izdanje: NN 79/07. Zagreb: Narodne novine; 2007.

[39] Types of internet security protocols. Preuzeto sa: https://www.geeksforgeeks.org/types-of-internet-security-protocols/. [Pristupljeno: rujan 2022].

[40] A. Kukec. Uvod u IPsec standard i IKEv2 protokol. Sveučilište u Zagrebu, Seminarski rad 2006.

[41] What is IPsec tunnel Preuzeto sa: https://hr.go-travels.com/what-is-ipsec-tunnel. [Pristupljeno: rujan 2022].

[42] Transport layer security tls Preuzeto sa: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/. [Pristupljeno: rujan 2022].

[43] Support how ssl works. Preuzeto sa: https://certs.securetrust.com/support/support-how-ssl-works.php. [Pristupljeno: rujan 2022].

[44] What is transport layer security and how does it work. Preuzeto sa: https://www.tokenex.com/blog/vh-what-is-transport-layer-security-and-how-does-it-work. [Pristupljeno: rujan 2022].

[45] Http ili https sto znaci to slovo s viska. Preuzeto sa: https://www.leramis.hr/2019/01/http-ili-https-sto-znaci-to-slovo-s-viska/. [Pristupljeno: rujan 2022].

[46] Republika Hrvatska. Zakon o informacijskoj sigurnosti. Izdanje: NN 79/07. Zagreb: Narodne novine; 2007.

[47] CERT godisnje izvjesce 2021. Preuzeto sa: https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf. [Pristupljeno: rujan 2022].

[48] Backdoor Trojan. Preuzeto sa: https://www.firewalls.com/blog/security-terms/backdoor-trojan/. [Pristupljeno: rujan 2022].

POPIS SLIKA

POPIS GRAFOVA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da 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/diplomskog rada pod naslovom Pregled metoda i alata primjenjivih u zaštiti mrežne komunikacije, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 06.03. A. Žmilić

(ime i prezime, *potpis*)