Analiza prijetnji i rizika kibernetičke sigurnosti te njihov utjecaj na poslovanje poduzeća

Šimić, Zvonimir

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilišni studij

Analiza prijetnji i rizika kibernetičke sigurnosti te njihov utjecaj na poslovanje poduzeća

Diplomski rad

Zvonimir Šimić

Osijek, 2023.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit

Osijek, 15.09.2023.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za diplomski ispit

Ime i prezime Pristupnika:	Zvonimir Šimić
Studij, smjer:	Diplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	D-1166R, 13.10.2020.
OIB studenta:	11058884546
Mentor:	izv. prof. dr. sc. Krešimir Grgić
Sumentor:	,
Sumentor iz tvrtke:	Boris Bajtl
Predsjednik Povjerenstva:	izv. prof. dr. sc. Višnja Križanović
Član Povjerenstva 1:	izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	mr. sc. Anđelko Lišnjić
Naslov diplomskog rada:	Analiza prijetnji i rizika kibernetičke sigurnosti te njihov utjecaj na poslovanje poduzeća
Znanstvena grana diplomskog rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak diplomskog rada:	U radu je potrebno analizirati i predstaviti potencijalne prijetnje i rizike kibernetičke sigurnosti, te analizirati i prikazati globalno stanje i posljedice kibernetskih napada na poslovanje poduzeća (uz konkretne primjere). Potrebno je provesti analizu prijetnji i rizika kibernetičke sigurnosti na lokalnom poduzeću prema ISO standardima. Tema rezervirana za: Zvonimir Šimić Sumentor iz tvrtke: Boris Bajtl (Atos)
Prijedlog ocjene pismenog dijela ispita (diplomskog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 3 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene od strane mentora:	15.09.2023.

Potvrda mentora o predaji konačne verzije rada:	*Mentor elektronički potpisao predaju konačne verzije.*
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

IZJAVA O ORIGINALNOSTI RADA

Osijek, 29.09.2023.

Ime i prezime studenta:	Zvonimir Šimić
Studij:	Diplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	D-1166R, 13.10.2020.
Turnitin podudaranje [%]:	3

Ovom izjavom izjavljujem da je rad pod nazivom**: Analiza prijetnji i rizika kibernetičke sigurnosti te njihov utjecaj na poslovanje poduzeća**

izrađen pod vodstvom mentora izv. prof. dr. sc. Krešimir Grgić

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

U današnjem svijetu, bilo to preko mrežnih stranica, televizije ili radija, sve više se spominje pojam kibernetičke sigurnosti (engl. *Cybersecurity*). Kako bi se moglo raspravljati o navedenom pojmu, prvo je potrebno definirati sam pojam. Dakle, kibernetička sigurnost je umjetnost zaštite mreža, uređaja i podataka od neovlaštenog pristupa ili nezakonite upotrebe te praksa osiguravanja povjerljivosti, integriteta i dostupnosti informacija [1]. Svijet se sve više oslanja na tehnologiju i taj trend će se nastaviti i na sljedeću generaciju nove tehnologije koja će sve više imati pristup našim povezanim uređajima putem tehnologija kao što su Bluetooth i Wi-Fi. Kako bi podaci koji se nalaze na tim uređajima bili zaštićeni od neovlaštenog pristupa i zloupotrebe, potrebno je implementirati određene sigurnosne mjere. Uređaje ne koriste samo pojedinci u privatne svrhe. Organizacije i poduzeća svih veličina svakodnevno razmjenjuju informacije, usluge, komuniciraju te vrše transkacije uz pomoć tehnologije. Uspješan kibernetički napad može uzrokovati veliku štetu u poslovanju. To može utjecati na ukupnu sliku organizacije ili poduzeća, kao i na ugled njihovog poslovanja i povjerenje klijenata. Uspješan kibernetički napad može poduzeću izazvati velike financijske, reputacijske i pravne posljedice. Rad se sastoji od pet poglavlja, uzimajući u obzir da je prvo poglavlje uvod. U drugom poglavlju se detaljnije objašnjava sam pojam kibernetičke sigurnosti, zatim se kibernetička sigurnost raščlanuje na njezine domene te se detaljno opisuju vrste sigurnosnih prijetnji te kako njima rukovati. U trećem poglavlju se analizira trenutno globalno stanje kibernetičke sigurnosti te se provodi analiza nekoliko stvarnih sigurnosnih incidenata. Zatim se raščlanjuju posljedice sigurnosnih incidenata, na koji bi način poduzeća trebala reagirati na njih te kako ih u budućnosti spriječiti. Na samom kraju trećeg poglavlja se govori o stanju kibernetičke sigurnosti u Republici Hrvatskoj. U četvrtom poglavlju je provedena analiza kibernetičke sigurnosti nad lokalnim poduzećem te u posljednjem poglavlju je izveden zaključak u kojem se daje osvrt na ciljeve samog diplomskog rada te postignute rezultate analize kibernetičke sigurnosti u lokalnom poduzeću.

2. KIBERNETIČKA SIGURNOST

U ovom poglavlju opisan je pojam kibernetičke sigurnosti, što on obuhvaća te zbog čega sam pojam nije uvijek shvaćen. Opisane su domene kibernetičke sigurnosti, kako su formirane i od čije strane. Dalje, u poglavlju su opisane i objašnjene vrste sigurnosnih prijetnji i posljedice njihove pojave, te na koji je način potrebno rukovati sigurnosnim prijetnjama i kako se to radi u praksi.

2.1. Pojam kibernetičke sigurnosti

Sam pojam kibernetičke sigurnosti je jednostavno definirati, ali pojam ne znači uvijek isto svim ljudima u različitim strukama i okruženjima u kojima se nalaze. Na primjer, kibernetička sigurnost pojedinca u prosječnom domu je stvoriti dovoljno snažnu lozinku za bežični internet kako se netko od susjeda ne bi spojio te stvarao dodatan promet na internet mreži, dok kibernetička sigurnost vladinih organizacija predstavlja nešto potpuno drugo.

Generalno, na primjer, za individualnu osobu, kibernetička sigurnost znači da su njegovi privatni podaci nedostupni svima onima kojima pristup nije autoriziran te njegovi računalni sustavi i uređaji rade ispravno bez zlonamjernog softvera. Za vlasnike manjih poduzeća, kibernetička sigurnost može uključivati osiguravanje da su podaci kreditnih kartica pravilno zaštičeni te da su standardi za sigurnost podataka pravilno implementirani na registrima prodajnih mjesta. Za pružatelje zajedničkih usluga , kibernetička sigurnost može uključivati zaštitu brojnih podatkovnih centara u kojima se nalaze razni poslužitelji koji drže virtualne poslužitelje koji pripadaju mnogim različitim organizacijama. Za poduzeća koja posluju o*nline,* to može biti uključivanje zaštite poslužitelja sa kojima neprovjereni eksterni korisnici redovito komuniciraju, dok za vladu, kibernetička sigurnost može uključivati uspostavljanje različitih klasifikacija podataka, svaku sa svojim skupom povezanih zakona, politika, postupaka i tehnologija [2].

Ovim primjerima su prikazana različita značenja pojma kibernetičke sigurnosti, dok bi jedna od formalnih definicija, koja je već spomenuta u samom uvodu ovog dokumenta, bila: kibernetička sigurnost je umjetnost zaštite mreža, uređaja i podataka od neovlaštenog pristupa ili nezakonite upotrebe te praksa osiguravanja povjerljivosti, integriteta i dostupnosti informacija [1].

2.2. Domene kibernetičke sigurnosti

Kibernetička sigurnost je vrlo opširan pojam te je iz toga razloga vrlo bitno definirati te kategorizirati sve aktivnosti koje pojam obuhvaća. Općeprihvaćena kategorizacija tih aktivnosti

na domene je ona koja se nalazi unutar strukture ispita za polaganje CISSP certifikata. CISSP (engl. *Certified Information Systems Security Professional*) je jedan od najjačih i najviše cjenjenih certifikata u industriji kibernetičke sigurnosti. CISSP certifikat izdaje Međunarodni konzorcij za certifikaciju stručnjaka za područje sigurnosti informacijskih sustava, poznatiji kao $(ISC)^2$. Prema $(ISC)^2$, CISSP je je globalno najpriznatiji certifikat na tržištu informacijske sigurnosti. CISSP potvrđuje duboko tehničko i menadžersko znanje i iskustvo stručnjaka za informacijsku sigurnost za učinkovito dizajniranje, projektiranje i upravljanje cjelokupnom sigurnosnom slikom organizacije [3]. Prema $(ISC)^2$, kibernetička sigurnost se dijeli na 8 kategorija ili domena:

- Sigurnost i upravljanje rizicima (engl. *Security and Risk Management)*
- Sigurnost imovine (engl. *Asset Security*)
- Sigurnosna arhitektura i inženjerstvo (engl. *Security Architecture and Engineering*)
- Sigurnost komunikacije i mreže (engl. *Communication and Network Security*)
- Upravljanje identitetom i pristupom (engl. *Identity and Access Management*, IAM)
- Procjena sigurnosti i sigurnosno testiranje (engl. *Security Assessment and Testing*)
- Sigurnosne operacije (engl. *Security Operations*)
- Sigurnost razvoja softvera (engl. *Software Development Security*)

Sigurnost i upravljanje rizicima pokriva područja pridržavanja profesionalne etike, sigurnosnih koncepata, načela upravljanja sigurnošću, određivanje usklađenosti i drugih sigurnosnih zahtjeva, pravna i regulatorna pitanja koja se odnose na informacijsku sigurnost, razumijevanje zahtjeva za različite vrste istraga (administrativne, kaznene, građanske i slično), razvijanje, dokumentiranje i implementiranje sigurnosne politike, standarda, postupaka i smjernica. Pokriva područja identificiranja, analiziranja i određivanja prioriteta zahtjeva za kontinuitet poslovanja, sigurnosne politike i procedure osoblja, koncepte upravljanje rizikom, koncepte i metodologije modeliranja prijetnji, koncepte upravljanja rizikom lanca opskrbe, uspostavljanje sigurnosnih treninga i edukacija. **Sigurnost imovine** uključuje identificirianje i klasificiranje informacija i imovine, uspostavljane zahtjeva za rukovanje informacijama i imovinom, ispravno osiguravanje resursa, upravljanje životnim ciklusom podataka, osiguravanje ispravne kontrole zadržavanja imovine, određivanje sigurnosnih kontrola podataka i zahtjeva usklađenosti. **Sigurnosna arhitektura i inženjerstvo** uključuje istraživanje, implementiranje i upravljanje inžinjerskim procesim koristeći načela sigurnosnog dizajna, temeljne koncepte sigurnosnih modela (*Biba, Star model, Bell-LaPadula*), odabir kontrola na temelju sigurnosnih zahtjeva sustava, sigurnosne mogućnosti informacijskih sustava kao što su zaštita memorije, enkripcija/dekripcija. Uključuje procjenjivanje i ublaživanje ranjivosti sigurnosnih arhitektura, dizajna i ostalih elemenata, primjenu sigurnosnih

načela na dizajn mjesta i objekata, dizajn sigurnosnih kontrola mjesta i objekata. **Sigurnost komunikacije i mreže** uključuje područja procjene i implementacije sigurnog dizajna u mrežnim arhitekturama, pod čim su uključeni OSI (engl. *Open System Interconnection*) i TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) modeli, sigurnosni protokoli, konvergirani protokoli, kao što su FcoE (engl. *Fiber Channel Over Ethernet*), iSCI (engl. *Internet Small Computer Systems Interface*) i VoIP (engl. *Voice over Internet Protocol*), bežične mreže, mobilne mreže te mreže za distribuciju sadržaja (engl. *Content Distribution Networks*). Pod ovom domenom još su uključena područja implementacije sigurnosnih komunikacijskih kanala te područja sigurnosnih mrežnih komponenti kao što su NAC (engl. *Network Access Control*) uređaji te krajnji uređaji (engl. *Endpoint devices*). **Upravljanje identitetom i pristupom** podrazumijeva kontrolu fizičkog i logičkog pristupa imovini, upravljanje identifikacijom i autorizacijom ljudi, uređaja i usluga, implementacije i upravljanje autorizacijskim mehanizmima kao što su RBAC (engl. *Role Based Access Control*), MAC (engl. *Mandatory Access Control*), DAC (engl. *Discretionary Access Control*) i ABAC (engl. *Attribute Based Access Control*). Podrazumijeva upravljanje životnim ciklusom pružanja identiteta i prava pristupa te implementaciju sustava autorizacije kao što su Oauth (engl. *Open Authorization*), SAML (engl. *Security Assertion Markup Language*), RADIUS (engl. *Remote Authentication Dial-In User Service*) i Kerberos. **Procjena sigurnosti i sigurnosno testiranje** podrazumijeva dizajniranje i provjeru strategije procjenjivanja testiranja i revizije, provođenje testiranje sigurnosnih kontrola pod čime se podrazumijeva procjena ranjivosti, penetracijsko testiranje, pregled zapisa sustava, pregled programskog koda i testiranje tog koda, simulacije uspješnog prodora napadača i slično. Podrazumijeva prikupljanje podataka o sigurnosnom procesu, kao što su tehnički i administrativni podaci. Pod time se podrazumijevaju podaci o upravljanju računa, odobravanju, ključnim pokazateljima uspješnsti, ključnim pokazateljima rizika, podaci o pohrani podataka te podaci kao što su plan oporavka od katastrofe (engl. *Disaster recovery plan*) i plan o kontinuitetu poslovanja (engl. *Business Continuity plan*). Pod ovom domenom se podrazumijeva analiziranje rezultata testiranja te generiranje izvješća na temelju analize rezultata te provođenje sigurnosnih revizija (engl. *Audit*), koje mogu biti interne, eksterne ili od treće strane (engl. *Third party*). Sedma domena, **Sigurnosne operacije**, uključuju aktivnosti kao što su razumijevanje i pridržavanje istraga, što znači skupljanje i pravilno rukovanje dokazima, dokumentiranje i izvještavanje, istražne tehnike, digitalne forenzičke alate, taktike i procedure. Podrazumijeva provođenje aktivnosti evidentiranja i praćenja, pod čime su uključene aktivnosti kao što je otkrivanje i sprječavanje neovlaštenog upada u sustav, sigurnosne informacije i upravljanje događajima, SIEM (engl. *Security Information and Event Management*), kontinuirano praćenje sustava, upravljanje zapisima (engl. *Log*

management), analitika ponašanja korisnika i entiteta, UEBA (engl. *User and Entity Behavior Analytics*). Ova domena uključuje još i aktivnosti upravljanja konfiguracijom (engl. *Configuration Management*), temeljne koncepte sigurnosnih operacija, primjenu zaštite resursa, upravljanje incidentima, provođenje i održavanje detektirajućih i preventivnih mjera, implementaciju i podršku sigurnosnih zakrpa ranjivosti, sudjelovanje u procesima upravljanja promjenama, provođenje strategija oporavka, implementiranje procese oporavka od katastrofe, DR (engl. *Disaster Recovery*), testiranje planova oporavka od katastrofe (engl. *Disaster recovery plan*), implementaciju i upravljanje fizičkim sigurnosnim sustavima te upravljanje pitanjima sigurnosti osoblja. Pod **sigurnost razvoja softvera** je uključeno razumijevanje i integracija sigurnosti u životni ciklus razvoja softvera, SLDC (engl. *Software Development Life Cycle*), koje se sastoji pojmova kao što su razvojne metodologije (npr. *DevOps, Waterfall, Agile*), modela zrelosti kao što je CMM (engl. *Capability Maturity Model*) ili SAMM (engl. *Software Assurance Maturity Model*) te rada i održavanja. Pod ovom domenom se podrazumijevaju aktivnosti identificiranja i primjene sigurnosnih kontrola u ekosustavima razvoja softvera, procjene efektivnosti sigurnosti softvera pomoću revizija i bilježenja promjena te analizom rizika i reagiranjem na rizik. Procjena sigurnosnog učinka novopristiglog softvera je bitan dio ove domene. Naposljetku, pod ovom domenom se podrazumijeva definicija i primjena smjernica i načela sigurnog kodiranja.

2.3. Vrste sigurnosnih prijetnji

U današnjem svijetu postoji veliki broj sigurnosnih prijetnji, iako je ovaj rad usredotočen na sigurnosne prijetnje u domeni kibernetičke sigurnosti, nije moguće pokriti sve sigurnosne prijetnje. Stoga, u ovom podnaslovu će se obraditi najčešće sigurnosne prijetnje koje mogu ugroziti sigurnost pojedinca te poduzeća ili organizacije. Prema Joseph Steinberg-u [2], najčešći kibernetički napadi su podjeljeni na sljedeće cjeline:

- Napadi kojima je primarni cilj nanošenje štete (engl. *Attacks That Inflict Damage*)
- Lažno predstavljanje (engl. *Impersonation*)
- Presretanje (engl. *Interception*)
- Krađa podataka (engl. *Data Theft*)
- Zlonamjerni softver (engl. *Malware*)
- Zatrovane web usluge (engl. *Poisoned Web Service Attacks*)
- Trovanje mrežne infrastrukture (engl. *Network Infrastructure Poisoning*)
- Zlonamjerno oglašavanje (engl. *Malvertising*)
- Iskorištavanje poteškoća u održavanju (engl. *Exploiting Maintenance Difficulties*)

- Napredni napadi (engl. *Advanced Attacks*)

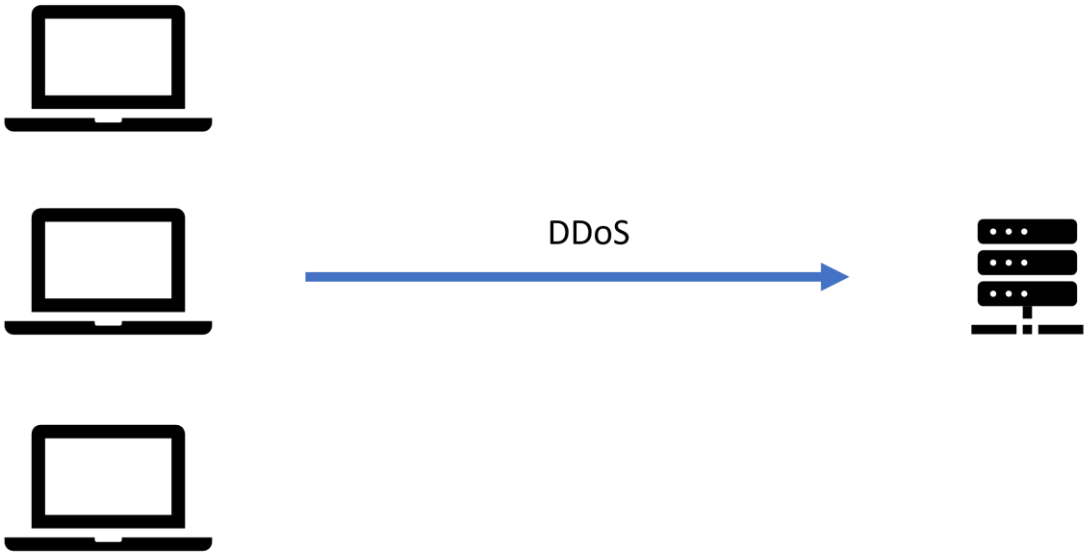
Napadi kojima je primarni cilj nanošenje štete su vrste napada gdje napadačima nije primarni cilj ukrasti žrtvin novac ili osjetljive podatke već prouzročiti štetu. Neki od takvih napada su:

- Napadi uskraćivanja usluge (engl. *Denial-of-service (DoS) attacks*)
- Distribuirani napadi uskraćivanja usluge (engl. *Distributed denial-of-service (DDoS) attacks*)
- Napadi uništavanja podataka (engl. *Data destruction attacks*)

Denial-of-service (DoS) napad je kada haker bombardira mrežu ili poslužitelja proizvoljnim brojem poruka koje uzrokuju to da poslužitelj provjerava autentičnost zahtjeva s nevažećim povratnim adresama. Kada se pošalje odobrenje za autentifikaciju, poslužitelj treba dugo čekati prije zatvaranja veze jer ne može pronaći povratnu adresu napadača, jer su povratne adrese nevažeće [4]. Kada poslužitelj napokon prekine vezu, haker nastavi slati veliki broj sličnih poruka te na taj način uskraćuje dostupnost poslužitelja legitimnim zahtjevima (porukama). Na slici 2.1. je prikazana jednostavna skica DoS napada.

Slika 2.1. *Denial-of-service (DoS)* napad

Distributed denial-of-service (DDoS) je napad u kojem višestruki zaraženi sustavi ciljaju poslužitelj, web stranicu ili bilo koji drugi mrežni resurs kako bi pokrenuli zahtjeve koji rezultiraju uskraćivanjem usluge ovlaštenim korisnicima. Poplava dolaznih poruka, zahtjeva za povezivanjem ili neispravnih paketa ciljnom sustavu može usporiti, zatvoriti ili srušiti sustav što dovodi do uskraćivanja usluge legitimnim korisnicima [4]. Na slici 2.2. je prikazana jednostavna skica DDoS napada.



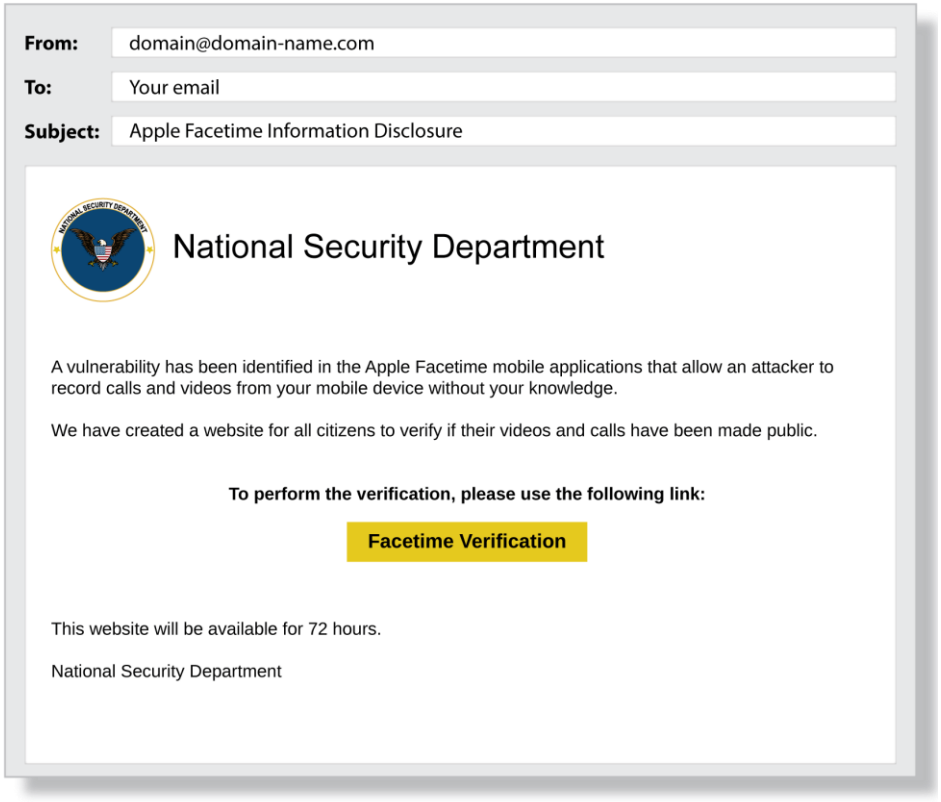
Slika 2.2. *Distributed denial-of-service (DDoS)* napad

Prema istraživanju Kasperky Lab-a iz 2018. godine [5], u istoj godini, prosječna šteta DDoS napada za mala poduzeća je iznosila u prosjeku 120,000$ po napadu, dok za velika poduzeća i organizacije, šteta je iznosila u prosjeku 2,000,000$ po napadu. Botnet-ovi (engl. *Botnets*) i zombiji su pojmovi koji opisuju kompromitirana računala koja pripadaju različitim ljudima ili grupama, kojima haker upravlja daljinski te ih koristi za izvođenje raznih zlonamjernih aktivnosti, bez znanja legitimnih vlasnika tih računala [2].

U slučaju kada je napadačima cilj uništiti ili ugroziti žrtvine podatke ili podatkovne sustave, na primjer, kada žrtva odbija platiti otkupninu prilikom *ransomware* napada, tada govorimo o **napadima uništavanja podataka** [2]. Još jedan primjer su *wiper* napadi. To su napredni napadi uništavanja podataka gdje napadač koristi zlonamjerni softver kako bi obrisao podatke sa žrtvinog tvrdog diska ili SSD-a.

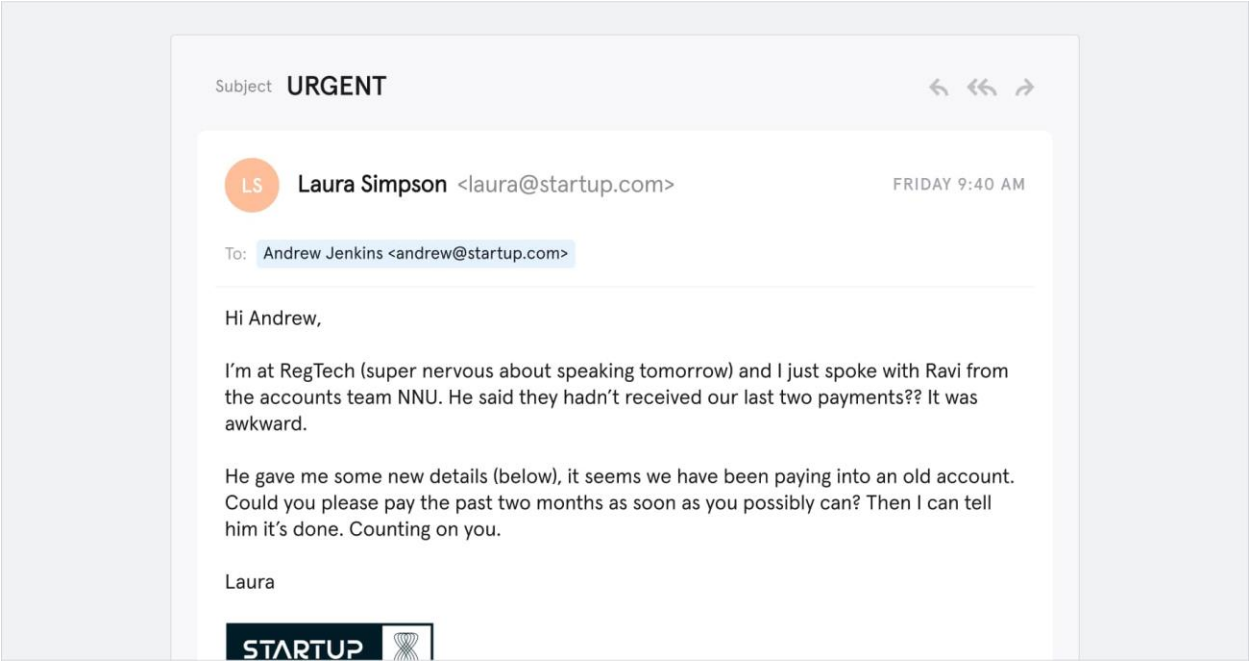
Lažno predstavljanje je jedno od najčešćih sigurnosnih prijetnji u današnjem svijetu što je moguće vidjeti iz raznih statističkih analiza i provedenih istraživanja. Prema provedenom istraživanju Valimail-a iz 2019. godine [6], phishing napadi su još uvijek jedna od najčešćih i najznačajnijih vrsta kibernetičkih napada. Prema provedenom istraživanju nevjerojatnih jedan trilijun phishing e-poruka se pošalje svake godine. Čini se da većina prijetećih e-poruka proizlazi iz SAD-a. Drugim riječima, skoro 3 i pol milijarde phishing e-poruka se slalo globalno svaki dan tijekom 2019. godine. S obzirom na sve veću dostupnost tehnologije te digitalnu transformaciju zadnjih par godina, može se pretpostaviti da je taj broj danas još veći.

Phishing predstavlja zlonamjernu aktivnost u kojoj napadač pokušava uvjeriti žrtvu da izvede nekakvu radnju, koja je uobičajeno štetna samoj žrtvi, a pogodi napadaču, oponašajući subjekt od povjerenja koji opravdano može tražiti takav zahtjev od korisnika [2]. Na primjer, napadač može poslati e-poruku koja izgleda kao legitimna poruka poslana od strane osiguravajuće kuće te tražiti od žrtve da klikne na link koji se nalazi u samoj e-poruci. Kada žrtva klikne na link, bude preusmjerena na lažnu stranicu koja izgleda kao da je legitimna stranica te se od korisnika traži da se prijavi sa svojim korisničkim računom. Na taj način napadač dobije pristup korisničkim podacima, među kojima se nalazi i njihova lozinka. Na slici 2.3. se vidi primjer phishing e-poruke.



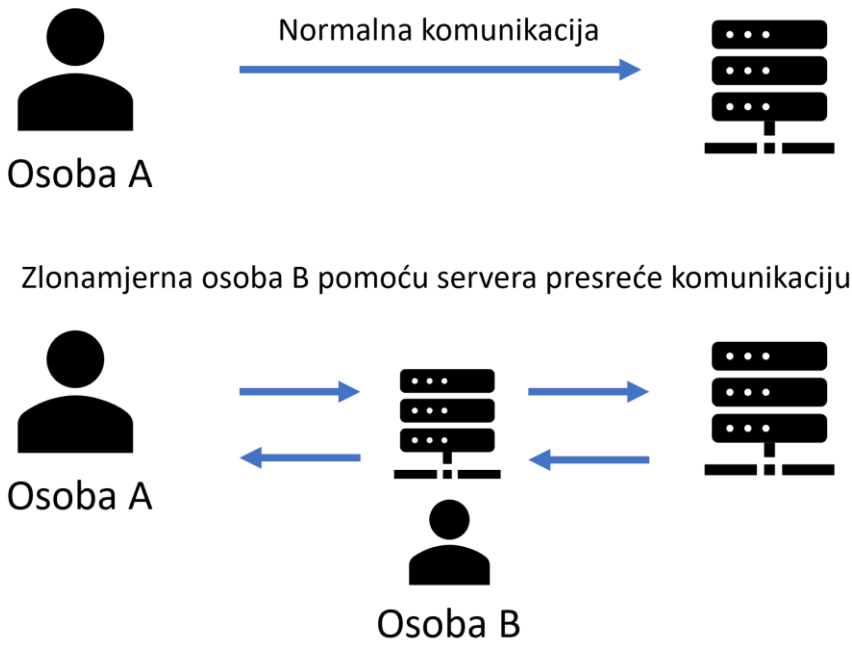
Slika 2.3. Primjer *phishing* E-poruke (https://terranovasecurity.com/wp-content/uploads/2019/08/scenario-3.png)

Spear phishing se odnosi na *phishing* napade koji su osmišljeni za ciljanje specifičnih osoba, poduzeća ili organizacija [2]. Napadač, na primjer, može iskoristiti informacije koje ciljana osoba objavljuje na društvenim mrežama te istražiti odnose sa njezinim poslovnim suradnicima te iskoristiti pronađene informacije za razvijanje personaliziranih i uvjerljivih e-poruka. Na slici 2.4. je prikazan primjer ovakvog pokušaja napada.



Slika 2.4. Primjer *spear phishing* E-poruke (https://www.tessian.com/wp-content/uploads/2019/12/WebsiteBlog-What-Is-Spear-Phishing_-Example-2.jpg.jpg)

Još neki oblici metoda lažnog predstavljanja su *smishing, vishing i whaling*. *Smishing* je vrsta *phishing* napada gdje napadač za komunikaciju koristi tekstualne poruke (SMS) umjesto E-poruka. Cilj napadača je doći do osjetljivih podataka korisnika kao što je lozinka ili ih natjerati da instaliraju zlonamjeran softver. *Vishing* je vrsta *phishing* napada gdje se koristi glasovna komunikacija preko VOIP (engl. *Voice Over IP*) sustava ili starijh sustava poput POTS (engl. *Plain Old Telephone Service*). *Whaling* je oblik *phishing* napada gdje su mete napada osobe visokog profila, kao što je visoko rangirano poslovno osoblje ili vladini dužnošnici[2]. **Presretanje** se najčešće odnosi na sigurnosnu prijetnju gdje zlonamjeran subjekt presreće komunikaciju između dva računala te pristupa podacima koji se prenose tim komunikacijskim kanalom[2]. Ukoliko ti podaci nisu enkriptirani, napadač ih može vrlo jednostavno zloupotrijebiti. Jedan tip napada presretanja je *man-in-the-middle-attack* (MITM). To je vrsta napada prisluškivanjem gdje se zlonamjerni agent ubacuje u komunikacijsku sesiju između ljudi ili sustava lažno predstavljajući obje strane i dobiva pristup povjerljivim podacima koji se razmjenjuju tim komunikacijskim kanalom. Obje žrtve obično nisu svjesne takve povrede jer iz njihove perspektive komunikacija se odvija normalno kao i prije samog napada [4]. Slika 2.5. prikazuje MITM napad.



Slika 2.5. *Man-in-the-middle* (MITM)

Veliki broj kibernetičkih napada uključuje **krađu podataka**. Napadači koji pokušavaju doći do žrtvinih podataka često pokušavaju monetizirati te podatke. Neki od tih podataka su:

- Podaci koji se mogu koristiti za krađu identiteta ili prodati kradljivcima identiteta
- Kompromitirajuće fotografije ili zdravstveni podaci koji se mogu prodati ili koristiti kao dio procesa ucjenjivanja
- Informacije koje su ukradene i zatim izbrisane s korisnikovog uređaja koje se mogu poslije nuditi kao otkup za korisnika
- Popisi lozinki koje se mogu koristiti za probijanje drugih sustava
- Povjerljive informacije o stvarima vezanim uz posao koje se mogu koristiti za nezakonito trgovanje dionicama na temelju povlaštenih informacija
- Informacije o nadolazećim planovima putovanja koje se mogu koristiti za planiranje pljački

Ljudi, poduzeća, neprofitne organizacije te vladina tijela, svi su podložni krađi podataka. Razlozi za krađu podataka od poduzeća i organizacija mogu biti razni, neki od njih su [2]:

- Trgovanje dionicama: Imati pristup financijskim podacima, te unaprijed znati kakav će kvartal poduzeće imati omogućuje napadaču da ostvari znatan profit na tržištu dionica

- Trgovina podataka konkurentima: Krađa dokumenata koje sadrže informacije kao što su poslovni planovi te informacije o nadolazećim projektima i ostalih dokumenata koje mogu konkurentima biti korisni
- Procurivanje podataka medijima
- Procurivanje privatnošću reguliranih podataka
- Preuzimanje zaposlenika: Ukoliko napadač dospije do podataka zaposlenika, ti podaci mogu biti vrijedni konkurentima koji traže zaposlenike sličnih profila
- Krađa i korištenje intelektualne imovine

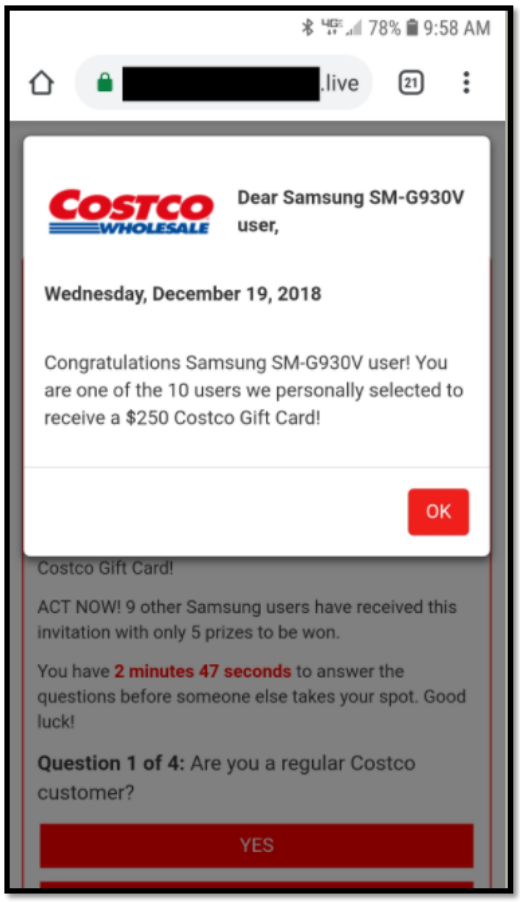
Zlonamjerni softver (engl. *Malware*) je naziv sa softver koji namjerno prouzrokuje štetu korisnicima koji često toga nisu ni svjesni. Pod zlonamjeran softver se podrazumijevaju virusi, crvi (engl. *Worms*), trojanci (engl. *Trojans*), *ransomware*, *scareware*, *spyware*, rudari kriptovaluta, *adware* i ostali programi čija je namjena iskoristiti računalne resurse u zlonamjerne svrhe [2]. Od svih navedenih bitno je izdvojiti ransomware napade, koji je najčešći i najuspješniji kibernetički napad zlonamjernim softverom. Prema provedenom istraživanju [7], čak 85% pružatelja upravljanih usluga u 2019. godini (engl. *Managed service providers*) su prijavili ransomware kao najčešću prijetnju njihovim malim i srednjim klijentskim poduzećima. To je vrsta napada gdje zlonamjerni softver enkriptira korisnikove podatke koristeći enkripcijski algoritam. Ti isti podaci mogu biti otključani samo koristeći dekripcijski ključ koji je u posjedu samog napadača. Nakon enkripcije podataka, napadač traži otkupninu (engl. *Ransom*) od korisnika, te zauzvrat korisniku predaje dekripcijski ključ [4]. Na slici 2.6. se nalazi primjer *ransomware* softvera.

Slika 2.6 Primjer *ransomware* softvera (https://sensorstechforum.com/wp-content/uploads/2021/02/nocry-ransomware-pop-up-ransom-message-stf.png)

Različite vrste napada iskorištavaju ranjivosti poslužitelja, a stalno se otkrivaju nove ranjivosti, zbog čega je bitno kontinuirano održavati sigurnost poslužitelja. Jedan takav oblik napada je **napad zatrovanim web servisom** (engl. *Poisoned Web Service Attacks*) ili **napad zatrovanom web stranicom**. U ovoj vrsti napada, napadač hakira web poslužitelj i na njega ubacuje kod koji ga navodi da napadne korisnike kada pristupe stranici ili skupu stranica koje poslužitelj poslužuje. Međutim, nije nužno da haker probije sustav kako bi oštetio web stranicu, a potom i korisnika. Na primjer, ako web-mjesto koje dopušta komentare korisnika nema odgovarajuće sigurnosne mjere, može omogućiti zlonamjernom korisniku umetanje raznih naredbi unutar komentara. Ove naredbe, ako su vješto izrađene, korisnički preglednici mogu izvršiti kad god učitaju stranicu koja sadrži takav komentar. Naredbom za pokretanje skripte na web stranici hakera, zlonamjerni pojedinac može dobiti vjerodajnice za autentifikaciju korisnika na legitimnoj stranici. Takav se napad obično naziva *cross-site scripting* [2]. Kao i kod web poslužitelja, mnoge različite vrste napada iskorištavaju ranjivosti u mrežnoj infrastrukturi, a stalno se otkrivaju nove slabosti. Takvi se napadi mogu svrstati pod napade **trovanja mrežne infrastrukture** (engl. *Network Infrastructure Poisoning*) Na primjer, kriminalci mogu iskoristiti razne slabosti kako bi dodali neispravne podatke sustava naziva domene (DNS) u DNS poslužitelj. DNS je direktorij na Internetu koji prevodi čovjeku čitljive adrese u njihove numeričke računalno upotrebljive ekvivalente (IP adrese). Na primjer, ako se upiše https://msn.com u svoj web preglednik, DNS usmjerava vezu na IP adresu 204.79.197.219. Umetanjem netočnih informacija u DNS tablice, kriminalac može uzrokovati da DNS poslužitelj vrati netočnu IP adresu na korisničko računalo [2]. Ova vrsta napada poznata je kao DNS *poisoning* ili *pharming*. Trovanje predmemorije DNS-a, također poznato kao lažiranje DNS-a, je napad koji iskorištava ranjivosti u DNS sustavu. Ovaj vrsta napada prevari DNS poslužitelj da povjeruje da je primio legitimne informacije i preusmjerava internetski promet s legitimnih poslužitelja na lažne. Tijekom pretvorbe web adresa u numeričke IP adrese, stvarnu IP adresu zamjenjuje lažnom.

Kao rezultat trovanja DNS-a, korisnici se usmjeravaju na pogrešne web stranice. Na primjer, ako korisnik unese "msn.com" u svoj web preglednik, može nesvjesno učitati web stranicu koju je odabrao haker. Budući da korisnici vjeruju da je domena koju su unijeli ispravna, možda neće shvatiti da se nalaze na lažnoj stranici. U ovom napadu napadač zamjenjuje IP adresu ciljane stranice na DNS poslužitelju lažnim IP adresama [4]. Dvije uobičajene tehnike koje napadači koriste za kompromitiranje sustava i krađu osjetljivih informacija su **zlonamjerno oglašavanje** (engl. *Malvertising*) i kompromitiranje legitimnih web stranica. Zlonamjerno oglašavanje uključuje skrivanje zlonamjernog koda unutar internetskih oglasa, čime se zaraze sustavi korisnika

kada kliknu na zaražene oglase. To može dovesti do oštećenja sustava i gubitka osjetljivih podataka. S druge strane, s ugroženim legitimnim web stranicama, napadači stvaraju zlonamjerne web stranice i u njih ugrađuju zlonamjerni softver [4]. Posjetitelji koji nisu svjesni opasnosti i koji nenamjerno pristupaju ovim web stranicama imaju svoje sustave zaražene ugrađenim zlonamjernim softverom. Obje tehnike iskorištavaju povjerenje korisnika u internetski sadržaj, zbog čega je ključno biti oprezan prilikom surfanja internetom. Primjer zlonamjernog oglašavanje je prikazan na slici 2.7.



Slika 2.7. Primjer zlonamjernog oglašavanja (https://sectigostore.com/blog/wp-content/uploads/2020/09/image-5.png)

Osiguravanje ispravnog održavanja računalnih sustava zadatak je od velike važnosti i ne smije se podcijeniti. Prodavači softvera često objavljuju ažuriranja, i dok mnoga od tih ažuriranja mogu utjecati na druge programe koji se izvode na računalu, određene softverske zakrpe su apsolutno ključne i moraju se instalirati što je prije moguće. To je zato što ukoliko se te zakrpe ne implementiraju, zlonamjerni pojedinac može iskoristiti sigurnosne ranjivosti. Takvi napadi se

mogu svrstati pod napade **iskorištavanja poteškoća u održavanju** (engl. *Exploiting Maintenance Difficulties*). S obzirom na subjektivnu perspektivu, može se smatrati da je svaki napad koji zahtijeva značajna ulaganja u istraživanje i razvoj kako bi se uspješno izveo, napredan. Naravno, definicija "značajnih ulaganja" također je subjektivna. U nekim slučajevima, troškovi istraživanja i razvoja su toliko visoki, a napadi toliko sofisticirani da postoji gotovo univerzalni dogovor da se radi o naprednom napadu. Neki stručnjaci smatraju da je svaki napad koji koristi ranjivost koja je tek otkrivena (zero-day) napredan, dok drugi to osporavaju. **Napredni napadi** (engl. *Advanced Attacks*) mogu biti oportunistički, ciljani ili kombinacija.

Oportunistički napadi imaju cilj pogoditi što veći broj potencijalnih žrtava s nadom da će pronaći ranjive sustave koje mogu iskoristiti. Napadač nema unaprijed definiran popis žrtava, već cilja na svaki dostupan sustav koji je podložan specifičnom napadu koji je pokrenut. S druge strane, ciljani napadi fokusiraju se na određene pojedince ili organizacije. Uključuju korištenje niza tehnika napada, uporno isprobavajući različite metode dok jedna ne uspije probiti ciljane sustave. Nakon što se uspije probiti, mogu se pokrenuti dodatni napadi kako bi se kretali unutar sustava cilja [2].

2.4. Rukovanje rizicima sigurnosnih prijetnji

Organizacije mogu reagirati na rizik na više načina. Prema NIST 800-39 publikaciji [7], to uključuje sljedeće:

- **Prihvaćanje rizika** (engl. *Risk acceptance*)
- **Izbjegavanje rizika** (engl. *Risk avoidance*)
- **Ublažavanje rizika** (engl. *Risk mitigation*)
- **Podjelu rizika** (engl. *Risk sharing*)
- **Prijenos rizika** (engl. *Risk transfer*)
- Kombinaciju gore navedenih pristupa

Prihvaćanje rizika je odgovarajući pristup kada utvrđeni rizik ulazi u organizacijski prag podnošljivosti rizika. Organizacije mogu prihvatiti rizike koji se smatraju niskim, umjerenim ili visokim, ovisno o konkretnim situacijama ili uvjetima [7]. Na primjer, organizacije čiji se podatkovni centri nalaze na području Qatar-a mogu odlučiti prihvatiti rizik od poplava ili sličnih prirodnih nepogoda, uzimajući u obzir poznatu vjerojatnost prirodnih nepogoda u toj regiji i ranjivost podatkovnih centara na oštećenje tih prirodnih nepogoda. Organizacije prihvaćaju činjenicu da su prirodne nepogode moguće, ali zbog rijetkosti većih prirodnih nepogoda u toj regiji

zemlje, smatraju da nije isplativo detaljno se baviti takvim rizikom – odnosno, organizacije su zaključile da je rizik povezan s prirodnim nepogodama nizak. S druge strane, organizacije mogu prihvatiti značajno veći rizik (u umjerenom/visokom rasponu) zbog važnih misija, poslovnih ili operativnih potreba. Na primjer, u slučaju nekakvog napada ili sumnji na teroristički čin, savezne agencije mogu odlučiti dijeliti vrlo osjetljive informacije s prvim odazivnicima koji obično nemaju pristup takvim informacijama, ali to je nužno kako bi se spriječila katastrofa. U takvim scenarijima, naglašena je hitnost situacije, što ima prednost nad rizikom kompromitiranja povjerljivosti informacija.

Utvrđivanje prihvatljive razine rizika i vrsta rizika koje je moguće prihvatiti obično uključuje razmatranje organizacijskih prioriteta i postizanje kompromisa između [7]:

- Trenutačnih potreba misija/poslovanja i potencijalnih dugoročnih posljedica za misije/poslovanje
- Interesa organizacije i potencijalnih utjecaja na pojedince, druge organizacije i cjelokupnu naciju.

Izbjegavanje rizika može biti odgovarajući odgovor na rizik kada utvrđeni rizik premašuje organizacijski prag podnošljivosti rizika. Organizacije mogu provoditi određene vrste aktivnosti ili koristiti određene informacijske tehnologije koje rezultiraju rizicima koji su neprihvatljivi. U takvim situacijama, izbjegavanje rizika podrazumijeva poduzimanje određenih mjera kako bi se eliminirale aktivnosti ili tehnologije koje predstavljaju temelj rizika, ili prilagodba i premještanje tih aktivnosti ili tehnologija unutar organizacijskih misija i poslovnih procesa kako bi se izbjegao potencijal neprihvatljivog rizika [7].

Na primjer, organizacije koje pohranjuju podatke svojih klijenata unutar nekakvog okruženja i pri određenim uvjetima mogu utvrditi putem procjene rizika da je pohrana određenih podataka u postojećem okruženju i uvjetima neprihvatljivog rizika. Također, organizacije mogu zaključiti da nije izvedivo implementirati učinkovite mjere zaštite i protumjere u danim okolnostima. Stoga se organizacije odlučuju izbjeći rizik ograničavajući pohranu podataka svojih klijenata tako što ih uopće neće pohranjivati ili će pohranjivati samo određene podatke (npr. podatke koji ne podliježu GDPR-u)

Ublažavanje rizika, također poznato kao smanjenje rizika, odgovarajući je odgovor za dio rizika koji se ne može prihvatiti, izbjeći, dijeliti ili prenijeti. Alternativne strategije za ublažavanje rizika ovise o dva ključna čimbenika [7]:

- razini odgovornosti za upravljanje rizikom i odlučivanja koja su dodijeljena ili prenesena organizacijskim dužnosnicima unutar uspostavljenih struktura upravljanja;
- strategiji upravljanja rizikom organizacije i povezanim planovima odgovora na rizik.

Primjer potencijalnog rizika koji zahtijeva ublažavanje može se prikazati kada zaposlenici preuzmu zlonamjernu datoteku ili kliknu na link koji su dobili u *phishing* poruci. Moguće mjere ublažavanja rizika uključuju, na primjer, organizacijske politike gdje zaposlenici moraju proći obvezni trening na tu tematiku kako bi znali prepoznati zlonamjerne poruke ili linkove. Ujedno je moguće implementirati, na razini organizacije, tehničke mjere kao što je sigurnosna filtracija *e-mail*-ova gdje se svaka poruka koja je poslana na službeni *e-mail* sandučić, pomoću softverskih alata, automatski pregledava sadržava ili zlonamjeran sadržaj.

Dijeljenje rizika ili **prijenos rizika** je prikladan odgovor na rizik kada organizacije žele i imaju sredstva za prebacivanje odgovornosti i odgovornosti za rizik na druge organizacije. Prijenos rizika podrazumijeva prebacivanje potpune odgovornosti ili odgovornosti za rizik s jedne organizacije na drugu organizaciju (npr. korištenjem osiguranja za prijenos rizika određenih organizacija na osiguravajuće društvo). Dijeljenje rizika podrazumijeva prebacivanje dijela odgovornosti ili odgovornosti za rizik na druge organizacije (obično organizacije koje su kvalificiranije za rješavanje rizika). Važno je napomenuti da prijenos rizika ne smanjuje vjerojatnost štetnih događaja niti posljedice u smislu štete na operacijama i imovini organizacije, pojedincima, drugim organizacijama ili državi. Dijeljenje rizika može biti dijeljenje odgovornosti ili dijeljenje odgovornosti za druge prikladne mjere odgovora na rizik, kao što je ublažavanje. Stoga, koncept prijenosa rizika manje je primjenjiv u javnom sektoru (npr. državne, savezne i lokalne vlade) nego u privatnom sektoru, jer se odgovornost organizacija u javnom sektoru obično utvrđuje zakonodavstvom ili politikama. Stoga, samoinicijativni prijenosi rizika od strane organizacija javnog sektora (kao što je kupovina osiguranja) obično nisu mogući. Dijeljenje rizika često se događa kada organizacije zaključe da rješavanje rizika zahtijeva stručnost ili resurse koje su bolje osigurane od strane drugih organizacija [7]. Na primjer, ukoliko je organizacija zaključila da nema adkvatne resurse te stručnost za sigurnosno pohranjivanje osjetljivih podataka, u tom slučaju odlučuje surađivati sa drugom organizacijom koja je kvalificiranija za sigurnosnu pohranu osjetljivih podataka, gdje su uvjeti i odgovornosti formalno dogovorene između dvije organizacije.

3. UTJECAJ KIBERNETIČKOG NAPADA NA ORGANIZACIJE I PODUZEĆA

Prije nego što počnemo sa rasčlanivanjem posljedica kibernetičkih incidenata pretrpljenih od strane organizacija i poduzeća, potrebno je prikazati trenutno globalno stanje kibernetičkog svijeta te prognozu posljedica kibernetičkih incidenata u slijedećim godinama.

3.1. Trenutno globalno stanje

Prema istraživanju [8] iz 2022. godine, provedeno od strane *Cybersecurity Ventures* i *Esentire,* kibernetički kriminal će do kraja 2023. godine koštati svijet čak 8 trilijuna dolara. Nadalje, tekst raspravlja o snažnom utjecaju kibernetičkog kriminala na globalnoj razini, ističući zabrinjavajući rast i razorne posljedice. Kao što je već spomenuto, predviđa se da će godišnji troškovi kibernetičkog kriminala doseći neviđenih 8 trilijuna dolara u 2023. godini, nadmašujući sve dosadašnje transfera ekonomske imovine u povijesti. Ovaj eksponencijalni rast predstavlja ozbiljne rizike za inovacije, investicije i opću ekonomsku stabilnost.

Šteta koju uzrokuje kibernetički kriminal očekuje se da će naglo porasti, s procijenjenim troškovima koje će doseći iznoseći zapanjujućih 10,5 trilijuna dolara do 2025. godine. To uključuje porast napada *ransomware*-a koji su se rapidno umnožili tijekom godina, nanoseći značajne financijske gubitke žrtvama. Do 2031. godine, samo *ransomware* se predviđa da će koštati oko 265 milijardi dolara godišnje, s napadima koji se događaju svake dvije sekunde.

Kriptokriminal je još jedna rastuća prijetnja, potaknuta eksponencijalnim rastom decentraliziranih financija. Kriminalci iskorištavaju ranjivosti u kriptovalutnim sustavima, što rezultira gubicima od otprilike 30 milijardi dolara u 2025. godini, gotovo dvostruko više nego što je zabilježeno u 2021. godini. Napadi na kripto mostove i prijevare usmjerene prema vlasnicima kriptovaluta pridonose ovom rastućem problemu.

Kibernetička površina napada znatno se proširila zbog porasta količine podataka i internetskog povezivanja. Gotovo svaki sektor suočava se s rizicima, posebno kritična infrastruktura, bolnice, javne službe, banke, telekomunikacijske tvrtke i tehnološke tvrtke. Rješavanje kibernetičkih rizika

postalo je prioritet za organizacije, a uprave za kibernetičku otpornost sve više traže pristupe zasnovane na riziku kako bi ojačale mjere kibernetičke sigurnosti.

Nedostatak talenata u kibernetičkoj industriji dodatno otežava izazove u suočavanju s kibernetičkim prijetnjama. Postoji nevjerojatnih 3,5 milijuna otvorenih radnih mjesta u području kibernetičke sigurnosti diljem svijeta, s više od 700.000 otvorenih radnih mjesta samo u Sjedinjenim Državama. Žene ostaju nedovoljno zastupljene u ovom području, čineći samo 25% ukupne svjetske radne snage u području kibernetičke sigurnosti, a taj se postotak predviđa da će doseći 30% do 2025. godine.

Usred ovih rastućih izazova, organizacije se potiču da prioritetno poboljšaju svoje obrane protiv evoluirajućih kibernetičkih prijetnji. S troškovima kibernetičkog kriminala u porastu i kibernetičkim krajolikom koji postaje sve složeniji, proaktivne mjere kibernetičke sigurnosti i suradnja s ekspertima ključne su za zaštitu poslovanja, vlada i pojedinaca od mogućih razaranja.

3.2. Analiza incidenata

U ovom poglavlju su obrađena tri slučaja gdje je organizacija bila meta uspješnog kibernetičkog napada. Svaki incident je obrađen na način da se u početku poduzeće predstavi te se da opis njihovih poslovnih aktivnosti. Zatim slijedi objašnjenje kako je došlo do kibernetičkog napada, njegove posljedice te na kraju zaključak.

3.2.1. Trgovački lanac Target

Target, veliki američki trgovac zajedno s Walmartom, suočio se s kršenjem podataka 19. prosinca 2013. Povreda je uključivala više od 40 milijuna podataka koji otkrivaju identitet potrošača, uključujući podatke o kreditnim i debitnim karticama koje su korištene u američkim trgovinama. Osim toga, tvrtka Target je u siječnju 2014. objavila da je ugroženo dodatnih 70 milijuna osobnih podataka korisnika, poput imena, telefonskih brojeva, adresa i e-pošte, što je utjecalo na oko 10% debitnih i kreditnih kartica sa sjedištem u SAD-u.

Prema [9], hakeri su se infiltrirali u Targetovu mrežu prodajnih mjesta između 15. i 27. studenog 2013. koristeći zlonamjerni softver "BlackPOS" podrijetlom iz Rusije. Zlonamjerni softver, alat za „struganje“ memorije, ciljao je terminale na prodajnim mjestima kako bi dobio osjetljive podatke o karticama pohranjene u RAM-u (engl. *Random-access memory*) ,kojeg su kasnije neovlašteno integrirali na jedan od Targetovih web poslužitelja.

Unatoč provedbi sigurnosnih mjera poput segmentacije mreže, vatrozida i paketa za otkrivanje zlonamjernog softvera te pridržavanju „Standarda sigurnosti podataka industrije kartičnog plaćanja" (PCI-DSS), napad je potekao od jednog Targetovog dobavljača, Fazio Mechanical Services. Incident je rezultat jednostavne *phishing* e-pošte koja je pomoću koje su pridobiveni korisnički kodovi i lozinke od zaposlenika tvrtke Fazio Mechanical Services, omogućujući napadačima daljinski pristup Targetovoj mreži.

Kako bi riješila sumnjive aktivnosti uzrokovane neovlaštenim pristupom, Tvrtka Target je uložila 1.6 milijuna dolara u FireEye sustav. Sustav je koristio virtualne komore kako bi namamio hakere i otkrio potencijalne incidente prije nego što su mogli prodrijeti u mrežu. Međutim, lokalni sigurnosni tim zanemario je eskalaciju upozorenja primljenih od 30. studenog 2013., što bi potencijalno spriječilo incident. Tvrtka Target je također odlučila ne aktivirati značajku sustava koja otkriva i uklonanja zlonamjerni ili neovlašteni softver, navodeći probleme s povjerenjem u novi sustav. Osim toga, zanemarena je sumnjiva aktivnost koju je otkrio jedan od Targetovih antivirusnih sustava na poslužitelju. Tvrtka Target je postala svjesna prodora tek kada su ih obavijestili predstavnici američkog Ministarstva pravosuđa.

Hakeri su uspjeli prodati ukradene kreditne kartice na *dark web*-u, uzrokujući ozbiljne posljedice za poslovanje Target-a. Posljedice su uključivale štetu na račun njihovog ugleda i tržišne vrijednosti. Unatoč pokušajima da se incident prikrije, tvrtka Target je, za incident, morala javno priznati 19. prosinca 2013. Tvrtka se suočila s kritikama zbog ignoriranja upozorenja koja su mogla spriječiti incident i zbog njihove nevoljkosti da otkriju incident javnosti i učinkovito riješe zabrinutost kupaca.

Negativna percepcija kupaca odrazila se na financijske rezultate Target-a, pri čemu je dobit pala za 46%, a prihodi za 5,3%, djelomično zbog straha potrošača. Ukupni nastali troškovi iznosili su 252 milijuna dolara, uključujući troškove kibernetičkog osiguranja i zatvaranje 133 trgovine u Kanadi. Tvrtka Target je također morala platiti do 67 milijuna dolara izdavateljima kreditnih kartica na temelju nagodbe s Visa-om. Banke poput JP Morgan-Chase morale su ponovno izdati kreditne kartice i nametnuti ograničenja transakcija, tražeći povrat troškova povezanih s

rješavanjem incidenta. Kao odgovor na krizu, tvrtka Target je prošla kroz organizacijske promjene, a šef informativnog odjela (engl. CIO) podnio je ostavku te su dvije ključne eksterne pozicije stvorene za ulogu informacijske sigurnosti i usklađenosti. Povreda podataka dovela je do promjene u strukturi vodstva tvrtke. Kako bi se riješila zabrinutost kupaca i poboljšale sigurnosne prakse, Tvrtka Target je pokrenula kampanju za odnose s javnošću, osiguravajući kupcima tehnološka poboljšanja i nudeći pretplate za praćenje kredita pogođenim pojedincima. Prioritet im je bila implementacija sustava plaćanja *chip-and-PIN* za poboljšanu sigurnost. Unatoč značajnim posljedicama, prema podacima iz 2020. godine, Tvrtka Target je i dalje glavni konkurent Walmartu.

Target je prepoznao rizik neosiguranih sustava preko treće strane i odgovorio na kršenje podataka onemogućavanjem računa dobavljača i rekonfiguriranjem organizacijske strukture s novim izvršnim pozicijama. Usredotočili su se na oporavak povjernja kupaca putem kampanja za odnose s javnošću i besplatnih usluga praćenja kredita. Tehnološka poboljšanja uključivala su implementaciju dvofaktorske autentifikacije, nove sigurnije sustave plaćanja te poboljšano praćenje mrežnog prometa. Dok inovacijske promjene nisu bile ključne, unaprjeđenje odjela za ljudske resurse uključivale su zapošljavanje novog vodstva i uspostavu jače radne snage za zaštitu podataka.

3.2.2. Osiguravajuća kuća Anthem

Anthem, veliko zdravstveno osiguravajuće društvo sa sjedištem u Indianapolisu u Indiani, suočilo se s povredom podataka u veljači 2015. Napadači su dobili neovlašteni pristup sustavu matične tvrtke, ugrožavajući osobne podatke gotovo 80 milijuna Amerikanaca, uključujući brojeve socijalnog osiguranja, medicinske iskaznice, datum rođenja, adrese, podatke o zaposlenju i prihodima. Srećom, nisu ukradene financijske ili zdrastvene informacije. U početku opisan kao "sofisticiran", proces prodora u sustav je vjerojatno bio manje kompliciran nego što se u početku tvrdilo. Otkriveno je kada je administrator baze podataka primijetio sumnjive aktivnosti sa svojim vjerodajnicama tijekom slanja jednog upita. Anthem-ova infrastruktura za skladištenje podataka, TeraData, imala je sigurnosne kontrole, ali neke datoteke nisu bile šifrirane. Kompromitiranje administratorskog računa s eskaliranim ovlastima učinilo je šifriranje nevažnim.

Prema [9] istraga je sugerirala umiješanost kineske skupine za kibernetičku špijunažu pod pokroviteljstvom države pod nazivom "*Deep Panda*". Moguće da je napad uključivao krađu identiteta ili zlonamjerni softver za dohvaćanje vjerodajnica za prijavu korisnika. Sigurnosna tvrtka Mandiant, angažirana za istragu, istaknula je da tvrtka Anthem nije poduzela dovoljno

koraka za zaštitu svojih podataka, uključujući upotrebu dvofaktorske autentifikacije i česte promjene lozinke, zajedno s neadekvatnim praćenjem korištenja i eksfiltracije podataka.

Iako incident tvrtke Anthem nije ugrozio osobne, zdravstvene ili financijske informacije, izloženost brojeva socijalnog osiguranja (SSN) i osobnih identifikacijskih podataka (PII) imala je značajne implikacije, potencijalno štetići i zaposlenicima i klijentima tvrtke Anthem. Zbog toga se tvrtka Anthem suočila s više tužbi građana, što je dovelo do sporazuma o nagodbi vrijednog 115 milijuna dolara kako bi se tužiteljima nadoknadila naknada. Sporazumom se također zahtijevalo da Anthem ulaže u financiranje informacijske sigurnosti i provede posebne promjene kako bi poboljšala svoje sustave sigurnosti podataka, kao što su šifriranje i strože kontrole pristupa. Iako je tvrtka Anthem odbila priznati bilo kakve prijestupe, savezni sudac naredio je otkrivanje njihovih sigurnosnih revizija prije i nakon kršenja. Tvrtka Anthem se obvezala na održavanje i poboljšanje praksi informacijske sigurnosti kao dio nagodbe. Napravili su razne sigurnosne promjene, uključujući resetiranje lozinki za suradnike i izvođače, izdavanje novih ID-ova i lozinki za privilegirane korisnike, implementaciju troslojnog modela provjere autentičnosti s lozinkama ograničenog trajanja i proširenje mogućnosti sigurnosnog zapisivanja i nadzora. Tvrtka Anthem je također naglasila predanost šifriranju određenih informacija. Kako bi ublažila utjecaj incidenta, tvrtka Anthem je ponudila besplatne usluge izvješćivanja o kreditima i zaštite identiteta pogođenima, pod nadzorom administracije treće strane.

Tvrtka Anthem prepoznala je potrebu za ažuriranom strategijom kibernetičke sigurnosti i imala za cilj postati usklađena s HIPAA-om. Surađivali su s administracijom treće strane kako bi zaštitili podatke kupaca i uspostavili trogodišnji plan zaštite kao dio svoje strategije kibernetičke sigurnosti. Oporavak štete učinjene klijentima bio je prioritet kroz kompenzaciju s besplatnim uslugama izvješćivanja o kreditima i popravka identiteta, usredotočujući se na poboljšanje njihovih marketinških mogućnosti. Anthem je također poboljšao tehnološku sigurnost šifriranjem kritičnih podataka i poboljšanjem pravila kontrole pristupa i lozinki, istovremeno proširujući mogućnosti sigurnosnog zapisivanja i praćenja. Djelovanje odjela ljudskih resursa smatrane su ključnima za obrazovanje o sigurnosti zaposlenika i poštivanje politike. Nedostatak kvalitetnih odluka odjela za ljudske resurse možda je pridonio njihovom drugom kršenju podataka u 2017. godini.

3.2.3. Equifax

Equifax je 7. rujna 2017. objavio incident kibernetičke sigurnosti koji je pogodio 143 milijuna potrošača, a kasnije je narastao na 148 milijuna pojedinaca, obuhvaćajući gotovo polovicu američke populacije i 56% odraslih Amerikanaca. Equifax se, u to vrijeme smatrala kao jedna od najvećih svjetskih agencija za izvješćivanje potrošača.

Equifax, značajna kreditna agencija, prikuplja, analizira i prodaje podatke o potrošačima kako bi generirala kreditni rejting i detaljna izvješća za svoje klijente. Agencije za kreditni rejting posjeduju ogromne količine osjetljivih osobnih podataka, što ih čini privlačnim metama za kiberkriminalce. Do incidenta je došlo zbog neuspjeha agencije Equifax da uspostavi odgovarajuće sigurnosne mjere za svoje podatke potrošača. Agresivna strategija rasta pod izvršnim direktorom Richard Smith-om dovela je do mnogih akvizicija, složenih IT sustava i povećanih rizika za sigurnost podataka.

Prema [10], u ožujku 2017. objavljena je kritična ranjivost softvera Apache Struts, a unatoč upozorenju Ministarstva domovinske sigurnosti, Equifax nije u potpunosti zakrpao ranjivost na svojim sustavima. Napadači su iskoristili ovu ranjivost i pokrenuli 76-dnevni kibernetički napad počevši od 13. svibnja 2017. Dobili su daljinski pristup nad Equifax mrežom, pristupili nešifriranim vjerodajnicama i izvukli osjetljive podatke iz 48 nepovezanih baza podataka. Equifax nije otkrio eksfiltraciju podataka zato što je uređaj koji nadzire mrežni promet bio neaktivan.

Odgovor Equifaxa uključivao je identificiranje sumnjivih aktivnosti, zatvaranje potrošačkog portala na internetu i angažiranje tvrtke za kibernetičku sigurnost Mandiant za forenzičku istragu. Do kraja kolovoza 2017. godine tvrtka Mandiant je potvrdila opseg kompromitiranih osobnih podataka koji pripadaju potrošačima. Equifax se pripremio obavijestiti javnost, stvarajući web stranicu o incidentu i pozivni centar za podršku pogođenim pojedincima, s ukupno 148 milijuna pogođenih potrošača.

Može se zaključiti da neuspjeh tvrtke Equifax da provede snažne sigurnosne mjere i riješi svoju problematiku složenosti IT sustava je doveo do masovnog kršenja podataka. Nepostojanje

odgovornosti i jasne vizije u upravljanju IT infrastrukturom otežali su provedbu politika, što je omogućilo da ranjivosti i dalje postoje. Equifaxova agresivna strategija rasta i prikupljanje podataka rezultirali su složenim IT okruženjem, pokretajući aplikacije kritične važnosti na zastarjelim sustavima. Tvrtka Equifax je dužnosnike odgovornima za prodor sustava kaznila umirovljenjem, otkazima i odlaskom izvršnog direktora. Da je tvrtka Equifax poduzela ranije mjere za rješavanje sigurnosnih problema, incident se mogao izbjeći.

Incident tvrtke Equifax rezultirao je značajnim financijskim i pravnim posljedicama za tvrtku. U incidentu su razotkriveni osjetljivi osobni podaci milijuna pojedinaca, što je dovelo do različitih financijskih gubitaka i troškova, uključujući troškove kršenja podataka gdje je tvrtka Equifax pretrpila znatne troškove povezane s istragom incidenta, obavještavanjem pogođenih pojedinaca, pružanjem usluga praćenja kredita i upravljanjem posljedicama incidenta. Tvrtka se suočila s brojnim tužbama pogođenih pojedinaca, financijskih institucija i drugih subjekata. Te su tužbe rezultirale znatnim pravnim nagodbama i novčanim isplatama tužiteljima. Regulativna tijela, uključujući Saveznu trgovinsku komisiju SAD-a (FTC), izrekla su tvrtki Equifax novčane kazne jer nije na odgovarajući način zaštitila podatke potrošača. FTC je, prema [11], postigao nagodbu s tvrtkom Equifax 2019. godine, koja je uključivala novčanu kaznu do 700 milijuna dolara. Incident je narušio ugled tvrtke i narušio povjerenje potrošača. Taj se utjecaj proširio na cijenu dionica tvrtke, koja je doživjela značajan pad nakon objave incidenta.

3.3. Posljedice kibernetičkih napada

Iz prošlog potpoglavlja, na primjerima se može primjetiti da se posljedice sigunorsnih i ncidenata mogu podjeliti na nekoliko skupina. Prema [12], one se dijele na:

1. Financijske gubitke
2. Štetu na račun ugleda poduzeća
3. Operativne poremećaje

Financijske posljedice kibernetičkog napada mogu biti pogubne za poduzeća. Neposredni troškovi uključuju napore za sanaciju, kao što su zapošljavanje stručnjaka za kibernetičku sigurnost, oporavak ili zamjenu ugroženih sustava i potencijalna plaćanja otkupnine. Dugoročni troškovi

mogu uključivati izgubljene prihode zbog zastoja poslovanja, pravne naknade i novčane kazne za nepoštivanje propisa o zaštiti podataka. Kibernetički napad može ozbiljno naštetiti ugledu tvrtke, što dovodi do gubitka povjerenja među kupcima, partnerima i investitorima. To može rezultirati gubitkom poslovanja, kao i poteškoćama u privlačenju novih kupaca ili osiguravanju ulaganja. Kibernetički napadi mogu uzrokovati znatne operativne poremećaje, kao što su zastoji sustava ili gubitak kritičnih podataka. Ti poremećaji mogu ometati sposobnost tvrtke da isporučuje proizvode i usluge, utječući na zadovoljstvo kupaca i potencijalno dovodeći do ugovornih kazni.

3.4. Odgovor na incident

Tijekom sigurnosnog incidenta, emocije poput panike, zbunjenosti, stresa, pa čak i ljutnje mogu se pojaviti među IT stručnjacima kada se otkrije prodor ili neovlašteni pristup mreži, sustava ili aplikacije. Takvi incidenti zahtijevaju sastavljenu i urednu reakciju osoba koje upravljaju sigurnosnim incidentima. Prema [13] proces odgovora na incidente sastoji se od četiri faze, koji je, uz manje varijacije kao što su nazivi i broj faza, analogan sa publikacijom NIST SP 800-61 i standardom ISO/IEC 27035-1:2023:

Identifikacija (engl. *Identification*): Prepoznavanje pojave sigurnosnog incidenta prvi je korak u procesu odgovora.

Obuzdavanje (engl. *Containment*): Poduzimanje hitnih mjera kako bi se spriječilo pogoršanje situacije od ključne je važnosti.

Iskorjenjivanje (engl. *Eradication*): Uklanjanje izvora incidenta iz okoline sljedeći je prioritet.

Oporavak (engl. *Recovery*): Obnova normalnog poslovanja i povratak redovnim poslovnim aktivnostima završna je faza.

Proces **identifikacije** sigurnosnih incidenata u kibernetičkoj sigurnosti predstavlja ključni izazov za organizacije. Sigurnosni incidenti se mogu manifestirati na različite načine, učinkovita identifikacija nije samo odgovornost IT timova već svi zaposlenici trebaju biti uključeni u taj proces. Izgradnja kulture povjerenja potiče zaposlenike da brzo prijavljuju potencijalne sigurnosne incidente, što i dalje ostaje jedan od glavnih načina za njihovo otkrivanje. Postoji značajna razlika između "vremena kompromitiranja" (kada napadač dobije pristup) i "vremena otkrivanja" (kada

se incident otkrije). I dok napadači mogu kompromitirati sustave u minutama, otkrivanje može potrajati mjesecima ili čak godinama, pogoršavajući posljedice incidenta. Potreba da se smanji vrijeme otkrivanja ističe važnost faze identifikacije incidenta u procesu odgovora na incidente.

Upravljanje informacijskim tehnologijama (engl. *IT Asset Management*) igra ključnu ulogu u identifikaciji sigurnosnih incidenata. Održavanje točnih zapisa i dokumentacije o tehnološkim resursima pomaže organizacijama prepoznati odstupanja od definirane norme. Uspostava repozitorija podataka o IT resursima omogućuje brže reagiranje na incidente koji uključuju te resurse. Proces identifikacije zahtijeva suradnju s IT administratorima, developerima i drugima kako bi se definiralo što je "normalno" ponašanje za različite resurse. Izvješća o aktualnim sigurnosnim prijetnjama, praćenje prometa na mreži, analiza zapisa, antivirusni softver i nadzor integriteta datoteka ključni su tehnički alati koji se koriste za otkrivanje sigurnosnih incidenata. OSINT (engl. *Open Source Intelligence*) i prijave zaposlenika također doprinose identifikaciji incidenata.

Izgradnja kulture koja potiče otvorenu komunikaciju o potencijalnim incidentima, korištenje tehnoloških alata za praćenje i njihovo razumijevanje su ključne komponente učinkovite identifikacije incidenata.

Faza **obuzdavanja** uključuje poduzimanje mjera kako bi se spriječilo daljnje širenje i eskalacija identificiranog sigurnosnog incidenta. Cilj je spriječiti pogoršanje situacije. Strategije obuzdavanja razlikuju se ovisno o prirodi incidenta. Na primjer, ako se uređaj na mreži zarazi zlonamjernim softverom, izolacija je ključna. Zaraženi uređaj treba odvojiti od mreže kako bi se zaustavilo širenje zlonamjernog softvera. To se može postići fizičkim odvajanjem mrežnih kabela ili onemogućavanjem bežične povezanosti. Slično tome, kada je ugrožena web stranica, cilj je utvrditi kompromitirani dio i izolirati poslužitelja web stranice. To može uključivati privremeno skidanje stranice s mreže.

Da bi se suzbio napad usmjeren uskraćivanjem usluge (DoS), napori mogu uključivati premještanje ciljane usluge na drugu IP adresu ili implementirao filter prometa kako bi se filtrirao napadački promet, a istovremeno omogućio prolazak legitimnog prometa. U slučaju kritične ranjivosti u web aplikaciji, fokus je na sprečavanju iskorištavanja ranjivosti tijekom vremenskog razdoblja između otkrivanja i otklanjanja. To može uključivati upotrebu vatrozida za web aplikacije kako bi se privremeno ublažila ranjivost. Kod incidenta curenja podataka korisnika na internetu, napori za obuzdavanje uključuju pokušaje uklanjanja podataka s interneta i identifikaciju

izvora curenja radi daljnjeg suzbijanja. Kod *phishing* incidenta, kada korisnik nasjedne na *phishing* e-poštu, obuzdavanje uključuje onemogućavanje kompromitiranog računa i pregledavanje zapisa e-pošte kako bi se osiguralo da drugi subjekti nisu bili ciljani ili ugroženi.

U slučajevima otkaza zaposlenika koji nisu završili u prijateljskom odnosu te postoji sumnja da taj zaposlenik želi prouzročiti štetu poduzeću, prioritet je povući fizičke i tehničke podatke za pristup sustavima, virtualnim i fizičkim, kako bi se spriječila šteta tvrtki. Uz napore obuzdavanja, također je bitno upravljati glasinama i dezinformacijama uključivanjem timova za odnose s javnošću kako bi pratili interne i eksterne komunikacijske kanale. U svim ovim slučajevima obuzdavanja, cilj je spriječiti pogoršanje situacije, pružiti vrijeme za daljnju istragu i odgovor te primijeniti različite strategije temeljem specifičnog incidenta kako bi se učinkovito kontrolirale i umanjile njegove posljedice.

Tijekom faze **iskorjenjivanja ili eradikacije** u obradi incidenata, glavni fokus prelazi na rješavanje osnovnog uzroka sigurnosnog incidenta. To može obuhvaćati različite aktivnosti, poput ponovnog formatiranja uređaja zaraženih zlonamjernim softverom, primjene zakrpa (engl. *Patching*) za ispravljanje ranjivosti softvera ili resetiranja kompromitiranih vjerodajnica. Tijekom ove faze postaje očito kako se povezuju dva pojma, odgovor na incident i digitalna forenzika. Digitalna forenzika stavlja naglasak na čuvanje dokaza, što se suprotstavlja cilju iskorjenjivanja - uklanjanju štetnih elemenata. Hitnost da se problem ukloni u što kraćem vremenu često dolazi do izražaja, posebno kada je pogođen ključni poslužitelj ili glavno računalo. Postizanje ravnoteže između brzog rješavanja problema i čuvanja dokaza zahtijeva temeljitu organizaciju i pažljivo rukovanje.

Obuhvat metoda eradikacije ili iskorjenjivanja obuhvaća raznolike strategije. Prema [13] Jedna takva strategija uključuje ponovno oblikovanje kompromitiranih sustava. Ova strategija podrazumijeva temeljito ponovno formatiranje kompromitiranih uređaja kako bi se uništili svi tragovi kompromisa. To je pouzdan pristup koji se često primjenjuje kao odgovor na upozorenja o zlonamjernom softveru. Kada je oporavak podataka nužan, forenzičko akviziranje kompromitiranog uređaja može biti izuzetno korisno, pružajući i oporavak datoteka i bolje razumijevanje kompromisa.

Još jedan pristup je oporavak podataka. U situacijama gdje je narušena cjelovitost podataka, uloga sigurnosnih kopija postaje ključna. Podaci se mogu vratiti na njihovo posljednje valjano stanje nakon što su poduzete mjere za suzbijanje problema. Redovita testiranja ovih sigurnosnih kopija osiguravaju njihovu pouzdanost. Dodatno, obnova kontrole pristupa ključna je strategija.

Rješavanje kompromitiranih vjerodajnica zahtijeva njihovo resetiranje kako bi se spriječila daljnja zloupotreba. Dok je to jednostavno za korisničke račune, postaje složenije za dijeljene ili servisne račune. Suština leži u identifikaciji svih izvora gdje su vjerodajnice pohranjene kako bi se spriječili nepredviđeni prekidi uzrokovani zastarjelim vjerodajnicama.

U fazi **oporavka** postupka odgovora na incident, naglasak se stavlja na vraćanje radnog okruženja u normalno stanje kako bi se poslovne aktivnosti mogle nastaviti. To uključuje različite radnje kao što su vraćanje šifriranih datoteka s sigurnosnih kopija u slučaju napada *ransomware*-om, ponovno uspostavljanje mrežne povezanosti za strojeve koji su bili izolirani i očišćeni te uklanjanje virtualnih zakrpa (engl. *Virtual patching*) nakon što su primijenjene stvarne zakrpe. Osim samog oporavka, ova faza uključuje mjere kako bi se spriječilo ponavljanje sličnih incidenata u budućnosti. Primjerice, ako je nedostatak konfiguracije pravila vatrozida doprinijelo incidentu, osiguravanje njegove primjene postaje obvezno. Također, rješavanje ranjivosti koje su omogućile širenje zlonamjernog softvera, poput neispravne instalacije antivirusnog softvera, dio je procesa obnove.

Ova faza također pruža priliku za timove za odnose s javnošću i komunikaciju da naprave javni izvještaj o incidentu, surađujući s sigurnosnim i pravnim odjelom kako bi pružili točne informacije. Kako se završava proces oporavka, važno je izraziti zahvalnost svima koji su sudjelovali u ovom procesu i potaknuti ih da razmisle o područjima za poboljšanje ili načinima za povećanje učinkovitosti procesa.

Dodatno, prema [14], preporuke za rukovanje sa incidentima su:

- Planirajte koordinaciju incidenta s eksternim stranama prije nego što do incidenta dođe
- Konzultirajte se s pravnim odjelom prije početka bilo kakvih koordinacijskih aktivnosti
- Dijelite informacije o incidentu tijekom trajanja incidenta i odgovora na isti
- Pokušajte automatizirati proces dijeljenja informacija koliko je moguće
- Uravnotežite prednosti dijeljenja informacija s nedostacima dijeljenja osjetljivih informacija.
- Podijelite što više odgovarajućih informacija o incidentu s drugim organizacijama.

Detaljnije, planirajte koordinaciju incidenata s vanjskim stranama prije nego što se incidenti dogode, uključujući entitete poput drugih timova za odgovor na incidente, agencija za provedbu zakona, pružatelja internetskih usluga te korisnika. Takav način pripreme pomaže uspostaviti jasne

uloge za sve uključene strane i komunikaciju koja je ključna u slučaju incidenta. Zatražite pomoć od pravnog odjela prije nego što započnete s aktivnostima koordinacije, budući da mogu postojati pravni ugovori ili drugi sporazumi koji trebaju biti razmotreni prije nego što se započnu razgovori ili druge aktivnosti.

Omogućite neometano dijeljenje informacija o incidentu tijekom njegovog životnog ciklusa te trajanja odgovora na taj incident. Dijeljenje informacija ključan je aspekt omogućavanja učinkovite koordinacije između različitih organizacija te sudionika. Važno je ne odgađati dijeljenje detalja incidenta, a pogotovo je važno ne čekati da se incident privede kraju već podijeliti informacije što je prije moguće. Nastojte automatizirati što je više moguće proces dijeljenja informacija. Ovaj pristup pojednostavljuje koordinaciju među organizacijama i ostalim sudionicima, čineći je efikasnom i učinkovitom. Organizacije bi trebale težiti ravnoteži između automatiziranog dijeljenja informacija uz ljudsku kontrolu nad tokom informacija. Tako da odgovarajuće informacije dođu na odgovarajuće mjesto.

Idealno, organizacije bi trebale dijeliti samo nužne informacije s odgovarajućim stranama. Informacije o poslovnim posljedicama često se dijele unutar timova i koordinacijskih timova, dok se tehničke informacije često dijele unutar svih vrsta timova. Kod djeljenja informacija s organizacijama i poslovnim partnerima, timovi zaduženi za odgovor na incidente trebali bi se usredotočiti na razmjenu tehničkih informacija.

Kod djeljenja informacija sa drugim organizacijama, razmislite o tome koje vrste tehničkih informacija treba ili ne treba dijeliti s različitim stranama. Primjerice, djeljenje informacija kao što je izvor napada ili ostale generalne informacije su sigurne za podijeliti sa ostalim organizacijama, ali mogu postojati sigurnosni i pravni razlozi zašto organizacija ne bi željela otkriti određene pojedinosti o iskorištavanju ranjivosti. Određene informacije mogu teško naštetiti reputaciji organizacije te prouzročiti dodatnu financijsku štetu.

3.5. Prevencija sigurnosnih incidenata

Prevencija velikog broja incidenata ključna je za zaštitu poslovnih procesa organizacije. Neodgovarajuće sigurnosne kontrole mogu dovesti do velikog broja incidenata, što rezultira

sporim i nepotpunim odgovorom na incident što uvećava negativne učinke na poslovanje, uzrokujući dulje vrijeme popravaka te nedostupnost podataka i sustava. U ovom tekstu nisu navedeni specifični savjeti i mjere za jačanje sigurnosti mreže, sustava i aplikacije unutar organizacije iz razloga što se ne može koristiti jedinstveno rješenje za svaku organizaciju već su dane generalne preporuke prema publikaciji NIST SP 800-61. Prema tom dokumentu [14] preporučene prakse za zaštitu mreža, sustava i aplikacija uključuju:

- Procjene rizika
- Sigurnost poslužitelja (glavnih računala):
- Mrežnu sigurnost
- Sprječavanje zlonamjernog softvera
- Osvjećenost korisnika i edukacija

Redovite procjene potencijalnih rizika povezanih sa sustavima i aplikacijama trebale bi utvrditi moguće opasnosti koje proizlaze iz međusobnog djelovanja prijetnji i ranjivosti. Procjene bi trebale obuhvatiti razumijevanje relevantnih prijetnji, čak i onih jedinstvenih za organizaciju. Svaki rizik trebao bi dobiti prioritet, i odgovarajuće mjere, bilo da se radi o ublažavanju, prijenosu ili prihvaćanju rizika, mjere bi se trebale poduzimati dok god se ne postigne razumna ukupna razina rizika. Još jedna prednost provođenja ovih procjena rizika kontinuirano je prepoznavanje ključnih resursa, omogućavajući organizaciji da se usredotoči na praćenje i odabir odgovarajućih mjera za te resurse. Svi poslužitelji trebaju biti prikladno ojačani korištenjem standariziranih konfiguracija. Osim redovitog ažuriranja svakog poslužitelja, poslužitelji se trebaju konfigurirati prema načelu najmanjih prava (engl. *principle of least privilege*) - dodjeljujući korisnicima samo prava potrebna za izvođenje njihovih ovlaštenih zadataka. Poslužitelji trebaju imati mogućnost provjere i bilježenja značajnih događaja povezanih sa sigurnošću. Sigurnost poslužitelja i njihovih konfiguracija potrebno je kontinuirano nadzirati.

Mreži parametar je potrebno konfigurirati tako da negia sve nedopuštene/neovlaštene aktivnosti. Pod tim se podrazumijeva osiguravanje konekcijskih točaka kao što su virtualne privatne mreže te veze namjenjene za spajanje na druge organizacije. Preporučljivo je implementirati softver diljem cijele organizacije koji može prepoznati i zaustaviti zlonamjerni softver. Zaštita od zlonamjernog softvera trebala bi biti postavljena na različitim razinama organizacije: na razini poslužitelja (kao

što su operacijski sustavi poslužitelja i radnih stanica), na razini poslužitelja aplikacija (na primjer, poslužitelji e-pošte) te na razini klijentskih aplikacija. Zaposlenike i ostale korisnike unutar organizacije treba obavijestiti o smjernicama i postupcima koji se odnose na pravilnu uporabu mreža, sustava i aplikacija. Također bi zaposlenicima i svim korisnicima trebale biti prenesene lekcije naučene iz prethodnih incidenata kako bi se uvjerili njihovo djelovanje može utjecati na sigurnost organizacije. Jačanje svijesti korisnika o incidentima trebalo bi smanjiti učestalost istih. Osoblje IT-a trebalo bi proći obuku kako bi mogli održavati mreže, sustave i aplikacije sukladno sigurnosnim standardima organizacije.

3.6. Kibernetička sigurnost u Republici Hrvatskoj

Stanje kibernetičke sigurnosti u Republici Hrvatskoj nije među prvim izborima tema koju ćete pronaći na naslovnim stranicama domaćih portala ili papirnath novina. Istraživanje [15] koje je provedeno u 2022. godini tijekom 6 mjeseci sadrži poprilično detaljnu analizu količine i vrste kibernetičkih napada u Republici Hrvatskoj. Istraživanje je provedeno od strane tvrtke CheckPoint, koja je američko-izraelski multinacionalni pružatelj softverskih proizvoda i kombiniranih hardverskih i softverskih proizvoda za IT sigurnost, uključujući sigurnost mreže, sigurnost krajnjih točaka, sigurnost u oblaku, sigurnost mobilnih uređaja, sigurnost podataka i upravljanje sigurnošću.

Prema rezultatima istraživanja, tijekom šest mjeseci, organizacije u Hrvatskoj su doživjele prosječno 1013 kibernetičkih napada tjedno, što nadmašuje europski prosjek od 839 napada po organizaciji. Prevladavajući zlonamjerni softver (engl. *Malware*) u Hrvatskoj je Emotet, koji je utjecao na 9% organizacija. Uz Emotet, lista najčešćih *malware*-a u Hrvatskoj uključuje tri Infostealer-a, jedan RAT (AgentTesla) i jedan Botnet (Emotet). Bitno je napomenuti da je čak 98% zlonamjernih datoteka u Hrvatskoj dostavljeno putem elektroničke pošte u posljednjih 30 dana. Među različitim vrstama iskorištavanja ranjivosti, najčešći je *Remote code execution* što je vrsta kibernetičkog napada koji se događa kada napadač iskorištava ranjivost u softverskoj aplikaciji ili sustavu kako bi izvršio zlonamjerni kod ili naredbe s udaljene lokacije. To omogućuje napadaču preuzimanje kontrole nad ciljanim sustavom i izvođenje neovlaštenih radnji, potencijalno kompromitirajući sigurnost i integritet sustav te utječe na oko 65% organizacija unutar Republike Hrvatske. U tablici ispod se mogu vidjeti pogođene organizacije prema vrstama malwarea na tjednoj bazi:

Tablica 3.1. Udio određenih vrsta zlonamjernog softvera na tjednoj bazi

	Cryptominer	*Ransomware*	Mobilni softver	*Infostealer*	Zlonamjerni softver namjenjen bankarstvu	*Botnet*
Hrvatski prosjek (%)	5,7	2,6	1,1	4,5	1,8	5,2
Europski prosjek (%)	3,1	1,4	0,9	2,6	2,1	4,2

Iz tablice 3.1. se može vidjeti usporedba sa ostatkom Europe, gdje se može zaključiti da je u prosjeku veća zastupljenost zlonamjernog softvera unutar Hrvatske u usporedbi sa Europskim prosjekom. Nadalje prema tablici 3.2. se može vidjeti koje su industrije unutar Republike Hrvatske najviše pogođene:

Tablica 3.2. Najpogođenije industrije unutar Republike Hrvatske

Indutrija	Broja kibernetičkih napada tjedno
Bankarstvo/financije	1535
Vojne/vladine organizacije	1523
Proizvodnja	374

Prema istraživanju, najpogođenije industrije unutar Republike Hrvatske su bankarski i financijski sektor, vojne i vladine organizacije te sektor proizvodnje. U istraživanju nema detalja o tome radi li se o uspješnim napadima ili o ukupnom broju pokušaja napada (od kojih neki mogu biti uspješni). U tablici 3.3. mogu se vidjeti najčešće vrste iskorištenih ranjivosti unutar Republike Hrvatske u zadnjih 30 dana istraživanja te postotak pogođenih organizacija iskorištavanjem tih ranjivosti unutar Republike Hrvatske:

Tablica 3.3. Najčešće vrste ranjivosti unutar Republike Hrvatske

Vrsta ranjivosti	% pogođenih organizacija u RH
Udaljeno izvođenje koda (engl. *Remote Code Execution*)	66%
Otkrivanje informacija (engl. *Information Disclosure*)	62%
Obilaženje autentikacije (engl. *Authentication Bypass*)	46%
Nemogućnost pružanja usluge (engl. *Denial of Service)*	29%

Vlada Republike Hrvatske je na sjednici održanoj 7. listopada 2015. godine donijela Odluku o donošenju nacionalne strategije kibernetičke sigurnosti i akcijskog plana za provedbu nacionalne strategije kibernetičke sigurnosti. Prema [16], Hrvatska sudjeluje u oblikovanju Strategije za kibernetičku sigurnost koja se usredotočuje na postizanje sistematične i koordinirane provedbe aktivnosti radi poboljšanja razvijenosti zemlje u tom području. Cilj Strategije je povezati različite sektore hrvatskog društva, uključujući državna tijela, pravne osobe s javnim ovlastima i ostale društvene sektore, kako bi se unaprijedilo razumijevanje i suradnja u rješavanju složenih operativnih i tehničkih pitanja vezanih za kibernetičku sigurnost. Dokument ističe važnost kibernetičke sigurnosti za građane, prosperitet društva i potrebu za provedbom zakona uz poštovanje temeljnih ljudskih prava u virtualnom dimenziji društva.

Opći ciljevi Strategije uključuju sistematično primjenjivanje i unaprjeđivanje nacionalnog pravnog okvira kako bi se prilagodilo rastućem kibernetičkom aspektu društva, uz usklađivanje s međunarodnim obvezama i globalnim trendovima kibernetičke sigurnosti. Aktivnosti i mjere provode se kako bi se ojačala sigurnost, otpornost i pouzdanost kibernetičkog prostora, osiguravajući dostupnost, integritet i povjerljivost informacijskih skupina. To se odnosi na pružatelje elektroničkih usluga i korisnike, kao što su pravne osobe i pojedinci povezani s kibernetičkim prostorom. Strategija također ima za cilj uspostaviti učinkovitiji mehanizam za dijeljenje informacija, što zahtijeva usklađene standarde za zaštitu podataka radi jačanja generalne sigurnosti. Nadalje, Strategija ističe podizanje svijesti o sigurnosti među korisnicima kibernetičkog prostora putem diferenciranih pristupa, uvodeći obrazovne elemente u redovne i izvannastavne školske aktivnosti te provodeći inicijative za osvještavanje generalne javnosti. Nastoji potaknuti razvoj usklađenih obrazovnih programa u školama i visokoškolskim institucijama, povezujući akademsku zajednicu, javni sektor i gospodarstvo. Osim toga, Strategija potiče rast e-usluga uspostavljajući povjerenje korisnika putem definiranih minimalnih sigurnosnih zahtjeva. Potiče se istraživanje i razvoj te poticanje suradnje između akademske, ekonomske i javne sfere. Naposljetku, Strategija zagovara sustavan pristup međunarodnoj suradnji, olakšavajući prijenos znanja i koordinirano dijeljenje informacija među različitim nadležnim državnim vlastima, institucijama i sektorima, s krajnjim ciljem unaprjeđenja sposobnosti za uspješno sudjelovanje u globalnom poslovnom okruženju.

4. ANALIZA SIGURNOSNOG STANJA PODUZEĆA

U ovom poglavlju je odrađena analiza rezultata sigurnosnog stanja lokalnog poduzeća. Poglavlje započinje sa opisom korištenih alata te nakon toga je objašnjena primjenjena metodologija. Zatim se navode pretpostavke te na samom kraju je raspisana detaljna analiza sigurnosnog stanja na temelju prikupljenih informacija i dobivenih rezultata.

4.1. Opis alata

Okvir NIST (engl. *National Institute of Standards and Technology*) za poboljšanje kibernetičke sigurnosti kritične infrastrukture, koji se često naziva jednostavno *NIST Cybersecurity Framework* ili *NIST CSF*, široko je prepoznat i korišten skup smjernica i najboljih praksi za upravljanje i poboljšanje kibernetičke sigurnosti unutar organizacija. Prvi put je predstavljen 2014. godine i od tada je postao vrijedan resurs za organizacije svih veličina i sektora za poboljšanje svog položaja u području kibernetičke sigurnosti.

NIST okvir za kibernetičku sigurnost osmišljen je kako bi pomogao organizacijama da bolje razumiju, upravljaju i smanje rizike kibernetičke sigurnosti. Pruža strukturirani pristup procjeni i poboljšanju praksi i otpornosti organizacije u području kibernetičke sigurnosti. Okvir je podijeljen u tri glavne komponente: Jezgra (engl. *Core*), Razine implementacije (engl. *Implementation tiers*) i Profili (engl. *Profiles*).

Osnovne funkcije (engl. *Core functions*):

1. IDENTIFY (ID) : Shvatiti i odrediti prioritete imovine, rizika i ranjivosti.
2. PROTECT (PR) : Provesti zaštitne mjere za zaštitu od prijetnji.
3. DETECT (DE) : Razviti mehanizme za brzo prepoznavanje sigurnosnih događaja.
4. RESPOND (RS) : Uspostaviti procedure za učinkovito reagiranje na sigurnosne incidente i njihovo ublažavanje.
5. RECOVER (RC) : Razviti i implementirati planove za obnovu usluga i oporavak od incidenata.

Svaka funkcija se sastoji od nekoliko kategorija, kojih ukupno ima 23, gdje svaka kategorija ima svoje podkategorije, kojih ukupno ima 108. Okvir koristi informativne izvore i referentne stanarde izdane od strane organizacija koje imaju znatnu ulogu u području istraživanja te unapređenja kibernetičke sigurnosti na svjetskoj razini, kao što su ISO, ISACA, CIS i druge . Na slici 4.1. se nalazi prikaz strukture kategorija i podkategorija NIST okvira, zajedno sa odgovarajućim informativnim referencama, raspoređene po odgovarajućim osnovnim funkcijama.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Slika 4.1. Struktura osnovnih funkcija NIST okvira

Implemetacijske razine predstavljaju zrelost kibernetičke sigurnosti organizacije. Postoje četiri razine:

- Razina 1 : Ograničena osviještenost i razumijevanje rizika za kibernetičku sigurnost.
- Razina 2 : Poboljšavanje osviještenosti i razumijevanja, uz postojanje nekih praksa kibernetičke sigurnosti.
- Razina 3 : Prakse kibernetičke sigurnosti formaliziraju se i dosljedno primjenjuju.
- Razina 4 : Kontinuirano poboljšanje i optimizacija praksi kibernetičke sigurnosti temeljenih na promjeni rizika i prijetnji.

Profili u kontekstu NIST okvira usklađuju funkcije, kategorije i potkategorije s poslovnim zahtjevima organizacije, tolerancijom na rizik i resursima. Profil omogućuje organizacijama da uspostave plan za smanjenje rizika kibernetičke sigurnosti usklađen s organizacijskim ciljevima.

4.2. Pretpostavke

U slučaju kada tvrtka zatraži analizu kibernetičke sigurnosti, ona se provodi sa određenim ciljem, kojeg sama tvrtka treba definirati. Taj cilj može biti usklađivanje poslovanja sa zakonom jer mnoge industrije i jurisdikcije imaju propise i zahtjeve za usklađivanje s kibernetičkom sigurnošću. Tvrtke su često pravno obvezane provoditi procjene kako bi osigurale usklađenost s tim zahtjevima. Nepridržavanje može rezultirati kaznama i pravnim posljedicama. Tvrtke često prikupljaju i pohranjuju osjetljive podatke o korisnicima, poput osobnih podataka i financijskih detalja. Procjene i analize pomažu osigurati da se ti podaci zaštite od krađe, prijevare i neovlaštenog pristupa, što je ključno za očuvanje povjerenja korisnika. Nepravilno rukovanje s takvim podacima može imati pravne posljedice. Uz veliki broj mogućih razloga za provedbu analize kibernetičke sigurnosti, najčešći je upravljanje i smanjenje rizika kibernetičke sigurnosti. Procjene pomažu identificirati ranjivosti i slabosti u sustavima, procesima i politikama organizacije, omogućavajući im da poduzmu korake za smanjenje utjecaja kibernetičkih napada.

U stvarnom slučaju, prije same provedbe procjene ili analize, tvrtka mora jasno definirati ciljeve te opseg procjene, odnosno što će sve ulaziti u procjenu. Zatim je potrebno definirati sve sudionike te njihove uloge i ono najbitnije, alokacija resursa, odnosno definiranje budžeta. Nakon toga slijedi još znatan broj aktivnosti, kako bi se došlo do izrade akcijskog plana temeljen na rezultatima procjene.

Stoga, analiza sigurnosne slike poduzeća (u daljnjem tekstu „Tvrtka“) u ovom radu je odrađena u skladu sa dostupnim resursima te je prilagođena tematici diplomskog rada. Rezultati procjene kibernetičke sigurnosti su temeljeni na informacijama dobivenim od sudionika Tvrtke. Bitno je napomenuti da je identitet Tvrtke te pristup određenim informacijama ograničen iz razloga što otkrivanje tih informacija predstavlja određeni rizik te potencijalno može prouzročiti štetu poslovanju. Rezultati procjene se smatraju informativnima.

4.3. Metodologija

Procjena stanja kibernetičke sigurnosti se vršila prema kategorijama i potkategorijama osnovnih funkcija NIST okvira. Kako bi rezultate procjene bilo moguće kvantificirati, korištene su,

prethodno spomenute, implementacijske razine. Raspon implementacijskih razina se kreće od 1 do 4, gdje veći broj predstavlja višu implementacijsku razinu, odnosno zreliju implementaciju kibernetičke sigurnosti. U idealnom slučaju, gdje poduzeće ima neograničeni budžet, sve bi kategorije imalu maksimalnu vrijednost ciljane implementacijske razine, naravno, u stvarnosti je to rijetko slučaj. U procjeni stanja kibernetičke sigurnosti odrađene u ovom diplomskom radu se nije vršilo priotiziranje jer kao što je već prethodno spomenuto, opseg analize kibernetičke sigurnosti za potrebe diplomskog obuhvaća samo prikupljanje podataka za provedbu analize te samu analizu rezultata. Nakon prikupljanja potrebnih informacija od Tvrtke te na temelju tih informacija svaka subkategorija je „ocijenjena“ ocjenom od 1 do 4. Za svaku subkategoriju se daju dvije ocjene, jedna ocjena predstavlja implementacijsku razinu politike kibernetičke sigurnosti Tvrtke, dok druga ocjena predstavlja implementacijsku razinu politike u praksi Tvrtke. Drugim riječima, vrednuje se politika kibernetičke sigurnosti Tvrtke te implementacija te politike u praksi Tvrtke. Zatim se za svaku kategoriju izračuna prosjek „ocjena“ njezinih subkategorija te ujedno taj prosjek ocjena predstavlja ukupnu ocjenu kategorije, odnosno procjenjenu vrijednost implementacijske razine. Konačni kvantificirani rezultati procjene su prikazani radarskim dijagramom gdje je moguće vizualno usporediti razinu zrelosti politike Tvrtke i zrelost njezine primjene u praksi poslovanja.

Naposljetku, za svaku kategoriju je odrađena detaljna analiza na temelju prikupljenih informacija. Prikupljanje potrebnih podataka i procjena kibernetičke slike je odrađeno tijekom dvije radionice.

Prva radionica pokrila je sljedeća područja:

- IDENTIFY (ID)
- PROTECT (PR)

Druga radionica pokrila je sljedeća područja:

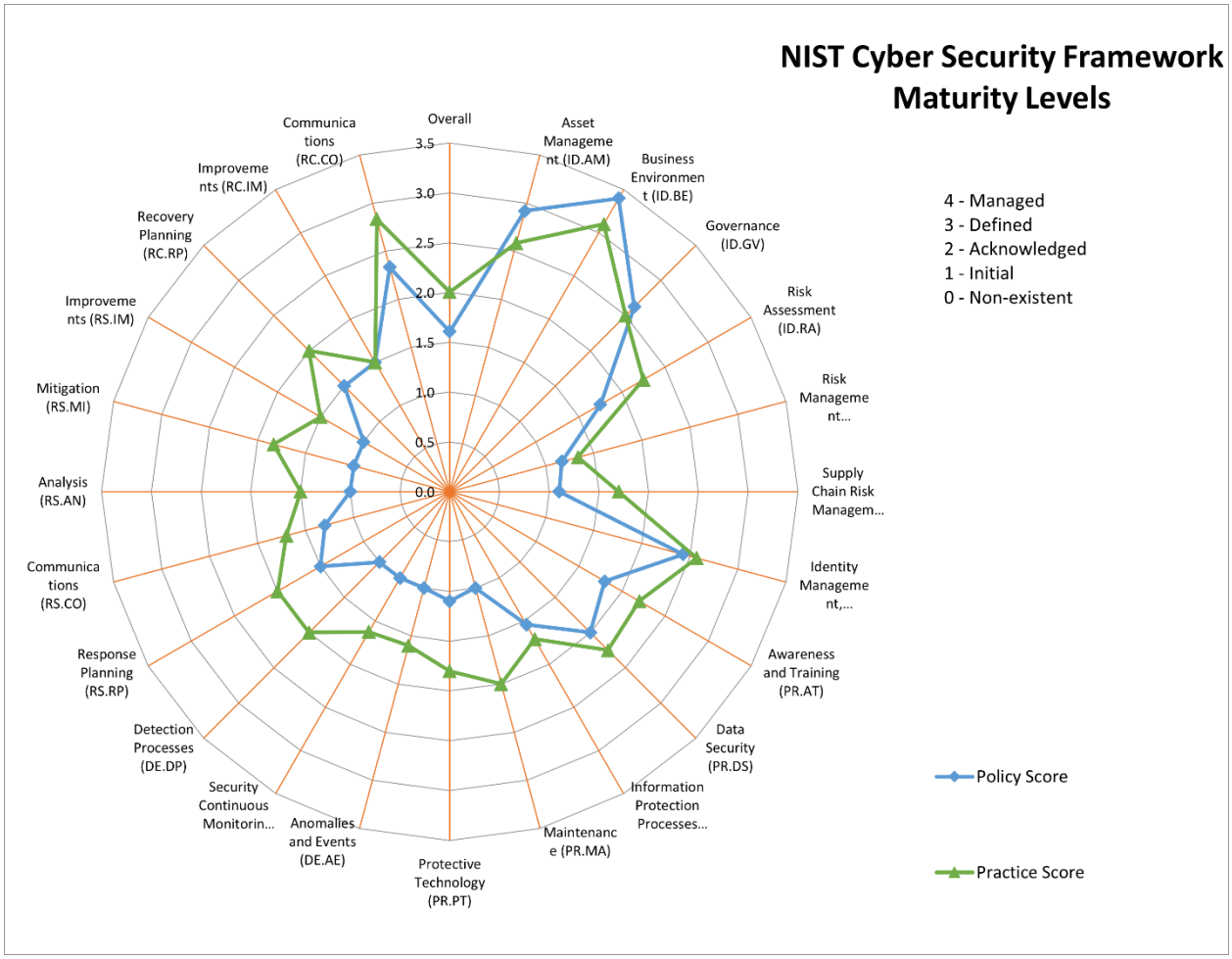
- DETECT (DE)
- RESPOND (RS)
- RECOVER (RC)

Detaljna analiza rezultata je prikazana u slijedećem potpoglavlju te je organizirana po kategorijama NIST okvira.

4.4. Analiza Rezultata

U ovom potpoglavlju je provedena analiza rezultata procjene kibernetičkog stanja Tvrtke. Analiza je organizirana prema osnovnim funkcijama NIST okvira. Kao što je već spomenuto, svaka osnovna funkcija sadrži kategorije koje sadrže svoje potkategorije. Svaka kategorija ima svoju oznaku, oznake kategorija se nalaze na slici 4.1.

Kako bi se rezultati mogli vizualizirati, svaka potkategorija je ocjenjena ocjenom od 1-4, gdje svaka ocjena predstavlja razinu zrelosti, postupak je opisan u potpoglavlju 4.3. Nakon što je svaka potkategorija ocjenjena, rezultati su prikazani na slici 4.2 pomoću radarskog dijagrama.



Slika 4.2. Prikaz rezultata procjene pomoću radarskog dijagrama

Na dijagramu su prikazane 23 kategorije koje pripadaju osnovnim funkcijama NIST okvira te su svakoj kategoriji dodjeljene ukupno dvije ocjene. Plavom linijom je prikazana ocjena politike

Tvrtke, dok je zelenom bojom prikazana ocjena primjene te politike u praksi poslovanja. Analiza procjene kibernetičkog stanja Tvrtke se nalazi u nastavku ovog potpoglavlja.

4.4.1. Upravljanje imovinom, poslovno upravljanje i upravljanje rizikom (ID.AM ID.BE ID.GV ID.RA)

Rezultati procjene upućuju na to da je Tvrtka uspostavila snažne politike za upravljanje imovinom i temeljito održavanje dokumentacije svih sustava, podataka i hardvera. Inventar je uredno održavan, vlasništva i odgovornost su jasno definirana. Uvjeti i kritične funkcionalnosti za pružanje kritičnih usluga su utemeljeni te uspostavljeni za sva operativna stanja kao što je stanje pod napadom, tijekom oporavka ili normalno operativno stanje. Razumijevanje pravnih i regulatornih zahtjeva u konteksu kibernetičke sigurnosti, uključujući obveze privatnosti i građanskih sloboda se provodi internom politikom firme te se u praksi njima adekvatno upravlja. Dok su rizici kibernetičke sigurnosti uključeni u politici upravljanja, pokriveni su vrlo površno. U praksi su implementirani određeni procesi upravljanja rizicima kibernetičke sigurnosti, ali su neredovito ažurirani te neadekvatno dokumentirani. Dok u praksi postoje standarizirani procesi vezani uz kibernetičku sigurnost, većina njih nisu standarizirani, odnosno ne provode se politikom nego se izvode neformalno, prema potrebi. Generalno, procesi i politke upravljanja specifično vezani uz kibernetičku sigurnosti su površinski definirani. Tvrtka bi trebala razmotriti redovite procjene rizika i razvoj plana za upravljanje rizicima kako bi učinkovito umanjila vjerojatnost njihove pojave te ublažio njihov učinak.

4.4.2. Kontrola pristupa, sigurnost podataka i sigurnosne politike (PR.AC PR.AT PR.DS PR.IP PR.MA PR.PT)

Tvrtka ima čvrste politike za fizičku zaštitu, što uključuje kontrolu pristupa, nadzor i sigurnosno osoblje. Postoje definirani proces stvaranja novih identiteta i izdavanje vjerodajnica kojima se uredno upravlja, nad njima vrši se provjera, opozivanje i revidiranje za ovlaštene uređaje, korisnike i procese. U Tvrtki su implementirane stroge sigurnosne fizičke kontrole pristupa te određeni postupci autentifikacije prilikom pristupa fizičkoj imovini kako bi se ona zaštitila. Međutim, većina kontrolnih mjera se odnosi na fizički pristup imovini te autentifikacija je većinom jednofaktorska. Daljinski pristup imovini je kontroliran te postoji digitalni zapis, međutim veliki rizik za kibernetičku sigurnost predstavlja neadekvatna segmentacija i segregacija mreže. Za podatke u mirovanju ili tranzitu ne postoji sigurnosna politika kojom se provodi njihova zaštita, kao što je enkripcija. Međutim, u praksi, osjetljivi podaci u mirovanju se enkriptiraju te se prilikom prijenosa podataka koriste sigurnosni komunikacijski kanali i protokoli. Politika Tvrtke provodi

stvaranje sigurnosnih kopija za kritične podatke te se u praksi uredno primjenjuje. Međutim, ne postji standarizirani proces provjere i testiranje sigurnosnih kopija već se to odrađuje prema potrebi. Politikom se ujedno provodi pravilno uništavanje podataka, poštujući postojeće propise i zakonske regulative. Također, pravilnici i regulative koji se odnose na fizičko radno okruženje za organizacijsku imovinu su adekvatno ispunjeni. Održavanje te daljinsko održavanje softvera nije strogo provođeno njezinom politikom te ne postoji adekvatna dokumentacija ili digitalni zapis u svrhu kontrole dok se u praksi softver održava nestandariziranim procesom. Prema rezultatima procjene, Tvrtka formalno neposjeduje razvijeni plan oporavka te plan odgovora na incident, dok se mogu primjetiti naznake rada na tom području. Potencijalni razlog tomu je što nedostaje adekvatnog znanja te eksperata za kibernetičku sigurnost. Potrebna je temeljitija procjena kibernetičkih rizika i ranjivosti kako bi se identificirale i ostale potencijalne prijetnje, pogotovo one koje zaobilaze fizičku kontrolu pristupa, te kako bi se prioritetno rasporedila sredstva za poboljšanje kibernetičke sigurnosti. Ujedno, postoji potreba za sveobuhvatnijim skupom mjera specifičnih za kibernetičku sigurnost, kao što su sigurnost krajnjih točaka, sustavi za otkrivanje i prevenciju provala. Tvrtka bi trebala razmotriti implementaciju ovih mjera kako bi zaštitila svoje sustave i podatke na učinkovit način.

4.4.3. Nadzor i otkrivanje anomalija (DE.AE DE.CM DE.DP)

Iako Tvrtka ima postavljene mjere za fizičku sigurnost i komunikaciju, ograničene su sposobnosti za otkrivanje kibernetičkih incidenata i prijetnji. Prema rezultatima procjene, ne postoji politika Tvrtke koja provodi analizu detektiranih kibernetičkih događaja u svrhu njihovog razumijevanja. Također, ne postoji utemeljena politika Tvrtke koja provodi praćenje mreže kako bi se otkrili potencijalni kibernetički događaji. Ujedno, politika Tvrtke ne provodi praćenje fizičkog okruženja kako bi se otkrili potencijalni kibernetički događaji. Ne postoje adekvatno implementirane sigurnosne kontrole za praćenje aktivnosti osoblja kako bi se otkrili potencijalni kibernetički događaji. Ne postoji adekvatna politika kojom se provode skeniranja ranjivosti, otkrivanje zlonamjernih kodova ili otkrivanje neovlaštenih mobilnih kodova. Politika Tvrtke ne provodi praćenje aktivnosti vanjskih pružatelja usluga kako bi se otkrili potencijalni kibernetički događaji. Praćenje neovlaštenih osoba, veza, uređaja i softvera se u praksi generalno provodi od strane IT osoblja, prema potrebi, bez definiranog i standardiziranog procesa. Robusni sustavi za otkrivanje provala u sustav, kontinuirano praćenje i postupci reakcije na incidente nisu još formalno uspostavljeni. Organizacija bi trebala ulagati u alate za praćenje kibernetičke sigurnosti, razviti plan reakcije na incidente i educirati zaposlenike kako bi brzo prepoznali i prijavili potencijalne prijetnje.

4.4.4. Odgovor na incident i komunikacija (RS.RP RS.CO RS.AN RS.MI)

Prema rezultatima procjene, Tvrtka nema formalno definiran plan reakcije na kibernetičke incidente. U praksi, incidenti se eventualno razriješe trudom IT odjela te sve relevantne stranke budu adekvatno informirane. U slučaju povrede, Tvrtka bi trebala imati dobro formalno definiran proces za ograničenje incidenta, ublažavanje njegova utjecaja i oporavak. Uspostavljanje tima za reakciju na incidente i redovito provođenje vježbi može pomoći organizaciji da razvije učinkovitiji odgovor na kibernetičke incidente.

4.4.5. Kontinuitet poslovanja i oporavak od katastrofe (RC.RP RC.IM)

Prema rezultatima procjene, odnosi s javnošću učinkovito se upravljaju, osiguravajući proaktivan pristup održavanju ugleda Tvrtke. U slučaju incidenta pravovremeno se provode strategije kako bi se vratilo povjerenje i ugled Tvrtke. Osim toga, aktivnosti oporavka komuniciraju se internim i eksternim strankama, kao i izvršnim i upravljačkim timovima, kako bi se osigurala transparentnost i održala usklađenost s organizacijskim ciljevima. Razvoj plana za kontinuitet poslovanja i oporavak od katastrofe specifičnih za kibernetičku sigurnost ključan je kako bi se osigurao brz oporavak kritičnih sustava i podataka u slučaju kibernetičkog incidenta.

4.5. Sažetak rezultata analize

U sažetku, rezultati su pokazali da je Tvrtka predana politikama koje reguliraju upravljanje imovinom, komunikaciju i fizičku zaštitu imovine, učinkovito ispunjavajući minimalne zahtjeve propisane relevantnim zakonima o kibernetičkoj sigurnosti. Međutim, za određena područja specifično vezana za kibernetičku sigurnost, kao što je sigurnosno praćenje sustava, otrkivanje softverskih anomalija ili priotiziranje softverskih ranjivosti, uopće ne postoji implementirana politika, dok se u praksi ipak poduzimaju određene mjere, neformalno, od strane IT odjela. Kako bi poboljšala ukupno stanje kibernetičke sigurnosti i uskladilo se s NIST-ovim okvirom za kibernetičku sigurnost, Tvrtka bi trebala implementirati mjere specifične za kibernetičku sigurnost. Takva transformacija zahtijeva redovito provođenje procjena rizika, analizu ranjivosti i njihovo priotiziranje, temeljitu izradu strategija odgovora na incidente te strategiju za oporavak od incidenta i stroge inicijative za obuku zaposlenika. Adresiranjem ovih ključnih područja, Tvrtka može učinkovito podignuti razinu sigurnosti svojih sustava, podataka i operacija, čime će ih zaštititi od konstantno razvijajućih prijetnji kibernetičkog svijeta. Ako se uprava Tvrtke odluči za takav podhvat, preporuka je da se potraži savjet i pomoć stručnjaka za kibernetičku sigurnost, istovremeno razmatrajući sudjelovanje u programima obuke i razumijevanja kibernetičke sigurnosti.

5. ZAKLJUČAK

U današnjem digitalnom svijetu, kibernetičke prijetnje predstavljaju značajnu zabrinutost za poduzeća, organizacije i pojedince diljem svijeta. Kao što je prikazano u ovom radu, konstantan rast kibernetičkih prijetnji, kao što su povrede osjetljivih podataka, ugrožavanje dostupnosti kritičnih sustava i napadi *ransomware*-a, ističe potrebu za snažnim mjerama kibernetičke sigurnosti. Iz nekoliko primjera sigurnosnih incidenata, koji su obrađeni u ovom radu, lako je primjetiti da takve prijetnje značajno utječu na poduzeća i organizacije, ugrožavajući njihovo poslovanje, ugled pa čak i opstanak. Izuzetno je važno da organizacije diljem svijeta adekvatno ulože u jačanje kibernetičke sigurnosti i shvate ovu problematiku ozbiljno. Osim ispunjavanja zahtjeva zakonskih regulativa vezanih za kibernetičku sigurnost, ulaganje u razvoj područja kibernetičke sigurnosti ne samo da štiti osjetljive podatke i kritične operacije, već i gradi povjerenje među klijentima i partnerima. Rezultati procjene obrađeni u praktičnom dijelu rada su pokazali da i dalje postoje poduzeća u Repuplici Hrvatskoj gdje rizici kibernetičke sigurnosti nisu u potpunosti usvojeni te da nedostaje stručnjaka u tom području koji bi pripomogli njezinom shvaćanju. U svijetu gdje je digitalni svijet sve više međusobno povezan i nepredvidljiv, očigledno je da organizacije svih vrsta moraju postaviti jačanje kibernetičke sigurnosti kao strateški cilj kako bi osigurale svoj dugoročni uspjeh na globalnom tržištu.

LITERATURA

[1] CISA (2019),What is Cybersecurity, URL: https://www.cisa.gov/news-events/news/what-cybersecurity

[2] J. Steinberg, Cybersecurity for dummies, John Wiley & Sons, SAD, 2019

[3] ISC2 (2021), CISSP Certification Exam Outline Summary , URL: https://www.isc2.org/Certifications/cissp/Certification-Exam-Outline

[4] STAR Ethical Hacking Experts, EHE: Ethical Hacking Expert (4th volume), Star Certification LLC, 2017

[5] Kaspersky (2018), DDoS Breach Costs Rise to over $2M for Enterprises finds Kaspersky Lab Report, URL: https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report

[6] Valimail (2019), More than 3 billion fake emails are sent worldwide every day, Valimail report finds, URL: https://www.valimail.com/newsroom/more-than-3-billion-fake-emails-are-sent-worldwide-every-day-valimail-report-finds/

[7] National Institute of Standards and Technology, Special Publication 800-39, Information Technology Laboratory, 2011, SAD

[8] Accenture, The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Research, Ponemon Institute LLC, SAD, 2019

[9] N. Shankar i Z. Mohammed, (2020). Surviving Data Breaches: A Multiple Case Study Analysis. Journal of Comparative International Management, 23(1), 35–54

[10] U.S. House of Representatives Committee on Oversight and Government Reform, The Equifax Data Breach report, SAD, 2018

[11] Federal Trade Commission (2019), Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, URL: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

[12] National Institute of Standards and Technology, The NIST Cybersecurity Framework, The NIST Research Library, SAD, 2018

[13] M. Sheward, Hands-on Incident Response and Digital Forensics, BCS Learning & Development Ltd, UK, 2018

[14] National Institute of Standards and Technology, Computer Security, Incident Handling Guide NIST.SP.800-61r2, The NIST Research Library , SAD, 2012

[15] Checkpoint (2022), Threat Intelligence report - Croatia, Check Point Software Technologies Ltd.

[16] Republika Hrvatska (2015), The national cyber security strategy of the Republic of Croatia. Official Gazette No. 108/2015, Zagreb, 7. Listopad 2015

SAŽETAK

U ovom diplomskom radu je obrađen sam pojam kibernetičke sigurnosti i njezina raščlanba na različite domene te vrste sigurnosnih prijetnji sa naglaskom na njihov utjecaj na poduzeća i organizacije te mogućnosti i načini kako njima adekvatno rukovati. Kroz rad se analizira trenutno globalno stanje kibernetičke sigurnosti te na nekoliko stvarnih primjera sigunosnih incidenata su prikazane posljedice kiberenetičkih prijetnji. Rad se osvrće na stanje kibernetičke sigurnosti u Republici Hrvatskoj te mjere koje je država poduzela sa ciljem njezinog jačanja. Obrađena tematika je po potkrijepljena praktičnim radom gdje je provedena analiza kibernetičke sigurnosti nad lokalnim poduzećem, prilagođena dostupnim resursima i potrebama ovog diplomskog rada.

Ključne riječi: Kibernetička sigurnost, sigurnosne prijetnje, upravljanje rizicima, poduzeća, analiza.

ABSTRACT

Cybersecurity threats and risk analysis with their impact on business operations

This thesis deals with the very concept of cybersecurity and its breakdown into different domains and types of most frequent cybersecurity threats with an emphasis on their impact on companies and organizations and the possibilities and ways to adequately handle them, referencing globally recognized cybersecurity standards. The paper analyzes the current global state of cybersecurity and on several real examples of security incidents the consequences of cyberthreats are presented which a reader can explore. The paper refers to the state of cyber security in the Republic of Croatia and the measures taken by the state with the aim of strengthening it. The topic is supported by practical work where a cybersecurity analysis was conducted using the industry recognized, NIST framework, over a local company, adapted to the available resources, and needs of this graduate thesis.

Key words: Cybersecurity, security threats, risk management, companies, analysis.