# Analiza uzroka i karakteristika kibernetičkih napada u privatnom sektoru

**Kovačić, Marko**





**SVEUČILIŠTE U SPLITU**

**EKONOMSKI FAKULTET**

**Završni sveučilišni prijediplomski rad**

# Analiza uzroka i karakteristika kibernetičkih napada u privatnom sektoru

**Mentor:**

**doc.dr.sc. Tea Mijač**

**Student:**

**Marko Kovačić**

**Split, kolovoz 2024**

## IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, Marko Kovačić,
(ime i prezime)

izjavljujem i svojim potpisom potvrđujem da je navedeni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja na objavljenu literaturu, što pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio navedenog rada nije napisan na nedozvoljeni način te da nijedan dio rada ne krši autorska prava. Izjavljujem, također, da nijedan dio rada nije korišten za bilo koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Split, 2024. godine

Vlastoručni potpis : MKovačić

**SADRŽAJ:**

## 1. DEFINICIJA PROBLEMA ISTRAŽIVANJA

Kibernetički napadi predstavljaju zlonamjerne pokušaje pojedinaca ili organizacija da neovlašteno pristupe informacijskim sustavima drugih organizacija s ciljem ostvarivanja prednosti. Organizacije u privatnom sektoru moraju prilagoditi svoje poslovanje novim tehnološkim zahtjevima koji proizlaze iz promjena u njihovom okruženju, što dovodi do povećane ovisnosti o tehnologiji. Ta ovisnost znatno povećava broj potencijalnih meta za kibernetičke napade. Prema izvještaju Svjetskog ekonomskog foruma (World Economic Forum) o globalnim rizicima za 2024. godinu, kibernetička nesigurnost se ističe kao jedna od glavnih briga privatnog sektora. Unatoč tome, informacije o uzrocima i karakteristikama kibernetičkih napada su raspršene i zahtijevaju mnogo truda za prikupljanje. Metode korištene u kibernetičkim napadima postaju sve sofisticiranije i neprestano se razvijaju, što ukazuje na to da problem nema jednostavno ni trajno rješenje. Stoga je nužno stalno praćenje novih trendova, analiza novih kibernetičkih napada i temeljita informiranost o tome kako i zašto privatne organizacije postaju mete takvih napada.

## 2. CILJ RADA

Primarni cilj ovoga rada je stvoriti sveobuhvatnu informacijsku podlogu o kibernetičkim napadima u privatnom sektoru. Analizom kompletiranih istraživačkih pitanja koja obuhvaćaju različite aspekte provedbe kibernetičkih napada, ističu se različite perspektive u domeni kibernetičke sigurnosti koje omogućuju otkrivanje novih uvida i obrazaca koji inače ne bi bili uočljivi analizom pojedinačnih aspekata. Također, sekundarni cilj ovog rada je istaknuti važnost informiranosti o kibernetičkim napadima koji predstavljaju globalnu prijetnju neovisnu o vremenu i djelatnosti, te istaknuti raspršenost informacija o kibernetičkim napadima i prevladavajuću nestandardiziranost pojmova, što otežava pronalazak relevantnih informacija.

Ključni istraživački ciljevi koje se želi postići u ovom radu su:

1. Definirati ključne pojmove koji omogućuju razumijevanje kibernetičkih napada i okruženja u kojem se događaju.

2. Definirati osnovne aktere u kibernetičkim napadima i analizirati potencijalne motive kibernetičkih napadača.

3. Istražiti uzroke u organizacijama privatnog sektora koji doprinose uspješnosti kibernetičkih napada.

4. Definirati prevladavajuće vrste kibernetičkih napada.

5. Analizirati potencijalne posljedice kibernetičkih napada u privatnom sektoru.

6. Definirati preventivne mjere koje doprinose smanjenju uspješnosti i vjerojatnosti događanja kibernetičkih napada.

7. Proučiti najveće uspješno provedene kibernetičke napade u privatnom sektoru.

## 3. METODE ISTRAŽIVANJA

Akademski rad se sastoji od teorijskog i praktičnog dijela. Za izradu teorijskog dijela korišten je pregled literature prema određenim ključnim riječima. S obzirom na nestandardiziranost pojmova u domeni kibernetičke sigurnosti te komplementarnim istraživačkim pitanjima s različitim karakteristikama, istraživanje teorijskog dijela provedeno je u više različitih faza. Početno je provedeno sveobuhvatno pretraživanje literature na više znanstvenih baza podataka koje uključuju Scopus, ScienceDirect, Google Scholar i IEEE Xplore. Tijekom početnog pregleda literature uočena je nekonzistentna i široka upotreba ključnih riječi koje se tiču teme ovog akademskog rada, što uzrokuje raspršenost relevantne literature. Svrha ovoga rada je stvoriti sveobuhvatnu informacijsku podlogu o kibernetičkim napadima, a s obzirom na to da je sustavni pregled literature postavljao ograničenja koja su onemogućila pronalazak relevantne literature, vođena je pretraga šireg obuhvata skupom relevantnih ključnih riječi: „Cybersecurity“, „Cyber Attack“, „Cybercrime“, „Data Breach“, „Corporate Espionage“, „Malware“, „Vulnerabilities“, „Security Threats“, „Business Security“. Proces odabira uključivao je pregled naslova, sažetaka i, prema potrebi, cijelih tekstova kako bi se osiguralo da odabrana literatura odgovara fokusu istraživanja. Prioritet su imale novije publikacije i utjecajni radovi koji doprinose razumijevanju izazova kibernetičke sigurnosti u privatnom sektoru. Ovakav pristup osigurao je sveobuhvatan, ali usmjeren pregled relevantne literature. Nakon uspostave primarne strukture rada, proveden je sustavni pregled literature za svako poglavlje akademskog rada prema ključnim riječima povezanih s pojedinim poglavljem, što je omogućilo temeljito istraživanje komplementarnih istraživačkih ciljeva te izradu konzistentnog teorijskog dijela koji obuhvaća različite aspekte kibernetičkih napada. Konačno, upotrebom web stranica, relevantnih sigurnosnih izvještaja i literature iz drugih znanstvenih disciplina, nadopunjeni su nedostaci u teorijskom dijelu.

Praktični dio akademskog rada je empirijsko istraživanje najvećih kibernetičkih napada u privatnom sektoru. Analiziran je skup sekundarnih podataka od 1147 slučajeva kibernetičkih napada koji imaju legitimno medijsko pokriće te koji su označeni kao kibernetički napadi s najvećim posljedicama. Izvori podataka prikupljeni su iz različitih internetskih izvora te očišćeni i usklađeni u jedinstveni skup podataka koji omogućuje primjenu deskriptivne statistike kako bi se uočili prisutni obrasci kibernetičkih napada u krajoliku prijetnji. Istraživanje je klasificirano kao eksplorativna analiza podataka, a glavni cilj bio je istaknuti prijetnje koje predstavljaju kibernetički napadi, ne ograničavajući se na specifične vremenske periode niti na pojedinačne djelatnosti u privatnom sektoru. Detaljniji opis provedenih koraka u empirijskom istraživanju te ograničenja prisutna tijekom istraživanja predstavljena su u pripadajućem poglavlju.

# 4. KIBERNETIČKI NAPADI U PRIVATNOM SEKTORU

## 4.1. Definicija kibernetičkih napada

Usprkos rastućoj važnosti i popularnosti kibernetičkih napada, definicije kibernetičkih napada te drugih pojmova u domeni kibernetičke sigurnosti su apstraktne i nedefinirane. Razlog prevladavajućeg nedostatka formaliziranosti općih ključnih pojmova djelomično potječe iz nedostatka preciznosti u kategorizaciji i nedefiniranog načina mjerenja ovakvih događaja (Harry, 2015). Mnogi događaji i pojave imaju jedinstvene karakteristike i specifičnosti, što onemogućava jedinstvenu klasifikaciju u kontekstu zakona zbog prevelike količine informacija. Različito kategoriziranje na svjetskoj i individualnoj razini dodatno povećava razinu nedefiniranosti jer se velik broj specifičnih pojmova dodjeljuje općenitim kategorijama kako bi se obuhvatilo što više pojava pod jednim sveobuhvatnim pojmom (Kosseff, 2020). Nadalje, problem koji se pojavljuje pri definiranju pojmova vezanih za kibernetičke napade je stalna evolucija i promjene koje se događaju zbog sinergije ljudskog i tehnološkog faktora, koji svojim utjecajem stvaraju potrebe za izmjenom pravila koja definiraju pojmove unutar domene kibernetičke sigurnosti (Singer & Friedman, 2014).

U ovom poglavlju opisat će se definicije ključnih pojmova za razumijevanje konteksta ovog akademskog rada. S obzirom na velik broj različitih tumačenja pojmova, bitno je istaknuti da je svrha ovog akademskog rada opisati važnost i utjecaj kibernetičkih napada u privatnom sektoru. Radi toga će se pri opisu pojmova koristiti perspektiva koja naglašava jednostavnost i preciznost, kako bi se uklonila dvosmislenost koja se javlja u upotrebi ovih pojmova u različitim kontekstima te kako bi svi čitatelji, neovisno o razini znanja, mogli razumjeti opisane pojmove.

### 4.1.1 Kibernetički prostor

*Kibernetički prostor (eng. cyberspace*) je globalni koncept unutar informacijskog okruženja koji predstavlja sustav svih međuzavisnih mreža informacijskog sustava sastavljenog od fizičkih i nefizičkih komponenti. Međuzavisne mreže predstavljaju nefizičku komponentu te obuhvaćaju sve online aktivnosti i interakcije na svjetskoj razini (uključujući Internet, telekomunikacijske mreže i elektromagnetski spektar) (National Institute of Standards and Technology, 2013). Bilo koja pohrana, izmjena i razmjena podataka putem umreženih sustava i softvera koji omogućuju navedene radnje predstavlja dio kibernetičkog prostora. Pojam kibernetičkog prostora također obuhvaća pripadajuću fizičku infrastrukturu koja omogućuje navedene aktivnosti te uključuje umrežene elektroničke uređaje koji se koriste za izvršavanje radnji nad podacima (Department of Defense, 2006). Iako se definicija kibernetičkog prostora odnosi na globalnu mrežu, ovaj pojam se često koristi za opis sustava

međuzavisnih mreža određene geografske cjeline, najčešće u kontekstu opisa otpornosti na digitalne prijetnje (The White House, 2023).

### 4.1.2 Krajolik prijetnji

*Krajolik prijetnji (eng. threat landscape)* označava sve potencijalne i identificirane kibernetičke prijetnje koje mogu utjecati na određeni sektor, skup korisnika ili vremensko razdoblje (Kaspersky Lab, 2024). Ovaj se pojam može promatrati kao perspektiva kroz koju se analiziraju specifični elementi u kibernetičkom prostoru. Za razumijevanje pojma krajolika prijetnji potrebno je razumjeti pojam kibernetičkog prostora i njegove značajke. To dovodi do zaključka da je krajolik prijetnji specifičniji pojam koji se koncentrira na ranjivosti, digitalne alate i specifične grupe napadača te njihove metode koje predstavljaju opasnost u određenom kontekstu (Kaspersky Lab, 2024). Zbog stalnog razvoja novih tehnologija i povećane povezanosti uzrokovane većom upotrebom digitalnih tehnologija, krajolik prijetnji se konstanto izmjenjuje pojavom novih kibernetičkih prijetnji (Lim, 2023).

### 4.1.3 Digitalni ekosustav

*Digitalni ekosustav (eng. digital ecosystem)* je otvoreni socio-tehnički sustav unutar kibernetičkog prostora koji se sastoji od digitalnih komponenti. Digitalne komponente mogu predstavljati softverske komponente, aplikacije, usluge, znanje, poslovne procese, zakone, odnosno sve koncepte koji se mogu izraziti određenim jezikom i prenositi u digitaliziranom obliku unutar ekosustava. Ovaj pojam obuhvaća i infrastrukturu koja podržava aktivnosti koje se vrše u kontekstu digitalnih komponenti. Nadalje, definiciji digitalnih ekosustava pripadaju entiteti (ljudi, organizacije) koji sudjeluju u digitalnom sustavu, što podrazumijeva međusobne interakcije i odnose među entitetima koje omogućavaju suradnju, dijeljenje znanja, evoluciju tehnologiju te promjenu samog ekosustava (Li, Badr, & Biennier, 2012).

Mnogi elementi unutar definicije pojma digitalnog ekosustava se preklapaju s već opisanim značenjem pojma kibernetičkog prostora. Karakteristike digitalnog ekosustava su samoorganizacija, skalabilnost i održivost, što su iste karakteristike koje opisuju pojam ekosustava u kontekstu biologije, a to je razlog zašto je sustav dobio naziv ekosustava (Zhang & Jacob, 2011). S obzirom na sličnosti pojava s definicijama u području biologije, koristit će se usporedba informatičkih pojmova s biološkim pojmovima zbog lakšeg razumijevanja. Promatrajući pojmove kroz razine biološke organizacije, ekosustav predstavlja zajednicu svih živih bića na određenom području, zajedno sa svim neživim komponentama okoliša s kojima ta bića stupaju u interakciju (Campbell et al., 2018). Navedeni pojam

jednako opisuje i digitalni ekosustav koji svojom definicijom stavlja naglasak na entitete koji se mogu promatrati kao sva živa bića na određenom području, dok digitalne komponente s kojima entiteti ustupaju u interakciju predstavljaju nežive komponente okoliša. Nadalje, kibernetički prostor se može usporediti s nadređenim pojmom ekosustava, biosferom, koja predstavlja naziv za globalni ekosustav, odnosno zbroj svih ekosustava. Biosfera uključuje razmjenu energije i materijala koji utječe na funkcioniranje i distribuciju živih bića kao što i pojam kibernetičkog prostora obuhvaća sve online aktivnosti i interakcije na svjetskoj razini (Campbellet al., 2018). Zaključak ove usporedbe je da se kibernetički prostor sastoji od digitalnih ekosustava, te s obzirom da krajolik prijetnji predstavlja perspektivu promatranja određenih elemenata kibernetičke sigurnosti, on se može primijeniti na razini kibernetičkog prostora, koja predstavlja veću cjelinu, i na razini digitalnog ekosustava, koji u kontekstu opisane teme može predstavljati manje cjeline, poput pojedinačnih država ili organizacija.

#### 4.1.4 Kibernetički napadi

*Kibernetički napadi (eng. cyber-attacks)* predstavljaju bilo koju vrstu aktivnosti provedenu unutar kibernetičkog prostora u svrhu ometanja, onesposobljavanja, uništavanja ili zlonamjernog kontroliranja računalnog okruženja (National Institute of Standards and Technology, n.d.). Iako to nije uvijek slučaj, kibernetički napadi najčešće predstavljaju zlonamjerne napade čija je svrha ostvariti motive napadača. Najjednostavnija podjela kibernetičkih napada bila bi na aktivne napade, koji podrazumijevaju modifikaciju podataka ili pokušaje dobivanja neautoriziranog pristupa u digitalne sustave, te pasivne napade koji ne stvaraju promjene u digitalnom sustavu, već služe za špijuniranje i prikupljanje informacija (Kim & Solomon, 2018). Komplementarni pojam koji se često povezuje s kibernetičkim napadima je *sigurnosni propust (eng. security breach).* Sigurnosni propust je bilo koji događaj koji uzrokuje kršenje načela sigurnosti: povjerljivost, integritet ili dostupnost (Aslan et al., 2023). Navedeni događaji mogu biti namjerni ili se dogoditi slučajno, ali ako negativno utječu na sposobnost poslovanja ili ugled organizacija, predstavljaju sigurnosni propust (National Institute of Standards and Technology, n.d.). Konačno, sintezom značenja oba komplementarna pojma dolazi se do zaključka da zlonamjerni kibernetički napadi uzrokuju namjerne sigurnosne propuste u organizaciji.

### 4.2. Motivi napadača

U kontekstu kibernetičkih napada, napadači koji izvršavaju aktivnosti kategorizirane kao kibernetički kriminal najčešće su zvani *hakeri (eng. hackers)*. Iako se pojam hakera u svakodnevnom govoru koristi kao opis za bilo kojeg pojedinca koji koristi svoja tehnološka znanja za provođenje zlonamjernih

napada, vandalizma, prevara, krađe identiteta ili drugih oblika kriminala (Kim & Solomon, 2018) ; pravo značenje titule hakera je pojedinac koji posjeduje tehnička znanja koja omogućuju savladavanje tehnoloških problema, neovisno o njegovoj namjeri (Chai & Rosencrance, 2021). Hakeri se mogu kategorizirati na dvije skupine: hakeri crnog šešira predstavljaju pojedince koji koriste svoja tehnička znanja i posebne alate za iskorištavanje ranjivosti bez autorizacije, s različitim motivima neprijateljske namjere. Nadalje, hakeri bijelog šešira ili češće zvani, etički hakeri predstavljaju autorizirane pojedince koji koriste svoje tehničke vještine kako bi pronašli slabosti u informacijskom sustavu koje se zatim prijavljuju ili popravljaju radi poboljšanja kibernetičke otpornosti sustava na napade (Kim & Solomon, 2018). Također, postoje hakeri sivog šešira koji koriste tehnička znanja za izvršavanje neautoriziranih aktivnosti koje nemaju izraženu neprijateljsku namjeru, već neki alternativni motiv (Kim & Solomon, 2018). Iako postoje dodatne klasifikacije hakera (npr. hakeri plavog šešira, *crackers*, *script kiddies*), one predstavljaju mješavinu karakteristika hakera bijelog i crnog šešira, stoga su dodatne klasifikacije nepotrebne za daljnje razumijevanje sadržaja rada. Tema ovog rada sporazumijeva hakere crnog šešira, koji ciljaju privatni sektor zbog različitih motiva. Iako bi točnije bilo koristiti nazive kibernetički napadači ili hakeri crnog šešira, zbog rijetke upotrebe navedenih pojmova u literaturi i svakodnevnom govoru, te uzimajući u obzir postojanje iznimka zbog promjenjive i složene prirode pojmova, nadalje u radu će se upotrebljavati nazivi: hakeri, kibernetički napadači i kibernetički kriminalci koji u kontekstu ovog rada predstavljaju pojedince s tehničkim znanjem koji izvode neautorizirane ilegalne radnje u kibernetičkom prostoru.

Mnogi kibernetički napadi uzrokovani su ljudskim greškama. Iako su ljudske greške neizbježne, kibernetički napadi predstavljaju relativno novi pojam koji zbog svoje opširnosti i apstraktnosti predstavljaju koncept kojem se mnogi entiteti digitalnih ekosustava još uvijek prilagođavaju. U kibernetičkim napadima je uočljivo iskorištavanje mnogih ljudskih psiholoških karakteristika. Navedene karakteristike uključuju sklonost povjerenju u druge osobe, sklonost pojedinaca da budu ljubazni, utjecaj anksioznosti i stresa, te osobne potrebe i želji. Hakeri često iskorištavaju ljudsku naivnost u procesu donošenja odluka koja je uzrokovana heurističkim brzim odlukama te stresnim situacijama koje stvaraju anksioznost i strah (Nurse & Bada, 2019). Kako bi se smanjila ljudska tendencija prema brzom odlučivanju umjesto prema odlučivanju na temelju vjerojatne istine (de Becker, 2000) potrebno je razumjeti sve aspekte kibernetičkih napada i hakera kako bi se smanjio broj ranjivosti uzrokovanih ljudskim greškama te kako bi se stvorila bolja kolektivna baza znanja za upravljanje rizikom u kibernetičkom prostoru. Razumijevanje motiva napadača omogućava entitetima da bolje razumiju što hakeri žele. S navedenim znanjem motiva napadača, pojedinci i organizacije se mogu zaštiti ciljane resurse i bolje upravljati rizikom (European Union Agency for Cybersecurity, 2023).

Uvjeti koji potiču povećanje broja kibernetičkih napada uključuju niske kriterije ulaska, koji se mogu promatrati kao visoki povrat na investicije (ROI). Minimalni uvjeti u 2024. godini za izvedbu kibernetičkog napada su:

- Potrebni hardver, što podrazumijeva bilo koji uređaj koji se može spojiti na Internet. Među najjeftinijim uređajima koji omogućuju povezivanje na Internet su laptopi i mobilni uređaji.
- Bežična veza, koja je već dostupna besplatno na mnogim lokacijama u svijetu.
- Softver potreban za kreiranje ili izvedbu kibernetičkog napada. Ovaj element predstavlja najskuplji minimalni uvjet te zahtjeva najviše truda za nabavu, jer najčešće predstavlja ilegalnu digitalnu komponentu.
- Anonimna *proxy* usluga, koja nije nužno potrebna za izvedbu napada, ali očekivana je upotreba alata za skrivanje identiteta napadača koji izvršava neautoriziranu aktivnost.

Također, bitno je napomenuti mogućnost nabave potrebnog softvera ilegalnim metodama ili korištenje besplatno dostupnog softvera (Gragido et al., 2013). Jedan od najvećih primjera koji dokazuje točnost navedenih minimalnih uvjeta je „Pljačka banke Bangladeš“. Ovaj kibernetički napad koristio je *phishing* napad u kojem su zaposlenici instalirali zlonamjerne programe otvarajući e-mail poslan od strane hakera. Zlonamjerni program je ciljao SWIFT sustav koji koriste banke, i hakeri su uspješno ukrali 81 milijun dolara koristeći vrlo jednostavnu metodu napada koja zahtjeva minimalne uvjete i dobru organizaciju među akterima u napadu (Bull, 2024). Zajedničko obilježje koje je uočljivo kod većine hakera, neovisno o motivu, je to da posjeduju karakteristike pragmatista. Tijekom planiranja izvedbe kibernetičkih napada, stavlja se naglasak na izvršavanje što efektivnijih radnji uz što manje troškove (Gragido et al., 2013).

Drugi uvjet koji potiče povećanje broja kibernetičkih napada je lakoća postizanja anonimnosti u digitalnom ekosustavu. Pronalazak identiteta hakera zahtjeva mnogo više resursa i vremena nego u tradicionalnom kriminalu, a čak i kad se hakeri pronađu, pravni postupci su mnogo kompleksniji i također zahtijevaju više vremena zbog već prethodno spomenute nedefiniranosti pravila vezane za kibernetički kriminal.

Motivi radi kojih se kibernetički napadi provode se mogu podijeliti u 5 kategorija (European Union Agency for Cybersecurity, 2023):

- Financijska dobit
- Špijunaža
- Destabilizacija
- Destruktivni

- Ideološki

Prevladavajući motiv u svim sektorima za sve vrste kibernetičkih napadača je financijska dobit (Verizon, 2024). Iako se u literaturi krađa podataka (eng. data theft) često spominje kao zaseban prevladavajući motiv, ona zapravo predstavlja komplementarni motiv koji je specifičnija komponenta drugih motiva, tj. najčešće se može uočiti kao komponenta motiva financijske dobiti (Ullah et al., 2017). Ideološki motivi, koji često spadaju pod pojam *haktivizma (eng. hacktivism)*, prikazuju različitu perspektivu u kojoj glavni cilj nije financijska dobit, već povećanje popularnosti određene ideologije ili entiteta (Chng et al., 2022). Iako njihove aktivnosti ne moraju biti nužno zlonamjerne, one predstavljaju neautorizirane radnje koje mogu prouzrokovati štetu u privatnom sektoru, što u određenom kontekstu uzrokuje da entiteti privatnog sektora postanu sporedne žrtve kibernetičkog kriminala. Kategorija destruktivnih motiva je najrjeđa, a razlog zašto se promatra pojedinačno je sklonost hakera da zaštite infrastrukturu nad kojom se napad izvršava umjesto da je unište, kako bi mogli iskoristiti informacije i potencijalne prilike koje su stvorili uspješnim napadom na određeni sustav. U većini slučajeva, motivi napadača obuhvaćaju elemente iz različitih navedenih kategorija motiva. Moguće je zaključiti da motivi špijunaže mogu nadalje stvoriti motive za financijsku dobit ili destabilizaciju nakon analize prikupljenih informacija (Nurse & Bada, 2019). Drugi primjer su primarni financijski motivi koji uzrokuju nastanak destabilizirajućih motiva u svrhu zaštite napadača (European Union Agency for Cybersecurity, 2023). Karakteristike kibernetičkog kriminala mogu se uočiti u karakteristikama kriminala bijelog ovratnika, koji u širem kontekstu predstavlja nefizička kaznena djela koja se najčešće provode zbog motiva financijske dobiti (Đeraj, 2023). Jedna od sličnosti koja se može uočiti jest da se zločin koji kriminalci počine može objasniti nedostatkom samokontrole. Takvi pojedinci imaju nižu samokontrolu što uzrokuje veće poteškoće u odupiranju iskušenjima i suzdržavanju od ponašanja uzrokovanih iracionalnim motivima, što konačno povećava vjerojatnost impulzivnih postupaka koji rezultiraju kriminalnim djelom (Soltes, 2016). Osim toga, studije sugeriraju da su kibernetički kriminalci često uključeni i u ilegalne aktivnosti u fizičkom svijetu, te se mnogi kriminalci fizičkog svijeta pridružuju kibernetičkim kriminalnim aktivnostima zbog nepostojanja mnogih ograničenja fizičkog svijeta. Konačno, bitno je napomenuti da su hakeri u suštini ljudske osobe koje su kompleksne i dinamične, što dovodi do zaključka da uvijek postoje neidentificirani motivi i iznimke, poput osvete, znatiželje i politike.

Konačno, važno je spomenuti sklonost hakera da se udružuju u grupe i mogućnost lakog regrutiranja novih članova. Organizirani kriminal u kibernetičkom prostoru može se definirati kao aktivnosti skupine pojedinaca koje djeluju transnacionalno i krše zakone barem jedne države (Nurse & Bada, 2019). Njihovi ciljevi se postižu ilegalnim neautoriziranim radnjama s ciljem ostvarivanja različitih motiva koji su već prethodno opisani. Organizacije hakera imaju različite vrste hijerarhije s različitim

razinama povezanosti, ali studije su pokazale da većina njih ima hijerarhiju temeljenu na povjerenju pojedinca prema članovima, kao i na povjerenju pojedinca da mu njegova digitalna okolina udovoljava očekivanim uvjetima poput anonimnosti, sigurnosti itd. Postoje različite kategorizacije grupa organiziranog kriminala u kibernetičkom prostoru, ali osnovna kategorizacija obuhvaća tradicionalne kriminalne grupe koje koriste tehnologiju kao pomoćni alat (uključujući kupnju usluga od drugih grupa povezanih s kibernetičkim napadima), organizirane grupe temeljene na kibernetičkom zločinu koje izvršavaju kibernetičke napade s ciljem postizanja zajedničkog cilja te grupe temeljene na ideologiji. Važno je istaknuti je da članovi grupa vrlo često imaju sličnosti u načinu razmišljanja, motivima i ciljevima. U mnogim slučajevima dokazano je da pojedinci ne sudjeluju u grupama samo zbog financijskih motiva, nego i zbog znatiželje, koja predstavlja česti sporedni motiv kod hakera (Nurse & Bada, 2019). Organizirane kriminalističke grupe uvode novu perspektivu u kojoj je potrebno promatrati ne samo pojedinačne motive članova grupe, već i motive grupe predstavljene kao jedinstveni entitet.

### 4.3. Uzroci kibernetičkih napada unutar poduzeća

Kroz pregled literature analizirani su globalni izvještaji za 2023. i 2024. godinu te je uočeno da svi izvještaji ističu organizirane hakerske grupe i krajnje korisnike kao glavne krivce zbog kojih se događaju uspješni kibernetički napadi (CrowdStrike, 2024; Office of the National Cyber Director, 2024; European Union Agency for Cybersecurity, 2023; Google Cloud, 2023; Verizon, 2024; World Economic Forum, 2024). Uzroci koji povećavaju rizik organizacije da bude ciljana kao meta kibernetičkog napada, kao i uzroci koji povećavaju vjerojatnost uspješnog provođenja kibernetičkog napada, mogu se kategorizirati u sljedeće kategorije:

- Ljudski faktor
- Karakteristike informatičkog sustava krajnjeg korisnika
- Razvoj tehnologije

#### 4.3.1 Ljudski faktor

Krajnji korisnici predstavljaju jedan od najvažnijih čimbenika koji omogućuju uspjeh kibernetičkih napada. U većini slučajeva pojedinci ne djeluju zlonamjerno, ali zbog nesvjesnih grešaka ili nepažnje stvaraju ranjivosti koje omogućuju kibernetičkim napadačima iskorištavanje sigurnosnih propusta. Posljednjih godina zabilježen je porast napada koji koriste metode psihološke manipulacije, poput phishinga, osobito putem e-mailova. Također, neadekvatno postupanje s osjetljivim podacima na

webu povećalo je broj kibernetičkih napada koji se koriste metodama socijalnog inženjeringa, što je uzrokovalo njihovu učestalost tijekom 2023. i početkom 2024. godine (Verizon, 2024; European Union Agency for Cybersecurity, 2023). Osim toga, nedostatak implementacije sigurnosnih standarda u organizacijskoj kulturi povećava rizik od ljudskih grešaka. Negativni stavovi i nedovoljno znanje o kibernetičkoj sigurnosti među zaposlenicima često rezultiraju neodgovornim ponašanjem koje može ozbiljno ugroziti sigurnost organizacije. Primjeri takvog ponašanja uključuju upotrebu jednostavnih lozinki, zanemarivanje ažuriranja softvera i operativnih sustava, nepažljivo rukovanje digitalnim sadržajem i dijeljenje osjetljivih informacija (Ogundare, 2024). Ovi problemi mogu se pogoršati nedostatkom adekvatne obuke i nepostojanjem jasnih procedura za postupanje u slučaju kibernetičkog napada (Selvan & Fonceca, 2023).

### 4.3.2 Karakteristike informatičkog sustava krajnjeg korisnika

#### Ranjivosti uzrokovane nedostacima hardvera

Napadi koji iskorištavaju hardverske nedostatke predstavljaju specifične izazove jer često zahtijevaju fizičke intervencije, poput ažuriranja ugrađenog softvera (eng. firmware) ili zamjene hardvera, za razliku od softverskih nedostataka koji se mogu riješiti digitalnim ispravcima (Mallick & Nath, 2024). Zlonamjerni programi korišteni u kibernetičkim napadima mogu uzrokovati hardverske probleme prekomjernim korištenjem resursa ili povećanom potrošnjom energije, što može dovesti do kvarova hardvera (Mallick & Nath, 2024). Dodatni sigurnosni rizici uzrokovani nedostacima hardvera uključuju mogućnost neovlaštenog kopiranja hardverskih komponenti i instalaciju zlonamjernih fizičkih komponenti (Aslan et al., 2023). Zbog složenosti integriranih sklopova i međusobne povezanosti hardverskih komponenti, otkrivanje ranjivosti može zahtijevati značajne resurse. Čak i male promjene u jednom dijelu sklopa mogu imati široke posljedice na druge komponente, a te promjene često ostaju neotkrivene duže vrijeme (Mallick & Nath, 2024). Proaktivne mjere, poput implementacije hardverskih uređaja otpornih na manipulacije, korištenja hardverskog označavanja za provjeru autentičnosti i primjene tehnika zamagljivanja, ključne su za povećanje kibernetičke sigurnosti (Aslan et al., 2023). .

#### Ranjivosti uzrokovane nedostacima softvera

Softverski nedostaci predstavljaju jedan od prevladavajućih uzroka kibernetičkih napada, uzrokovanih pogreškama i propustima u softverskom kodu. Razvoj tehnologije stvara potrebu za složenijim softverskim komponentama, što dovodi do pojave novih, raznovrsnih nedostataka koji mogu postati ranjivosti (Aslan et al., 2023). Uobičajeni uzroci koji stvaraju softverske nedostatke uključuju

nedostatke u validaciji unosa, neadekvatnu kontrolu pristupa, nepotpunu autentifikaciju i probleme s migracijom podataka. Prijetnje u kibernetičkom prostoru, kao što su *napadi uskraćivanja usluge (DoS)*, *SQL injekcije* i *cross-site scripting* (XSS) dodatno povećavaju rizik, omogućujući napadačima uspješnu izvedbu napada iskorištavanjem slabosti u softveru (Mallick & Nath, 2024). Nadalje, ubrzani razvojni ciklusi unutar organizacija često rezultiraju nedostatkom temeljitog sigurnosnog testiranja, ostavljajući softver podložnim napadima uslijed neadekvatnog upravljanja ranjivostima (Aslan et al., 2023).

Ranjivosti uzrokovane nedostacima mreže

Mrežni nedostaci predstavljaju kompleksne ranjivosti jer omogućuju napadačima presretanje, izmjenu ili potpuno zaustavljanje prijenosa podataka putem Interneta, osobito ako nisu primijenjene odgovarajuće sigurnosne mjere (Aslan et al., 2023). Upotreba zastarjelih mrežnih protokola i uređaja bez adekvatne sigurnosne zaštite glavni je uzrok ovih prijetnji. Ranjivosti u osnovnim mrežnim protokolima, kao što su *TCP, IP, ARP, DHCP* i *DNS*, stvaraju mogućnosti za različite metode napada, uključujući lažno predstavljanje IP adrese ili DoS napade (Aslan et al., 2023). . Neispravne konfiguracije mrežnih uređaja, poput preklopnika, usmjerivača i bežičnih pristupnih točaka, dodatno pogoršavaju situaciju omogućujući napadačima pristup osjetljivim informacijama tijekom prijenosa (Mallick & Nath, 2024).

### 4.3.3 Razvoj tehnologije

Umjetna inteligencija i strojno učenje

Umjetna inteligencija (UI) i strojno učenje značajno su promijenili krajolik prijetnji u kibernetičkom prostoru, pružajući napredne mogućnosti kibernetičkim napadačima. UI tehnologije omogućuju sofisticirane napade koji se prilagođavaju promjenjivim okruženjima, često nadmašujući mogućnosti tradicionalnih sigurnosnih mjera (Google Cloud, 2024; Guembe et al., 2022; Thanh & Zelinka, 2019). Kibernetički napadi temeljeni na upotrebi umjetne inteligencije koriste napredne algoritme za identifikaciju i iskorištavanje ranjivosti sustava, primjenjujući tehnike poput trovanja podataka i napada uzorcima protivnika kako bi oslabili postojeće sigurnosne sustave (Guembe et al., 2022). Ovi napadi dinamički prilagođavaju svoje strategije na temelju kontekstualnih podataka, čineći ih sve težima za otkrivanje i sprječavanje (Thanh & Zelinka, 2019). Iako UI može pojačati obrambene sposobnosti, njezina zloupotreba od strane zlonamjernih aktera naglašava potrebu za inovativnim rješenjima i prilagodbom postojećih sigurnosnih protokola (Zeng, 2022).

### Računarstvo u oblaku

Brzi porast upotrebe *računalstva u oblaku (eng. cloud computing),* koje omogućuje pristup digitalnim resursima putem Interneta, stvorio je složenije okruženje za kibernetičke prijetnje. Napadi sve češće ciljaju ključnu infrastrukturu oblaka, uzrokujući značajne sigurnosne izazove. Povećana primjena oblaka i njegova integracija s Internetom stvari (IoT) potaknula je zabrinutost zbog povreda podataka, ranjivosti, nesigurnih aplikacijskih programskih sučelja (API) i pogrešnih konfiguracija sustava (Abdi, Bennouri & Keane, 2024). Tradicionalni sigurnosni alati, dizajnirani za statična okruženja, često ne uspijevaju zaštititi dinamičke infrastrukture oblaka, što ukazuje na potrebu za naprednijim sigurnosnim mjerama (Abdi et al., 2024). Dodatni izazov predstavlja fragmentirana priroda tržišta oblaka, što otežava kompatibilnost i učinkovito upravljanje resursima (Hossain et al., 2016).

### Internet stvari

*Internet stvari* obuhvaća složenu mrežu povezanih uređaja, senzora i svakodnevnih predmeta koji omogućuju komunikaciju i razmjenu podataka putem Interneta. Ova komponenta digitalnog ekosustava uključuje raznolike uređaje, od pametnih kućanskih aparata do industrijskih strojeva i medicinskih uređaja, pružajući široku primjenu u različitim djelatnostima (Amoo et al., 2024). Međutim, širenje IoT sustava predstavlja povećanje kompleksnog sustava povezanih uređaja, što uzrokuje veći broj ranjivosti u raznovrsnim uređajima te različitim mrežnim sustavima koji kibernetički napadači mogu iskoristiti. Uspješni kibernetički napadi mogu stvoriti značajne posljedice koje utječu na veliki broj uređaja, a posljedice napada mogu širiti na povezane uređaje. Neusklađeni standardi koje upotrebljavaju komponente IoT sustava, kao i porast količine proizvedenih podataka predstavljaju dodatne izazove uzrokovane IoT sustavom. (IBM , 2024).

### Kriptovalute

Kriptovalute su oblik digitalne valute koji koristi kriptografske tehnike za osiguranje transakcija i kontrolu stvaranja novih jedinica (Kaspersky Lab, 2024). Kriptovalute, koje obično koriste *blockchain* tehnologiju, omogućuju *peer-to-peer* transakcije bez potrebe za centraliziranim financijskim institucijama. Iako nude prednosti poput povećane privatnosti i sigurnosti, kriptovalute su također podložne sigurnosnim rizicima, uključujući hakiranje i manipulacije, što može ugroziti podatke korisnika i transakcije. Osim tehničkih rizika, psihološki rizici povezani s upotrebom kriptovaluta, poput stresa ili nezadovoljstva zbog mogućih gubitaka, također mogu utjecati na percepciju i prihvaćanje od strane korisnika (Mirza et al., 2024).

#### 4.3.4 Povećana dostupnost znanja i alata za hakiranje

S vremenom su dostupnost znanja i alata za kibernetičke napade značajno smanjili prepreke za sudjelovanje u takvim aktivnostima. Dok su 1990-ih i ranih 2000-ih godina napadi zahtijevali visoku razinu tehničke stručnosti, danas internet i online forumi omogućuju čak i pojedincima s minimalnim tehničkim znanjima, poznatim kao script kiddies, da pokreću napade koristeći unaprijed razvijene alate (Mallick & Nath, 2024). Povratno inženjerstvo također je postalo uobičajeno, omogućujući napadačima da analiziraju postojeći softver kako bi identificirali ranjivosti ili replicirali funkcionalnosti (Ramkumar & Tanwar, 2023). Platforme koje nude kibernetičke napade kao uslugu dodatno olakšavaju pristup ovim alatima, omogućujući sofisticirane napade bez dubinskog tehničkog znanja (Mallick & Nath, 2024). Unatoč rastu složenosti napada, tehničko razumijevanje potrebno za njihovu provedbu smanjilo se, što predstavlja izazov za sigurnosne stručnjake (Aslan et al., 2023; Mallick & Nath, 2024; Ramkumar & Tanwar, 2023).

### 4.4. Vrste kibernetičkih napada

U domeni kibernetičkih napada postoje mnoge klasifikacije prema karakteristikama napada. Ključno je razlikovati načine izvedbe napada i alate koji koriste hakeri. U mnogim svjetskim izvještajima i literaturi pojmovi se raznovrsno kategoriziraju, te se u ovom poglavlju želi stvoriti kategorizacija prema glavnim zajedničkim obilježjima radi lakšeg razumijevanja. Također, pojmovi mogu biti komplementarni i metode izvedbe napada mogu uključivati alate za hakere.

#### 4.4.1 Zlonamjerni softver

*Zlonamjerni softver (eng. malware)* je naziv za skup različitih vrsta digitalnih alata koji se koriste u provedbi kibernetičkih napada. Postoji veliki broj različitih vrsta zlonamjernog softvera s mnogo specifičnih varijacija. U ovom poglavlju će se opisati najpoznatiji digitalni alati u krajoliku prijetnji koji su uočeni pregledom aktualnih sigurnosnih izvještaja.

##### Virusi

*Virusi* su zlonamjerni softveri koji, kada se uspješno izvrše, dupliciraju sami sebe tako što mijenjaju osjetljive datoteke i umeću svoj specifični kod. Tijekom izvršavanja, virusi repliciraju svoj zlonamjerni kod u drugi izvršni strojni kod ili skriptni kod. Ako se navedeni postupak izvrši uspješno, kod se smatra zaraženim te kada se kod izvrši, virusu se također omogućava da se izvrši, što omogućava ostvarenje

zlonamjernih naredbi (Stallings & Brown, 2024). Kao što je uočljivo iz definicije, virusi su zlonamjerni alati koji ima dvije primarne funkcije: dupliciranje u nezaraženim datotekama ili programima te izvršavanje zlonamjernih naredbi koje je odredio kreator virusa (Alhebshi et al., 2023). Izvršni strojni kod sastoji se od datoteka u binarnom formatu koje, kada se pokrenu, operativni sustav učitava u memoriju, a procesor ih izvršava. Najčešći primjer su *.exe* datoteke. Skriptni kod za pokretanje zahtijeva interpreter, koji izvršava upute po linijama koda. Kreatori virusa koriste raznovrsne metode kako bi sakrili detekciju virusa od antivirusnih programa. Neke od metoda uključuju:

- *Padding* - pridruživanje dodatnih datoteka kako bi se sakrio virus
- *Pressing* - kompresija virusa
- Enkripcija - mijenjanje prvobitnog formata (Alhebshi et al., 2023)

Postoje različite vrste virusa koje se mogu nalaziti u različitim datotekama, neki do primjera su makro virusi koji se nalaze u dokumentima s makronaredbama, *boot sector* virusi koji se nalaze u operativnim datotekama i program virusi koji se nalaze u softveru kojeg korisnici mogu instalirati. Također, virusi se mogu dobiti iz različitih izvora (e-mail, internet, bluetooth, piratizirani sadržaj, aplikacije s propustima itd.), a simptomi koje uzrokuju se mogu znatno razlikovati ovisno o vrsti i namjeni virusa (Alhebshi et al., 2023).

### Računalni crvi

*Računalni crvi (eng. worms)* su samoreplicirajući zlonamjerni kod koji se može samostalno širiti putem mrežnih veza iskorištavajući propuste uređaja spojenih na mrežu. Životni ciklus računalnog crva sastoji se od pronalaženja ciljeva, prijenosa, aktivacije i infekcije. Za razliku od virusa, sve faze životnog ciklusa crva se mogu provoditi bez ljudske intervencije, a većina se širi neovisno. Osim što crvi otvaraju kanale za daljnje širenje na druge uređaje, često zauzimaju mnogo resursa zbog kontinuiranog skeniranja za nove mete te mogu sadržavati dijelove koda za neovlašteno upravljanje podacima ili uređajem (Li, Salour, & Su, 2008; Namanya et al., 2018).

### Trojan

*Trojan ili trojanski konj (eng. Trojan Horse)* je zlonamjerni softver koji se predstavlja kao legitimni, čisti softver. Kada se trojan preuzme i izvrši, provode se ugrađene naredbe koje je kreator ugradio. Njegovo izvršenje ovisi o korisniku uređaja koji mora instalirati ili aktivirati zlonamjerni softver te se korisnika često manipulira metodom socijalnog inženjeringa da aktivira trojan (Namanya et al., 2018). Posljedice

izvršenja mogu biti znatno različite ovisno o dizajnu trojana, neke od čestih posljedica su: instalacija virusa, neautorizirano prikupljanje i slanje informacija (*spyware*), neautorizirane promjene na uređaju (*adware, rootkits*), odgođene promjene (*time bombs*) i dobivanje pristupa uređaju koristeći *Remote Access Trojan* (Mathur & Nwokedi, 2007; Mohanta & Saldanha, 2020).

Ucjenjivački softver

*Ucjenjivački softver (eng. ransomware)* je dominantna vrsta zlonamjernog softvera čija upotreba iznimno brzo raste u kibernetičkom prostoru te predstavlja značajnu prijetnju koja ugrožava mnoge segmente privatnog sektora (Office of the National Cyber Director, 2024; European Union Agency for Cybersecurity, 2023). Nakon što se uređaj zarazi ucjenjivačkim softverom, on omogućava kibernetičkom napadaču da zabrani pristup uređaju (*locker ransomware*) ili da šifrira datoteke na uređaju (*crypto ransomware*). Nadalje, krajnjeg korisnika se obavještava da mora platiti određenu svotu novca ili podijeliti osjetljive informacije ako želi dobiti ponovni pristup svom uređaju ili datotekama. Značajno je napomenuti da zadovoljavanje postavljenih uvjeta napadača ne garantira popravak posljedica. Često se koriste metode psihološke manipulacije kao što su vremenska ograničenja te neugodni zvučni i slikovni sadržaj, kako bi se stvorio osjećaj stresa i hitnosti, koji tjera žrtvu da nepromišljeno zadovolji zahtjeve kibernetičkog napadača. Dominantna upotreba ucjenjivačkog softvera u kibernetičkom prostoru uzrokovana je njegovom jednostavnošću izvedbe, koja omogućava napadačima da ciljaju veliki broj meta u različitim industrijama. Također, nabava ovakvog zlonamjernog softvera na „Dark webu“ je vrlo jeftina i dostupna velikom broju potencijalnih napadača kao usluga za iznajmljivanje (Temara, 2024). S obzirom na razvoj tehnologije, ucjenjivački softver je razvio mogućnosti da zarazi mrežne sustave kako bi spriječio povratak izgubljenih podataka putem mrežnih usluga, kao i mogućnosti da zarazi vanjski hardver povezan s zaraženim uređajem. Uz to, programski kod ucjenjivačkog softvera je vrlo zahtjevno koristiti za obrnuto inženjerstvo što otežava izradu antivirusa te ukazuje da je mnogo lakše spriječiti zarazu uređaja ucjenjivačkim softverom nego popravljati posljedice (Kim & Solomon, 2018). Konačno, neki od poznatih primjera ucjenjivačkog softvera su:

- *Locky ransomware*: Korišten u phishing metodama kako bi zarazio krajnje korisnike putem privitaka u zaraženim e-mailovima. Imao je mogućnost šifriranja 160 različitih vrsta datoteka.
- *Ryuk ransomware*: Onemogućavao funkciju oporavka ugrađenu u Windows operativnim sustavima, što je onemogućilo krajnjim korisnicima povratak podataka ako nisu imali vanjsku sigurnosnu kopiju.

- *Bad Rabbit*: Širio se preko nesigurnih stranica čije su ranjivosti koristili hakeri za provedbu napada. Krajnji korisnici koji su posjetili zaraženu web stranicu, nesvjesno su preuzimali zaraženi softver, koji se predstavljao kao legitimni program (Kaspersky Lab, 2024).

### Rootkit

*Rootkit* je naziv za zlonamjerni softver koji hakeri koriste kako bi prikrili prisutnost ostalih zlonamjernih programa u zaraženom sustavu (Lobo, Watters & Wu, 2010). Karakteristike koje obilježavaju rootkite su diskretnost i perzistencija, koje su komplementarne s primarnom svrhom rootkita da sakrije prisutnost virusa, računalnih crva i ostalih zlonamjernih programa od sigurnosnih detektora i krajnjih korisnika. Sustavi se mogu zaraziti upotrebom ranjivosti u već instaliranom softveru ili zbog grešaka uzrokovanih krajnjim korisnikom (Kumar, Stephen & Rumysia, 2024). Također, rootkiti su često prvi alat koji hakeri koriste nakon što dobiju neautorizirani pristup u sustav, što ih čini ključnim za uspješnu izvedbu mnogih metoda kibernetičkih napada (Lobo et al., 2010).

### Špijunski softver

*Špijunski softver (eng. spyware)* predstavlja skup zlonamjernih digitalnih alata za neautorizirano prikupljanje osjetljivih podataka koji se šalju kibernetičkim napadačima bez znanja krajnjeg korisnika. Tipične karakteristike ove vrste zlonamjernog softvera su diskretnost i perzistencija, što omogućava hakerima upotrebu špijunskog softvera za održavanje dugotrajne prisutnosti u zaraženim sustavima, što je značajno za metode napada poput *APT* napada, koji se koriste za postizanje dugoročnih ciljeva (Javaheri, Hosseinzadeh & Rahmani, 2018). Nadalje, špijunski softver dijeli mnoge slične karakteristike s virusima, poput nemogućnosti samostalnog kopiranja na druge uređaje i ovisnosti o radnjama krajnjeg korisnika, koji mora otvoriti datoteku sa špijunskim softverom instaliranu kroz nesigurne web stranice, e-mailove ili dobivenu spajanjem na nesigurne mreže (Aslan et al., 2023). Za razliku od virusa, koji stvaraju uočljive posljedice u zaraženom sustavu, špijunski softver se koristi kako bi se izbjegla detekcija od strane krajnjeg korisnika. Zbog široke uporabe takvog digitalnog alata razvile su se mnoge tehnike koje omogućuju prekrivanje zlonamjernog koda i dinamično izmjenjivanje strukture špijunskog softvera, što otežava detekciju na zaraženim uređajima (Javaheri et al., 2018).

### Keyloggeri

*Keyloggeri* su vrsta špijunskog softverskog programa koji se može instalirati na digitalne uređaje kako bi se prikupljali uneseni podaci. Ovaj alat omogućava hakerima neautorizirano prikupljanje osjetljivih podataka, poput lozinki ili podataka o kreditnim karticama, tako što presreće signale koji se razmjenjuju između tipkovnice i operativnog sustava uređaja. Prikupljeni podaci najčešće se zapisuju u *log* datoteku kojoj haker može pristupiti i analizirati prikupljene podatke. Također, keyloggeri mogu prikupljati dodatne podatke koji ne potječu od tipkovnica, poput aktivnosti na Internetu, slika zaslona ekrana uređaja ili zvučnog sadržaja mikrofona (Sabu et al., 2023). Povećani trend uporabe navedenog alata uočen je na svjetskoj razini, a može se pojavljivati u obliku softvera ili fizičke komponente koja se ugrađuje u hardver. Razvoj keyloggera je stvorio dodatne prednosti za kibernetičke napadače, poput filtriranja prikupljenih podataka i izbjegavanja antivirusnih zaštita (Javaheri et al., 2018). Konačno, naprednom analizom ponašanja krajnjih korisnika, od kojih se prikupljaju uneseni podaci, napadači mogu postići svoje ciljeve stvaranjem informacijske podloge koja omogućuje usporedbu različitih prikupljenih podataka korištenjem drugih vrsta digitalnog alata (Sabu et al., 2023).

### Logička bomba

*Logička bomba (eng. Logic Bomb)* je zlonamjerni kod koji se izvršava samo kada se zadovolje specifični kriteriji koje je postavio kibernetički napadač. Osim potrebe zadovoljavanja specifičnih uvjeta aktivacije, logičke bombe se kreiraju za specifične softvere i scenarije te se ne mogu samostalno replicirati. Navedena ograničenja omogućuju logičkim bombama izbjegavanje mnogih vrsta detekcije, jer testeri često ne mogu zadovoljiti potrebne uvjete za aktivaciju logičke bombe. Nadalje, kada su logičke bombe u neaktiviranom stanju, ne uzrokuju mnoge posljedice (npr. *runtime* greške) koje dinamički alati za detekciju koriste kako bi pronašli zlonamjerni kod, što čini ovaj kibernetički alat iznimno teškim za pronaći dok se ne aktivira (Dusane & Pavithra, 2020; Samhi, Bissyandé & Klein, 2022).

### Backdoor

*Backdoor* je skriveni dio softvera ili hardvera koji je instaliran kako bi se stvorila diskretna metoda ulaza koja izbjegava postojeće ugrađene sigurnosne zaštite. Navedeni digitalni alat koristi se za različite svrhe koje ne moraju nužno biti zlonamjerne. Mnogi proizvođači informatičkih tehnologija ugrađuju ovu vrstu ulaza kako bi olakšali pristup službama podrške koje pomažu krajnjim korisnicima. Hakeri mogu iskoristiti ranjivosti već postojećih ulaza ili umetnuti svoj backdoor, što im omogućava

neautorizirani pristup digitalnom sustavu, koji mogu iskoristiti za krađu podataka, instaliranje dodatnog zlonamjernog softvera i preuzimanje kontrole. S obzirom na to da hakeri žele održati dugotrajnu prisutnost, napadači koriste tehnike kojima izbjegavaju detekciju ovakvih ulaza. Najpoznatiji backdoor alat koji se koristi za stvaranje diskretnih ulaza je Netcat (Kim & Solomon, 2018; Malwarebytes, 2024).

Botnet mreža

*Botnet mreža* je skup zaraženih računala koji hakeri mogu neovlašteno kontrolirati kako bi postigli svoje ciljeve. Bilo koji nezaštićeni uređaj spojen na internet može se zaraziti zlonamjernim kodom, čime se hakeru omogućava komunikacija sa zaraženim uređajima koji se zovu botovi ili zombiji. Zaraženi uređaji mogu dalje širiti zlonamjerni kod i pretvarati druge uređaje u botove. Hakeri koriste botnetove za izvođenje kompleksnih metoda napada ili za povećanje efektivnosti kibernetičkog napada. S obzirom na to da botovi služe kao digitalni alat za provedbu napada, botnetovi razvijaju nove tehnike izbjegavanja detekcije kako bi održali dugotrajnu prisutnost (Zhang et al., 2011; Li & Liu, 2021). Osim što hakeri imaju mogućnost krađe podataka od zaraženih uređaja, botnetovi se koriste i za automatizaciju slanja spam e-mailova te za povećanje veličine DoS napada (European Union Agency for Cybersecurity, 2023).

Snifferi

*Snifferi* su pojam za digitalne program ili uređaj koji služe za prikupljanje podataka o mrežnom prometu specifičnih mrežnih sustava (Kulshrestha & Dubey, 2014). Predstavlja vrstu alata za prisluškivanje koji može prikupljati informacije potrebne za izvođenje kibernetičkih napada poput lozinki, DNS prometa, sadržaja e-mailova, chat sesija, konfiguracija usmjerivača ili web prometa. Često se upotrebljavaju za izvedbu metoda kibernetičkih napada kao što su phishing, DoS napadi i napadi na web aplikacije (Anu & Vimala, 2017).

### 4.4.2 Metode izvedbe kibernetičkih napada

Metode izvedbe kibernetičkih napada odnose se na raznovrsne načine na koje hakeri provode kibernetičke napade kako bi postigli određene ciljeve uvjetovane njihovim motivima. S obzirom na već opisanu apstrakciju pojmova koji se koriste u literaturi, izabrane su najpoznatije metode koje daju

pregled raznolikih karakteristika napada s kojima se krajnji korisnici mogu susresti.

## Socijalni inženjering

Socijalni inženjering obuhvaća sve metode napada u kojima napadač pokušava prevariti žrtvu da otkrije osjetljive informacije potrebne za postizanje krajnjih ciljeva ili omogućavanje daljnje izvedbe drugih metoda napada (Parsaei, 2024). Uspješnost napada temelji se na psihološkoj manipulaciji tijekom interakcije s žrtvom, u kojoj se iskorištavaju ljudske emocije i nedostatak opreznosti kako bi se osvojilo povjerenje žrtve (Ribeiro, Mateus-Coelho, & Mamede, 2023). Najzastupljenija metoda socijalnog inženjeringa u kibernetičkom prostoru je phishing, koji predstavlja značajnu prijetnju pojedincima i organizacijama (European Union Agency for Cybersecurity, 2023; Verizon, 2024). *Phishing* je metoda napada u kojoj napadač pokušava pridobiti osjetljive informacije od žrtve oponašajući povjerljivi entitet u digitalnoj komunikaciji. Ova metoda napada temelji se na automatizaciji koja se koristi kako bi zahvatila što veći broj potencijalnih žrtva, a najčešće se provodi korištenjem e-mailova koji preusmjeravaju krajnje korisnike na zlonamjerne web stranice (Alabdan, 2020; Alkhalil et al., 2021). *Spear phishing* je varijacija opisane metode koja se fokusira na pojedinačne žrtve, pri čemu je u ovoj metodi manje izražena uloga automatizacije, s obzirom da se napadač koncentrira na ciljane žrtve od kojih želi pridobiti osobne informacije (Atmojo et al., 2021). Također, iako je e-mail najčešće korišten komunikacijski kanal za provedbu phishing napada, mogu se koristiti drugi načini izvedbe. Primjer navedene tvrdnje su *pharming* napadi, koji opisuju naprednije oblike phishing napada u kojima se koriste identične kopije legitimnih web stranica za krađu podataka krajnjih korisnika (Gastellier-Prevost & Laurent, 2011). Razvoj tehnologije omogućuje kibernetičkim napadačima stvaranje sofisticiranijih varijacija phishing napada. *Deepfakes* su vrsta modificiranog medija temeljenog na naprednom strojnom učenju, koji koristi već postojeći vizualni i zvučni sadržaj za stvaranje lažne imitacije postojeće osobe ili događaja. Njihova upotreba omogućila je napadačima razvoj novih načina izvedbe phishing napada (Garg & Gill, 2023).

## Napadi uskraćivanjem usluga

*Napadi uskraćivanjem usluga (eng. Denial of Service)* jedna su od najzastupljenijih metoda napada u kibernetičkom prostoru, a njihova učestalost i sofisticiranost značajno raste prolaskom vremena. Pojavom novih vrsta napadačkih digitalnih alata te kombiniranjem starih identificiranih ranjivosti s novim *zero-day* ranjivostima, očekuje se daljnja evolucija ove metode napada i pojava novih varijacija (Verizon, 2024; Google Cloud, 2023). Cilj DoS napada je oštetiti servere, usluge ili mrežne sustave

slanjem iznimno velike količinu digitalnog prometa, koju sustav nije u mogućnosti procesirati. DoS napadi mogu se kategorizirati u sljedeće kategorije:

1. Protokolne napade, kao što su *SYN flood* i *Ping od death*, koji ciljaju slabosti u mrežnim protokolima.

2. Volumetrijske napade, kao što su *UDP* I *ICMP floods*, koji se temelje na slanju prekomjerne količine digitalnog prometa.

3. Aplikacijske napade, kao što je *HTTP flood*, u kojem napadači šalju prekomjeran broj legitimnih zahtjeva kako bi zauzeli resurse potrebne za normalno funkcioniranje aplikacija.

Cilj svih kategorija DoS napada je zauzeti ključne digitalne resurse (CPU, RAM, diskovni prostor) potrebne za normalno funkcioniranje informatičkog sustava organizacije. Krajnji ciljevi koje napadači pokušavaju postići su onemogućivanje mrežnog sustava, pri čemu je primarni motiv ove vrste napada destabilizacija. Također, preopterećenje mrežnih komponenti može oštetiti fizički hardver i stvoriti dodatne ranjivosti dok su žrtve zauzete rješavanjem posljedica samog DoS napada. Zbog razvoja tehnologije, ova metoda napada ima niske prepreke koje povećavaju uspješnost, jer se ranjivosti koje omogućuju ovu vrstu napada teško identificiraju. Nadalje, osim DoS napada, postoje *distribuirani napadi uskraćivanjem usluga (DDoS),* koji koriste dodatne zaražene uređaje, sustave i resurse spojene na internet kako bi povećali efektivnost napada. Ciljevi DoS i DDoS napada su identični, a temeljna razlika je u tome što DDoS napadi uključuju korištenje botneta za dodatnu snagu i efektivnost napada. (Brooks & Özçelik, 2020; Elleithy et al., 2005; Sujatha, Kanchal & George, 2022).

Lažno predstavljanje IP adrese

*Lažno predstavljanje IP adrese (eng. IP Address Spoofing)* jednostavna je metoda napada na web mrežne sustave koja se temelji na zloupotrebljavanju IP adresa. IP adrese su osnovni protokoli za izmjenu podataka preko Interneta, čija zaglavlja sadrže brojčane podatke o izvoru podataka, odnosno adresu pošiljatelja, te podatke o adresi gdje se paket šalje. Napadači izmjenom dijelova IP adrese mogu modificirati adrese i pritom pokušavati imitirati cjelovitu IP adresu legitimnog uređaja, kako bi prevarili žrtvu koja očekuje povratnu komunikaciju s drugim sigurnim uređajem. Uspješnost ovog napada ovisi o sposobnosti napadača da stvori što sličniju IP adresu sustava kojem žrtva vjeruje, a koriste ga napadači kojima nije bitna povratna reakcija žrtve. Ova metoda omogućava napadačima implementaciju backdoora u sustave žrtva te iskorištavanje ranjivosti rutera koji se koriste za komunikaciju, poput modifikacije IP adresa i pojedinačnog slanja podatkovnih paketa (Rashid & Paul, 2013).

Replay napadi

*Replay napadi* su metoda napada na web mrežne sustave koja može uništiti komponente digitalnog sustava kritične za sigurnost, i to bez potrebe za osjetljivim informacijama o sustavu. Zbog niskih zahtjeva za početnu izvedbu, ova metoda ne predstavlja složen način napada. U ovoj metodi napadač presreće podatkovne pakete iz mreže te ih kasnije ponovno koristi kako bi stvorio nepravilnosti na serveru koji ih je prvobitno slao. Slanje dupliciranih podatkovnih paketa pogoršava rad komponenti u sustavu, što može uzrokovati prekid usluge ili stvaranje ranjivosti koje omogućuju napadaču neovlašteni pristup sustavu (Kim & Solomon, 2018; Yu, et al., 2023).

Man-in-the-Middle napadi

*Man-in-the-Middle napadi* su metoda napada koja uključuje dvije ili više krajnjih točaka u raznovrsnim digitalnim komunikacijskim kanalima, uz kibernetičkog napadača koji dobiva pristup komunikacijskom kanalu. Za razliku od špijuniranja, napadač ovom metodom preuzima kontrolu nad komunikacijskim kanalom, što mu omogućava da modificira ili zamijeni sadržaj koji se prenosi kanalom, bez znanja krajnjih točaka koje primaju sadržaj. Napadač također može manipulirati dostupnošću sadržaja, uništavajući ili dodavajući komunikacijski sadržaj. Primjeri komunikacijskih kanala na koje se ova metoda može primijeniti uključuju GSM, UMTS, Long-Term Evolution (LTE), Bluetooth, Near Field Communication (NFC) i Wi-Fi (Conti, Dragoni, & Lesyk, 2016*). Otimanje (eng. hijacking)* je širi pojam koji obuhvaća Man-in-the-Middle napade te označava metode napada u kojima napadač preuzima kontrolu nad specifičnim dijelom digitalnog ekosustava (Aslan et al., 2023). Naziv Man-In-The-Middle potječe od košarkaškog termina u kojem jedan igrač presreće loptu dok je dvojica drugih pokušavaju dodati jedan drugome (Conti et al., 2016). Osim za krađu i manipulaciju informacija, ova se metoda napada može koristiti i za izvedbu DoS napada ili za slanje zlonamjernih datoteka (Kim & Solomon, 2018).

Brute-Force napadi

*Brute-Force napadi (eng. brute-force password attacks)* su jednostavna metoda napada na šifrirane digitalne elemente koja se temelji na ponavljajućem slučajnom pogađanju lozinki. Ova metoda ne zahtijeva prethodno znanje o ciljanoj meti, a uspješnost metode raste kada se primjenjuje na veliki broj korisnika (Herley & Florêncio, 2008). Hakeri mogu koristiti različiti softver i napredniji hardver za poboljšanje brzine kojom se napadi izvode, a mogu se primijeniti i mnogi alati za automatizaciju koji povećavaju broj zahvaćenih pojedinaca (Gautam, 2024). Iako navedena metoda ne zahtijeva složene

tehnike i mnogo resursa, ovo je jedna od najčešćih vrsta napada na autentifikacijske podatke koja se uspješno provodi u kibernetičkom prostoru (Verizon, 2024).

### Napadi rječnikom

*Napadi rječnikom (eng. dictionary password attack)* su metoda napada koja se koristi za probijanje digitalnih sigurnosnih slojeva zaštićenih lozinkama. Metoda podrazumijeva sistematsko testiranje svih fraza u rječniku, koji u navedenom kontekstu predstavlja datoteku s čestim lozinkama i njihovim varijacijama, uključujući velika slova, dodatne brojeve ili zamijenjene znakove. Uspješnost ove metode ovisi o rječniku koji se koristi za unos i uključenim varijacijama u rječniku. Ova metoda je često uspješna jer pojedinci i organizacije koriste predvidljive lozinke koje se već nalaze u rječniku (Gautam, 2024)

### Zloupotreba privilegija

*Zloupotreba privilegija (eng. privilege misuse)* istovremeno predstavlja metodu napada i potencijalnu ranjivost, u kojoj akteri unutar organizacije, uključujući trenutne i bivše radnike te poslovne partnere, kradu povjerljive informacije ili sabotiraju organizaciju koristeći vlastite ili tuđe privilegije. Akteri unutar poduzeća su u mogućnosti stvoriti veće negativne posljedice u usporedbi s napadima koji potječu izvan organizacije, jer imaju bolje poznavanje unutarnjih procesa. Otkrivanje ove metode napada otežano je, jer se zlonamjerne radnje pojedinaca, kojima je organizacija dala ovlasti, mogu zanemariti kada se promatraju izolirano. Motivi koji potiču ovu metodu napada uključuju financijsku dobit, špijunažu ili destabilizaciju. Prikupljene osjetljive informacije ili stvorene ranjivosti koriste se kao korak za postizanje primarnog cilja napadača ili se prodaju kibernetičkim kriminalcima kako bi se upotrijebili za uspješno provođenje drugih napada (Duessel, et al., 2020; Yilmaz & Can, 2024).

### Napadi na web aplikacije

*Napadi na web aplikacije (eng. web application attacks)* metoda su napada koja cilja aplikacijske programe pohranjene na udaljenim serverima, a koji se korisnicima dostavljaju putem internetske veze i prikazuju u pregledniku (TechTarget Contributer, 2023). Web usluge su web aplikacije koje se koriste na mnogim web stranicama, a najčešće ranjivosti u njima uzrokovane su nepravilnim sigurnosnim postavkama, poput nepravilne autentifikacije ili problema filtriranja nepouzdanih unosa, što omogućuje hakerima umetanje zlonamjernog koda u komponente web aplikacije (Mitropoulos et al., 2019). Razvoj web aplikacija uključuje korištenje većeg broja poslužitelja, a porast složenosti i broja

korisnika također predstavlja ranjivosti koje omogućuju kibernetičkim napadima da zahvate veliki broj korisnika ako su uspješno izvedeni (El Moussaid & Toumanari, 2014). Najčešće vrste ove metode napada su Cross-Site Scripting (XSS) i SQL injekcijski napadi. Iako postoje mnoga sigurnosna rješenja, broj ovih napada ne smanjuje se zbog lake prilagodljivosti napada hakera i niskih kriterija koji povećavaju uspješnost, poput nemogućnosti kontrole svih nepouzdanih unosa, što omogućuje injekciju zlonamjernog koda (Mitropoulos et al., 2019).

### Napadi na opskrbni lanac

*Napadi na opskrbni lanac (eng. supply chain attacks)* predstavljaju neizravnu metodu napada u kojoj hakeri stvaraju i iskorištavaju ranjivosti komponenti informatičkog sustava koje čine bilo koji dio opskrbnog lanca. U ovoj metodi hakeri pokušavaju umetnuti zlonamjerni alat u opskrbni lanac ili izmijeniti postojeće komponente u svoju korist. Ova vrsta napada često cilja partnere povezane s glavnom ciljanom metom, a napadi često iskorištavaju ranjivosti tih partnera koji nesvjesno šire umetnuti zlonamjerni alat na glavnu metu, smatrajući svog partnera u opskrbnom lancu pouzdanim izvorom. Navedena tvrdnja pokazuje da uspješnost napada, nakon što je izveden, ovisi o tome kako hakeri koriste pristup opskrbnom lancu kako bi postigli svoje ciljeve i utjecali na lanac opskrbe (Heinbockel, Laderman, & Serrao, 2017). Posljedice uspješnih napada na opskrbni lanac mogu uključivati nestašice, prekide opskrbe i stvaranje dodatnih ranjivosti u informatičkom sustavu (Squillace & Cappella, 2024). Organizacije za kibernetičku sigurnost često su ciljane ovom metodom napada i predstavljaju ključnu komponentu opskrbnog lanca u razdoblju digitalizacije poslovanja, što naglašava nepredvidljivost kretanja ove metode napada u opskrbnom lancu i otežani pronalazak izvora napada nakon što je izveden (Cloudflare, 2024).

### Zero-Day napadi

*Zero-Day napadi* opisuju metodu napada u kojoj hakeri koriste ranjivosti koje prethodno nisu bile poznate. Ovi napadi koriste neotkrivene ranjivosti koje postoje u sustavu i za koje ne postoji rješenje koje bi moglo popraviti ranjivost ili posljedice napada (Roopak et al., 2024). Broj provedenih zero-day napada ima značajni porast prolaskom vremena, a razlog ovog trenda leži u prednostima koje ova metoda nudi. Koristeći novu, neotkrivenu ranjivost, hakeri dobivaju znatno više vremena za postizanje svojih ciljeva jer je u prosjeku potrebno 17 dana da se zero-day napad detektira. Nakon detekcije, potrebno je razviti rješenje koje će popraviti novu ranjivost, što u prosjeku zahtjeva dodatnih 15 dana.

Zbog otežane detekcije napada, hakeri imaju priliku proširiti svoj utjecaj kroz sustav i održati prisutnost čak i nakon popravka nove primarne ranjivosti (Google Cloud, 2023; Roopak et al., 2024).

APT napadi

*APT napadi (eng. Advanced Persistent Threats)* predstavljaju kompleksne metode izvedbe kibernetičkih napada koje se provode tijekom duljeg vremenskog razdoblja kako bi se ostvarili specifični ciljevi. Ova vrsta napada sporazumijeva dugotrajne planove organiziranih kriminalnih grupa koje se sastoje od više koraka, koristeći sofisticirane tehnike te stalno prilagođavajući korake napada kako bi se postigli dugotrajni ciljevi (Ussath, Jaeger, Cheng, & Meinel, 2016). Standardizirani koraci u APT napadima su (Wang, Liu, Li, Su, & Li, 2024):

1. Uspostavljanje ulaza u sustav organizacije korištenjem socijalnog inženjeringa ili iskorištavanjem ranjivosti.

2. Kretanje kroz sustav organizacije, koje uključuje korištenje različitih metode napada i alata kako bi napadači dobili veće razine autorizacije u sustavu i prikupili potrebne informacije za daljnje korake.

3. Perzistencija je ključni korak koji opisuje sve metode i alate koje napadači koriste kako bi osigurali dugotrajnu prisutnost u sustavu i omogućili sebi ponovni ulazak. Ovaj korak najčešće uključuje alate kao što su backdoorovi i trojanski konji.

4. Izvlačenje podataka iz sustava organizacije uspostavljanjem dugotrajne nevidljive prisutnosti i dobivanjem potrebnih autorizacija tijekom duljeg razdoblja.

APT napadi koriste različite metode i alate koji ciljaju različite slabosti sustava istovremeno te se konstanto prilagođavaju sustavu koji napadaju, što ih čini vrlo teškim za sprječavanje, otkrivanje i analizu. U mnogim slučajevima uočena je njihova sposobnost zaobilaženja sigurnosnih mjera i standarda, a napadači se često aktivno suprotstavljaju sigurnosnim preprekama, zbog čega su ti napadi opisani kao perzistentni (Ussath et al., 2016).

### 4.5 Potencijalne posljedice kibernetičkih napada

Posljedice kibernetičkih napada ovise o mnogim faktorima, što otežava izravnu procjenu štete s kojom se organizacije suočavaju tijekom i nakon napada. Osim izravnih financijskih troškova koji nastaju pri oporavku informatičkog sustava na stanje prije napada, žrtve kibernetičkih napada suočavaju se s mnogim vrstama troškova koji se ne mogu iskazati kvantitativno. Kibernetički napadi također utječu

na mnoge elemente organizacije i njezine okoline, a rezultati tih utjecaja postaju vidljivi u različitim vremenskim razdobljima. Ovi razlozi otežavaju efektivno planiranje i upravljanje rizikom u kibernetičkom prostoru zbog nemogućnosti predviđanja posljedica (Cashell et al., 2004). Nije moguće obuhvatiti sve vrste posljedica koje se pojavljuju u privatnom sektoru jer ovise o veličini napada i organizacije, djelatnosti organizacije, utjecaju medija, vrsti i značaju ukradenih resursa te mnogim drugim faktorima. U ovom poglavlju bit će obrađene najčešće vrste posljedica s kojima su se suočavale različite djelatnosti privatnog sektora.

### 4.5.1 Financijski troškovi

Procjenjuje se da su kibernetički napadi u 2023. godini uzrokovali trošak od približno osam trilijuna USD, s očekivanjima da će ta brojka rasti u narednim godinama (Lim, 2024). Kao što je prethodno navedeno, pregledom literature uočljivo je da su primarni motivi kibernetičkih napadača financijska dobit. Ovo opažanje ističe da organizacije privatnog sektora, nad kojima se uspješno provode kibernetički napadi, mogu očekivati povećani rizik krađe financijskih sredstava. Organizacije koje postanu žrtve kibernetičkih napada moraju uložiti dodatne resurse i angažirati vanjske stručnjake kako bi uklonile zlonamjerne programe i oporavile zahvaćene komponente informatičkog sustava na prvobitno stanje (Cashell et al., 2004). Također, potrebno je popraviti ranjivosti koje su omogućile uspješnu izvedbu napada, što može zahtijevati dodatne investicije u kibernetičku sigurnost, osiguranje i novu informatičku opremu, ovisno o odlukama organizacije (Lewis & Baker, 2013). Neizravni financijski troškovi mogu nastati zbog zahtjeva zahvaćenih dionika organizacije za dodatne odštete putem pravnim postupaka, što zahtjeva ulaganje dodatnih resursa kako bi se razriješile pravne poteškoće. Ovi troškovi nastaju čak i u slučajevima kada organizacije ne moraju plaćati odštetu (Cashell et al., 2004).

### 4.5.2 Utjecaj na poslovne procese

Ovisno o vrsti napada, kibernetički napadi mogu stvoriti mnoge oportunitetne troškove, uključujući izgubljenu prodaju, izgubljene poslovne prilike ili izgubljene prednosti. Ovisnost poslovnih procesa organizacije o kibernetičkom prostoru značajno utječe na visinu oportunitetnih troškova, što je izraženo u organizacijama koje posluju isključivo putem digitalnih kanala (Lewis & Baker, 2013). Mnogi zlonamjerni programi i metode kibernetičkih napada, poput virusa, računalnih crva ili DoS napada, negativno utječu na produktivnost organizacije i zaposlenika. Česti uzroci pada produktivnosti

uključuju onemogućavanje ključnih mrežnih sustava, usporavanje uređaja te onemogućavanje ili oštećenje servera (Saini, Rao, & Panda, 2012).

### 4.5.3 Utjecaj na reputaciju i povjerenje kupaca

Jedna od ključnih posljedica kibernetičkih napada je negativan utjecaj na reputaciju organizacije nad kojom je uspješno proveden kibernetički napad. Reputacija i povjerenje kupaca apstraktni su pojmovi ključni za poslovanje organizacija, a negativni utjecaji na njih mogu stvoriti značajne oportunitetne troškove tijekom dužeg vremenskog razdoblja (Lewis & Baker, 2013). Česti primjeri takvih oportunitetnih troškova su gubitak kupaca, investitora i drugih dionika. Kibernetički napadi također mogu pogoršati položaj organizacije na financijskom tržištu, što može povećati cijenu kapitala, troškove osiguranja, a banke mogu smatrati oštećenu organizaciju rizičnom (Cashell et al., 2004). Troškove uzrokovane negativnim utjecajem na reputaciju teško je precizno kvantificirati zbog mnogih specifičnosti prisutnih u analizi povezanog rizika. Značajnost posljedica u različitim vremenskim razdobljima ovisi o postupanju organizacije i medijskom pokriću, koji značajno utječu na razinu rizika koju navedene posljedice stvaraju (Makridis, 2021). Osim novčanih jedinica, česta mjerna jedinica koja se koristi pri procjeni veličine napada je broj izgubljenih ili ukradenih jedinica podataka (zapisa), pri čemu se analizira količina zahvaćenih podataka te se na temelju tih informacija stvara informacijska podloga za procjenu štete.

### 4.5.4 Krađa intelektualnog vlasništva i poslovnih tajni

Krađa intelektualnog vlasništva može imati različite posljedice, ovisno o postupcima organizacije i napadača koji je ukrao informacije. Iako krađa intelektualnog vlasništva ne utječe na poslovne procese organizacije, njezine posljedice mogu se uočiti u kasnijem vremenskom razdoblju i ugroziti položaj organizacije u odnosu na konkurente koji imaju pristup ukradenim informacijama. Intelektualno vlasništvo omogućava organizacijama lakšu provedbu poslovnih procesa i održavanje konkurentske pozicije jedinstvenošću, ali ukradene informacije se mogu implementirati u druge organizacije, što može uzrokovati gubitak kupaca u dužem roku. Nadalje, poslovne tajne predstavljaju osjetljive informacije koje omogućuju bolju poziciju u poslovnim pregovorima ili u razvoju ključnih poslovnih strategija. Za razliku od intelektualnog vlasništva, kibernetički napadači mogu odmah iskoristiti poslovne tajne na ilegalnim tržištima. Oportunitetni trošak nastao krađom intelektualnog vlasništva i poslovnih tajni predstavlja mnogo veću prijetnju od izravnih financijskih troškova, s obzirom na

nemogućnost povratka informacija od konkurenta i zbog dugotrajne prisutnosti navedenih posljedica (Lewis & Baker, 2013).

#### 4.5.5 Psihološki utjecaj

Kibernetički napadi imaju različite psihološke utjecaje na razne entitete unutar i izvan organizacije. Uspješno izvedeni kibernetički napadi potiču druge kibernetičke napadače da ciljaju već napadnutu organizaciju, pretpostavljajući da ona nema adekvatnu zaštitu protiv kibernetičkih prijetnji. Nadalje, postoji mogućnost da zaposlenici koji su svjedočili kibernetičkom napadu razviju strah. Mnogi zaposlenici nakon kibernetičkih napada smatraju da su njihovi poslovi ugroženi jer ne znaju jesu li njihove greške uzrokovale napad te izbjegavaju odgovornost skrivajući informacije (Cashell et al., 2004). Konačno, kibernetički napadi na velike organizacije mogu stvoriti paniku među korisnicima ili u široj javnosti, a utjecaj medija i postupci organizacija ključni su za sprječavanje pogoršanja ovakvih posljedica (Gandhi, Laplante, & Sousan, 2011).

### 4.6 Preventivne mjere kibernetičkih napada

Kibernetička sigurnost (eng. cybersecurity) širok je pojam koji obuhvaća sve resurse, procese i sustave korištene za zaštitu elemenata kibernetičkog prostora (Craigen, Diakun-Thibault, & Purse, 2014). Tri ključna načela kibernetičke sigurnosti su povjerljivost, integritet i dostupnost. Načelo povjerljivosti predstavlja zaštitu podataka od neautoriziranog pristupa u kibernetičkom prostoru. Ovo načelo podrazumijeva potrebu klasifikacije podataka u različite kategorije te uključuje sigurnosne mjere poput šifriranja, autentifikacije i tehnika kontrole pristupa. Nadalje, načelo integriteta odnosi se na održavanje preciznosti, potpunosti i informacijske vrijednosti podataka. Integritet se održava izmjenom podataka od strane autoriziranih entiteta te omogućava pravilnu upotrebu, transparentnost i mogućnost oporavka podataka. Konačno, načelo dostupnosti odnosi se na mogućnost pristupa podacima od strane autoriziranih osoba (Aslan et al., 2023). U domeni kibernetičke sigurnosti postoje mnogi digitalni alati i tehnike za zaštitu informatičkih sustava od specifičnih vrsta kibernetičkih napada. Nadalje će biti opisane često korištene tehnike koje smanjuju uspješnost raznovrsnih kibernetičkih napada.

#### 4.6.1 Pretpostavka kibernetičkog napada

Jedan od glavnih uzroka koji omogućava hakerima uspješnu izvedbu kibernetičkih napada jest ljudski faktor u kibernetičkom prostoru. Zbog navedenog razloga, potrebno je isticati mogućnost

kibernetičkog napada u bilo kojem trenutku te integrirati u organizacijsku kulturu shvaćanje da uporni hakeri mogu uvijek dobiti neautorizirani pristup ulaganjem resursa i vremena. Komplementarne metode s ovom perspektivom uključuju provođenje sigurnosnih testova, kreiranje planova oporavka i provođenje simulacija napada (npr. crveno/plavi tim metoda) (Diogenes & Ozkaya, 2022).

### 4.6.2 „Zero Trust“ arhitektura

Organizacije mogu implementirati „Zero Trust“ arhitekturu koja izvorno potječe iz međunarodnog standarda „NIST 800-207“. „Zero Trust“ arhitektura obuhvaća širi koncept od same tehnologije te uključuje pravila, politike i perspektive koje se temelje na načelu da je povjerljivost, integritet i dostupnost podataka potrebno kontinuirano nadzirati i štititi od mogućih prijetnji. Za uspješnu implementaciju ove arhitekture, organizacije trebaju usvojiti pretpostavku da se kibernetički napadi mogu ili se već događaju, bez obzira na lokaciju ili okruženje.

Ključni principi koji definiraju „Zero Trust“ arhitekturu su:

- Ne postoji implicitno povjerenje u mrežne sustave: Niti jedan mrežni sustav, uključujući unutarnje mreže organizacije, ne smije se automatski smatrati sigurnim.
- Raznoliki uređaji u mrežnom sustavu: Mnogi uređaji povezani s mrežom organizacije možda nisu u njezinom vlasništvu, što zahtijeva dodatne mjere sigurnosti.
- Provjera svih resursa: Potrebno je provjeravati sve resurse, a ne samo njihove komunikacijske kanale, kako bi se osigurala cjelokupna sigurnost.
- Sigurnosne politike za vanjske entitete: Potrebno je uspostaviti sigurnosne politike i pristupe prema resursima i komunikacijskim kanalima koji su povezani s entitetima izvan organizacije (Brotherston & Berlin, 2017).

### 4.6.3 Edukacija zaposlenika

Mnoge organizacije podcjenjuju prijetnje kibernetičkih napada, što rezultira minimalnim ulaganjima u edukaciju zaposlenika o kibernetičkoj sigurnosti. Stvaranje efektivnog edukacijskog programa zahtijeva mnogo resursa, a rezultati mnogih edukacijskih programa pokazali su se neuspješnim zbog nedostatka kontinuirane primjene usvojenog znanja. Socijalni inženjering i phishing metode napada predstavljaju dominantne prijetnje u kibernetičkom prostoru, a njihova uspješnost znatno ovisi o znanju i percepciji krajnjeg korisnika. Provođenje uspješnog edukacijskog programa za usvajanje

osnovnog znanja o kibernetičke sigurnosti zahtijeva definiranje jasnih ciljeva i informacijske podloge o trenutnom stanju organizacije i zaposlenika. Uspješnost edukacije također ovisi o definiranim pravilima i smjernicama u organizaciji jer izravno utječu na organizacijsku kulturu. Kako bi se povećala efektivnost i efikasnost pri usvajanju znanja, organizacije mogu implementirati metode poput gamifikacije ili pozitivne motivacije. Konačno, definiranje metode praćenja napretka tijekom edukacije potiče zaposlenike da rade prema definiranim ciljevima te omogućuje praćenje uspješnosti programa (Brotherston & Berlin, 2017).

### 4.6.4 Upravljanje ranjivostima

Upravljanje ranjivostima ključni je faktor za sve organizacija u kibernetičkom prostoru jer sprječava povećanje broja potencijalnih kibernetičkih napada. Prije svega, organizacije moraju odabrati alat za analizu ranjivosti, uzimajući u obzir svoje potrebe, dostupne resurse i razinu znanja o kibernetičkoj sigurnosti. Odabir alata za procjenu ranjivosti zahtijeva analizu mnogih faktora zbog velikog broja dostupnih alata s različitim svrhama, prednostima i manama. Također, korištenjem vanjskih suradnika moguće je provoditi testne kibernetičke napade kako bi se otkrile specifične ranjivosti u kompleksnim sustavima (Brotherston & Berlin, 2017). Opće sigurnosne mjere koje smanjuju broj potencijalnih ranjivosti su:

- Implementacija pouzdanog antivirusnog softvera.
- Odabir pouzdanog web preglednika koji omogućuje upravljanje dopuštenjima .
- Upravljanje aplikacijama i web dodacima poput Adobe PDF reader ili Java te redovito ažuriranje softvera.
- Primjena sigurnosnih ispravaka i ažuriranje sustava.
- Implementacija zaštite mrežnih sustava poput prevenciju upada (IPS), sustava za otkrivanje upada (IDS) i vatrozida.
- Kontinuirana kontrola i filtriranje mrežnih komunikacijskih kanala te zatvaranje nepotrebnih ulaza.
- Šifriranje podataka koji putuju kroz mrežne komunikacijske kanala.
- Korištenje virtualnih privatnih mreža (VPN) za sakrivanje internetskog prometa.
- Kreiranje jakih lozinki i korištenje multifaktorske autentifikacije (Black Kite, 2023; Sood & Enbody, 2014).

### 4.6.5 Virtualizacija

Virtualizacija je proces koji koristi softver za segmentaciju resursa jednog uređaja, poput procesora, memorije i pohrane, na više *virtualnih strojeva (eng. virtual machines)*. Virtualni strojevi pokreću se na zasebnim operativnim sustavima i ponašaju se kao pojedinačni neovisni uređaji koji dijele zajednički hardver za pravilno funkcioniranje. Ova tehnologija omogućuje efikasniju upotrebu hardvera organizacije i ključni je faktor u funkcioniranju cloud sustava (IBM, n.d.). Korištenje virtualizacije ograničava posljedice velikog broja zlonamjernih programa izoliranjem zlonamjernog programa u pojedinačnom virtualnom stroju. Iako postoje zlonamjerni programi koji su razvili mogućnost negiranja prednosti virtualizacije i mogu se širiti na druge virtualne strojeve, takvi kibernetički napadi zahtijevaju visoku razinu sofisticiranosti i resursa. Organizacije mogu koristiti virtualizaciju kako bi ograničile pristup ključnim segmentima informatičkog sustava, implementirajući obvezne postupke za pristup specifičnim virtualnim strojevima (Sood & Enbody, 2014).

### 4.6.6 Plan oporavka

Procjena rizika i kategorizacija podataka u organizaciji ključni su koraci koji omogućuju efektivno postupanje tijekom kibernetičkog napada te smanjenju utjecaj potencijalnih posljedica (Diogenes & Ozkaya, 2022). Kategorizacija podataka stvara informacijsku podlogu koja pruža podršku u odlučivanju. U slučajevima kada organizacije procijene da će popravak određenih ranjivosti ili povratak informacija stvoriti veće troškove od onih uzrokovanih kibernetičkih napadima, mogu se odlučiti za prihvaćenje posljedica ili rizika (Brotherston & Berlin, 2017). Prihvaćenje rizika trebalo bi predstavljati posljednju mjeru, a organizacije bi trebale implementirati plan oporavka koji uključuje jasno definirane uloge i odgovornosti, komunikacijske protokole i strategije oporavka (Black Kite, 2023). Uspješni planovi oporavka dizajnirani su tako da omogućuju efektivnu reakciju u što kraćem vremenskom roku kako bi se spriječile daljnje posljedice kibernetičkih napada. Razumijevanje mjesta pohrane određenih vrsta podataka, ugrađenih sigurnosnih mjera i uloga korisnika s određenim razinama ovlasti ključno je za izradu planova oporavka (Sood & Enbody, 2014). Nedostatak planova oporavka je potreba za stalnim ažuriranjem, što stvara dodatne troškove za organizaciju (Diogenes & Ozkaya, 2022).

# 5. EMPIRIJSKO ISTRAŽIVANJE NAJVEĆIH KIBERNETIČKIH NAPADA

## 5.1. Ciljevi istraživanja

U ovom poglavlju opisani su detalji provedenog empirijskog istraživanja najvećih kibernetičkih napada. Istraživanje se klasificira kao eksplorativna analiza podataka, čija je primarna svrha stvoriti informacijsku podlogu za otkrivanje obrazaca te stjecanje novih uvida u kombinaciji s teorijskim dijelom ovog akademskog rada upotrebom deskriptivne statistike. Glavni cilj istraživanja je istaknuti prijetnje koje predstavljaju kibernetički napadi, a koje nisu ograničene na specifične vremenske periode niti na pojedinačne djelatnosti u privatnom sektoru. Ovaj glavni cilj ostvaruje se koncentracijom na specifičnije ciljeve koji uključuju:

- Identifikacija različitih djelatnosti privatnog sektora na kojima su provedeni uspješni kibernetički napadi.
- Analiza broja napada u različitim djelatnostima privatnog sektora.
- Analiza primarnih uzroka uspješnih kibernetičkih napada.
- Analiza uspješnih kibernetičkih napada kroz različita vremenska razdoblja.

## 5.2 Metodologija empirijskog istraživanja

U istraživanju su korišteni sekundarni podaci prikupljeni iz različitih internetskih izvora za provedbu empirijskog istraživanja. Prikupljanje podataka o kibernetičkim napadima nosi određena ograničenja koja je važno uzeti u obzir pri analizi ovog istraživanja. Prvo, nije moguće obuhvatiti sve incidente kibernetičkih napada. Kao što je već opisano u radu, podaci o kibernetičkim napadima su znatno raspršeni i nestandardizirani te ne postoje adekvatni skupovi podataka koji obuhvaćaju sve kibernetičke napade. Veliki broj kibernetičkih napada u privatnom sektoru nije objavljen na internetskim izvorima. Također, mnogi povijesni kibernetički napadi nisu zabilježeni ili još nisu ni otkriveni. Uz to, velika raspršenost podataka rezultira podacima u različitim oblicima s neusklađenim klasifikacijama, što otežava jedinstvenu analizu. Svi izvještaji o kibernetičkoj sigurnosti koji koriste skupove podataka, kao i sami skupovi podataka o kibernetičkim napadima, imaju određena ograničenja koja je važno uzeti u obzir prije analize podataka.

Kako bi se stvorila informacijska podloga za ostvarenje ciljeva ovog istraživanja, postavljeni su određeni kriteriji za prikupljanje i obradi podataka. Navedeni kriteriji su sljedeći:

- U istraživanju će se koristiti samo javno dostupni skupovi podatka. Ovaj kriterij je neizbježan zbog nemogućnosti nabave i upotrebe nedostupnih podataka.

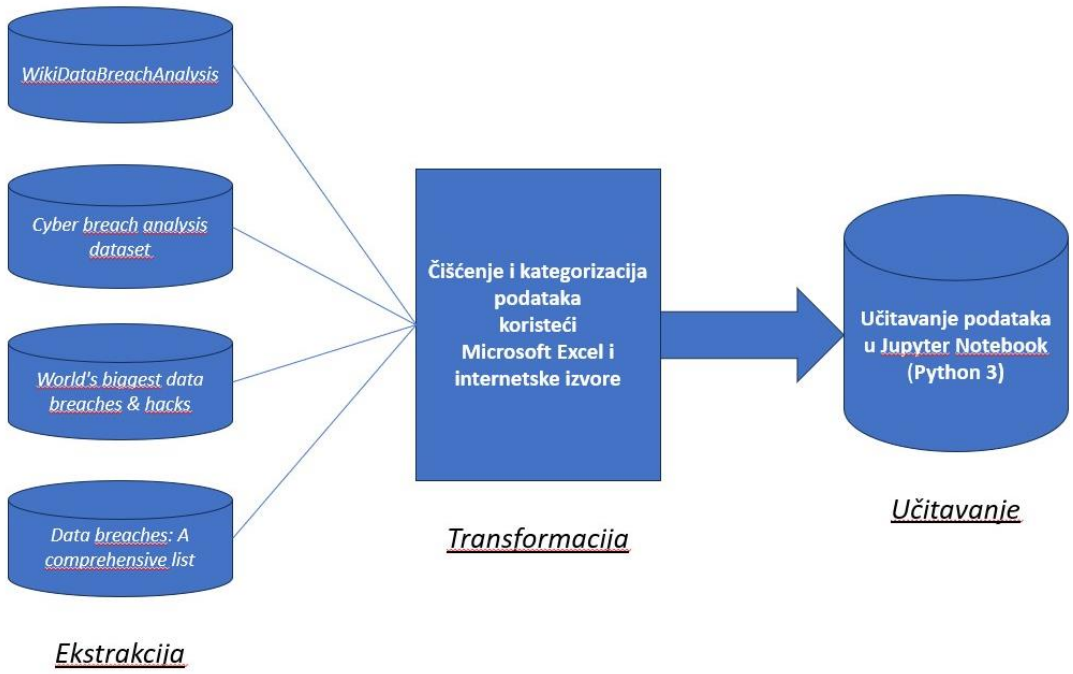
- Skupovi podataka moraju sadržavati: naziv organizacije nad kojom su provedeni kibernetički napadi, godinu u kojoj su napadi provedeni ili otkriveni te kategorizaciju ili opis vrste kibernetičkog napada.
- Svaka upotrijebljena instanca u skupovima podataka mora imati legitimni izvor. Svi podaci korišteni u istraživanju imaju različite vrste digitalnog medijskog pokrića i pripadajuće izvore podataka.
- Skupovi podataka moraju sadržavati broj izgubljenih zapisa u kibernetičkom napadu. Ovaj kriterij je odabran kao mjerna jedinica koja preciznije prikazuje posljedice kibernetičkog napada od memorijske veličine izgubljenih podataka ili procijenjene novčane vrijednosti. Izgubljeni zapisi odnose se na različite vrste podataka, poput lozinki, korisničkih računa ili poslovnih tajni. Važno je napomenuti da brojevi prijavljeni u medijima mogu biti generalizirani ili procijenjeni.

Primjenom ovih kriterija pronađena su četiri skupa podataka koja zadovoljavaju sve kriterije. Za kombinaciju različitih podataka iz različitih izvora u jedinstvenu cjelinu korišten je ETL proces koji je prikazan u *Grafičkom prikazu 1*. ETL proces se odvija u tri ključna koraka: ekstrakcija, transformacija te učitavanje (IBM, n.d.). Prvi korak, ekstrakcija, odnosi se na prikupljanje podataka iz različitih izvora. U ovom istraživanju ekstrakcija se odnosi na četiri navedena skupa podataka pronađena na različitim internetskim izvorima. Nadalje, proveden je korak transformacije, u kojem su prikupljeni skupovi podataka kombinirani u jednu cjelinu korištenjem Microsoft Excela. Jedinstveni skup prikazuje kibernetičke napade na globalnoj razini u vremenskom razdoblju od 2004. do 2024. godine. Početni skup sadržavao je 1964 pojedinačnih slučajeva kibernetičkih napada. Korištenjem izvora od kojih potječu instance kibernetičkih napada te dodatnim pretraživanjem novih internetskih izvora, kibernetički napadi razvrstani su u opće kategorije koje su omogućile daljnje čišćenje podataka. Skup podataka početno je očišćen od kibernetičkih napada koji se odnose na javni sektor, s obzirom na to da je fokus akademskog rada na organizacijama privatnog sektora. Također, uklonjene su duplicirane instance i povezani događaji koji se odnose na iste kibernetičke napade. Djelatnosti unutar privatnog sektora kategorizirane su kao: društveni mediji, financije, maloprodaja i e-trgovina, obrazovanje, prijevoz, tehnologija, telekomunikacije, zabava i mediji, zdravstvo te ostalo. Vrste napada prikazuju primarni uzrok koji je omogućio izvedbu kibernetičkog napada i kategorizirane su kao: hakirani, izgubljeni uređaj, loša sigurnosna zaštita, namjerno izgubljeno, nepoznato, slučajna greška, unutarnja prijetnja. Kategorija „hakirani“ opisuje postupke kibernetičkog napadača kao primarni uzrok, dok kategorija „loša sigurnosna zaštita“ ističe upotrebu postojećih ranjivosti, bez kojih napad ne bi bio moguć. Kategorija „slučajna greška“ uključena je jer su te greške omogućile napadačima provedbu neprijateljskih radnji i kibernetičkih napada. Nakon čišćenja podataka, u skupu je ostalo 1147

kibernetičkih napada, koji su korišteni u empirijskom istraživanju. Konačno, proveden je zadnji korak učitavanja, koji je uključivao učitavanje očišćenog skupa podataka u radnu okolinu Jupyter Notebook. Radna okolina se temeljila na programskom jeziku Python 3, koji je omogućio korištenje biblioteke Pandas za detaljnu analizu kibernetičkih napada u skupu podataka. Pomoću biblioteke Pandas provedene su tehnike deskriptivne statistike, a izračuni grafički prikazani upotrebom biblioteka Matplotlib i Seaborn.

**Grafički prikaz 1.**

*Vizualizacija ETL procesa*




Izvor: Prikaz autora

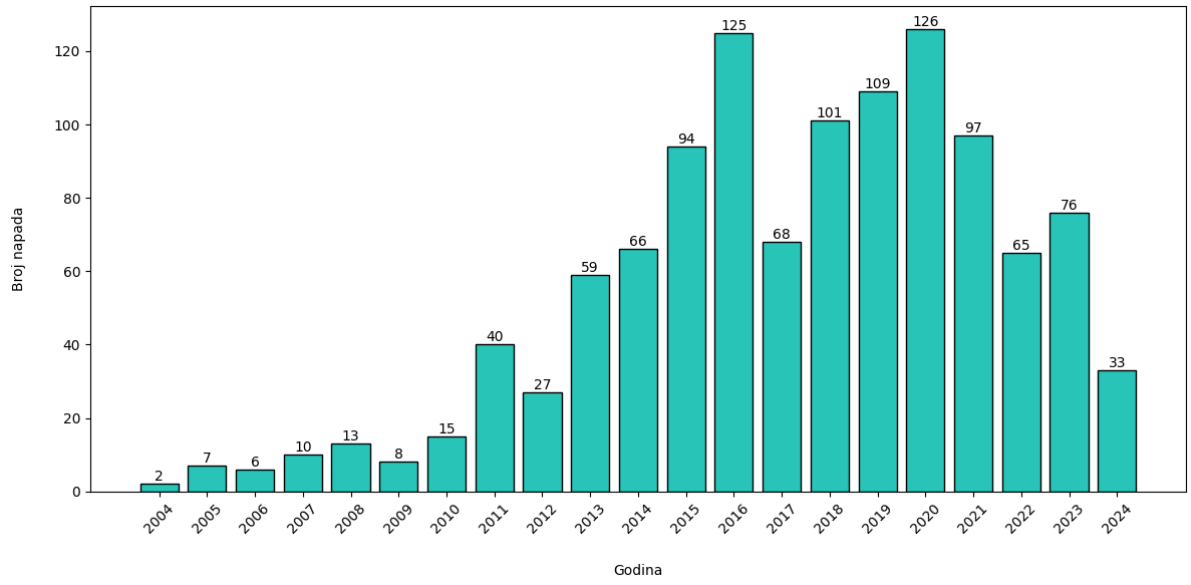
## 6. REZULTATI ISTRAŽIVANJA

U ovom poglavlju predstavljeni su rezultati empirijskog istraživanja provedenog na uzorku od 1147 kibernetičkih napada koji zadovoljavaju prethodno opisane kriterije.

*Grafički prikaz 2*. prikazuje raspodjelu pojedinačnih kibernetičkih napada po godinama u razdoblju od 2004. do 2024. godine. Godine u vremenskom razdoblju od 2004. do 2010. sadrže najmanji broj kibernetičkih napada u skupu podataka. Razdoblje od 2013. do 2023. godine bilježi značajno veći broj kibernetičkih napada, s najvećim brojem napada u 2016. i 2020. godini, kada su zabilježena 126 jedinstvena kibernetička napada koja zadovoljavaju postavljene kriterije. Godina 2024. bilježi manji broj kibernetičkih napada u usporedbi s prethodnim godinama, što je uzrokovano datumom provedenog istraživanja te trendom da se veliki broj kibernetičkih napada otkriva ili službeno prijavljuje tek kasnije.

**Grafički prikaz 2.**

*Broj kibernetičkih napada po godinama*

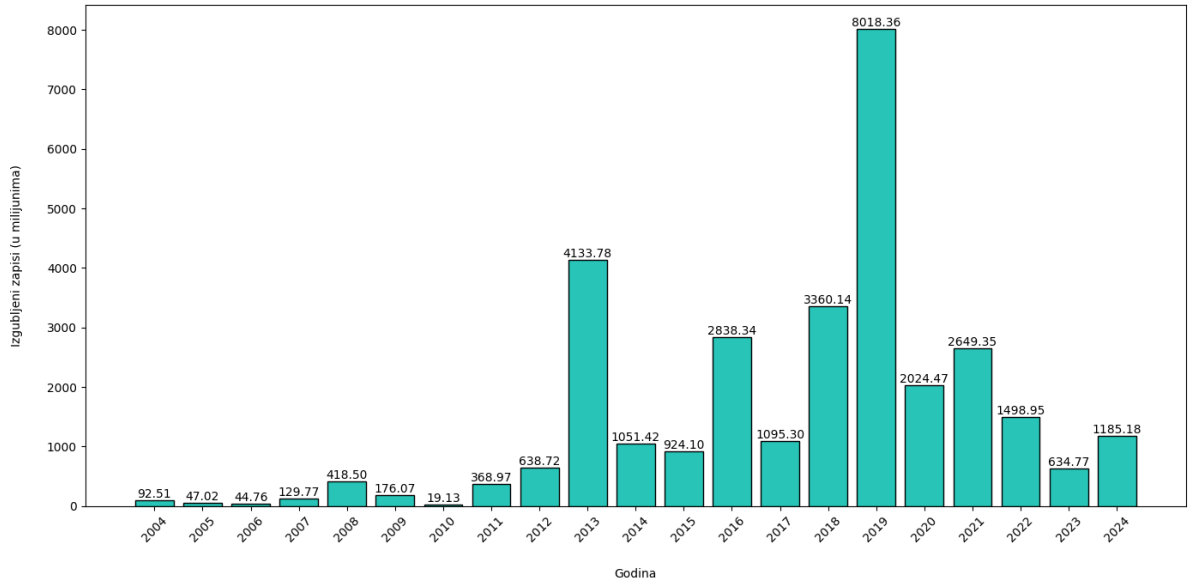



Izvor: Prikaz autora

*Grafički prikaz 3.* prikazuje broj izgubljenih zapisa po pojedinačnim godinama. Uočljivo je da broj izgubljenih zapisa nije izravno povezan s brojem napada u skupu podataka ,što ukazuje na prisutnost različitih kibernetičkih napada s različitim posljedicama. Godine 2013. i 2019. bilježe najveći broj izgubljenih zapisa, što je povezano s najvećim kibernetičkim napadima prikazanim u *Grafičkom prikazu 4.* Nad organizacijom Yahoo je 2013. godine proveden najveći kibernetički napad u povijesti koji je uzrokovao curenje 3 milijarde zapisa s osjetljivim informacijama krajnjih korisnika. Nadalje, 2019. godine se dogodilo više kibernetičkih napada koji se smatraju jednim od najvećih u povijesti, što uključuje organizacije: „Verifications.io“ čija je primarna djelatnost bila provjera valjanosti e-mail adresa, društvena platforma „Facebook“ te „First America Corporation“ organizacija za osiguranje nekretnina.

**Grafički prikaz 3.**

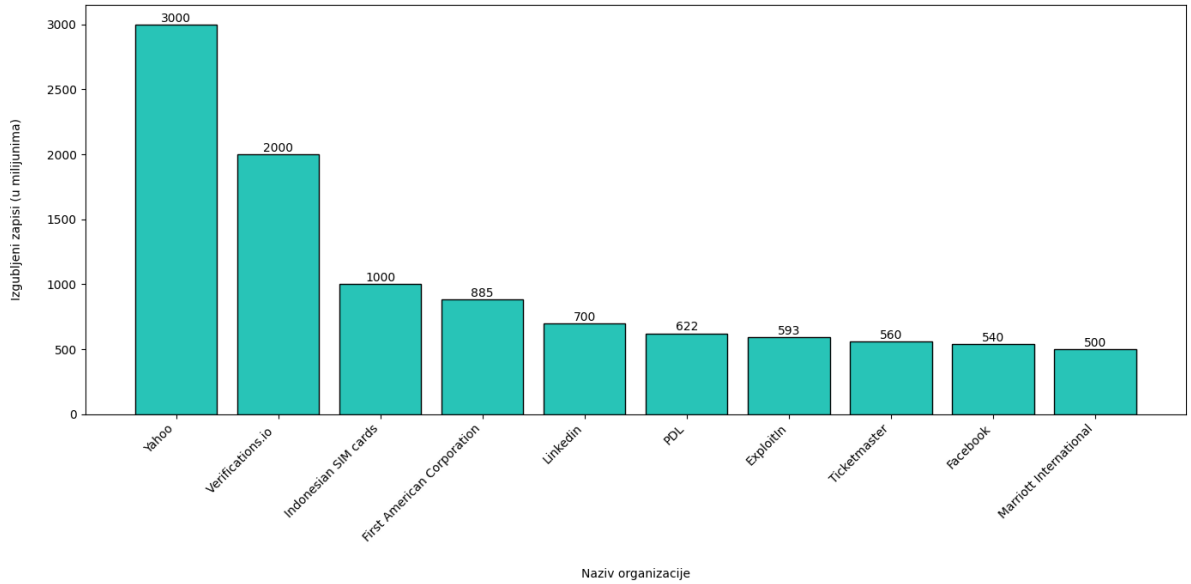
*Broj izgubljenih zapisa po godinama*




Izvor: Prikaz autora

**Grafički prikaz 4.**

*Najveći kibernetički napadi po broju izgubljenih zapisa*

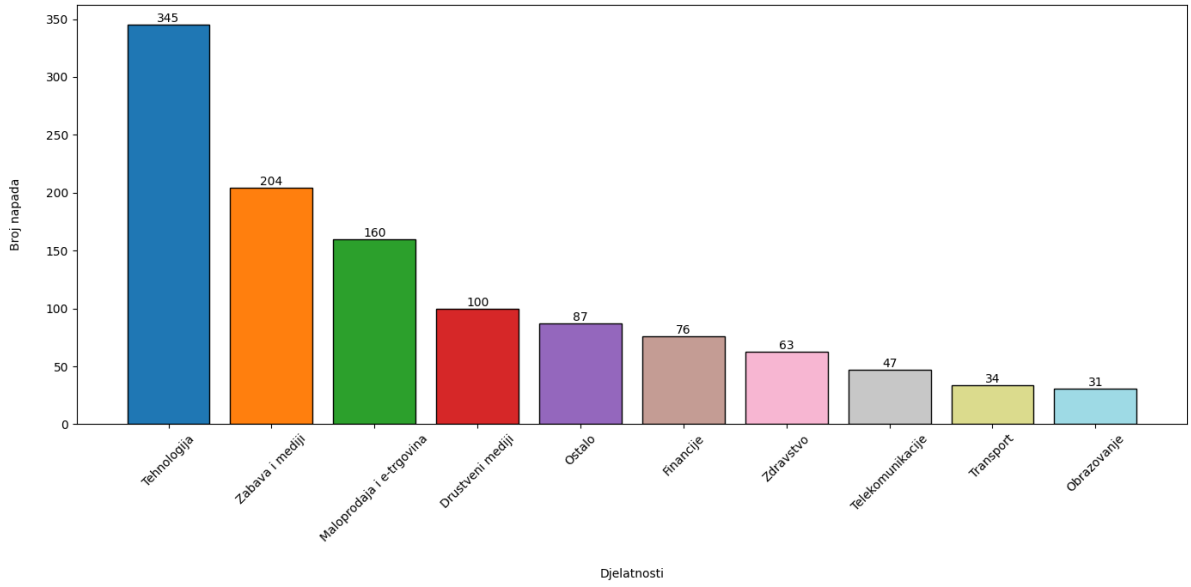



Izvor: Prikaz autora

*Grafički prikaz 5.* prikazuje broj jedinstvenih kibernetičkih napada raspoređenih po općoj kategorizaciji djelatnosti. Skup podataka sadrži najviše kibernetičkih napada u organizacijama čija je primarna djelatnost „Tehnologija“, koja obuhvaća široki spektar pojmova, uključujući digitalne platforme, online usluge, komunikacijske tehnologije i umjetnu inteligenciju. Organizacije sa značajnim brojem jednakih specifičnijih kategorizacija su smještene u zasebne djelatnosti kako bi se prikazali precizniji rezultati.

**Grafički prikaz 5.**

*Broj napada po djelatnostima*

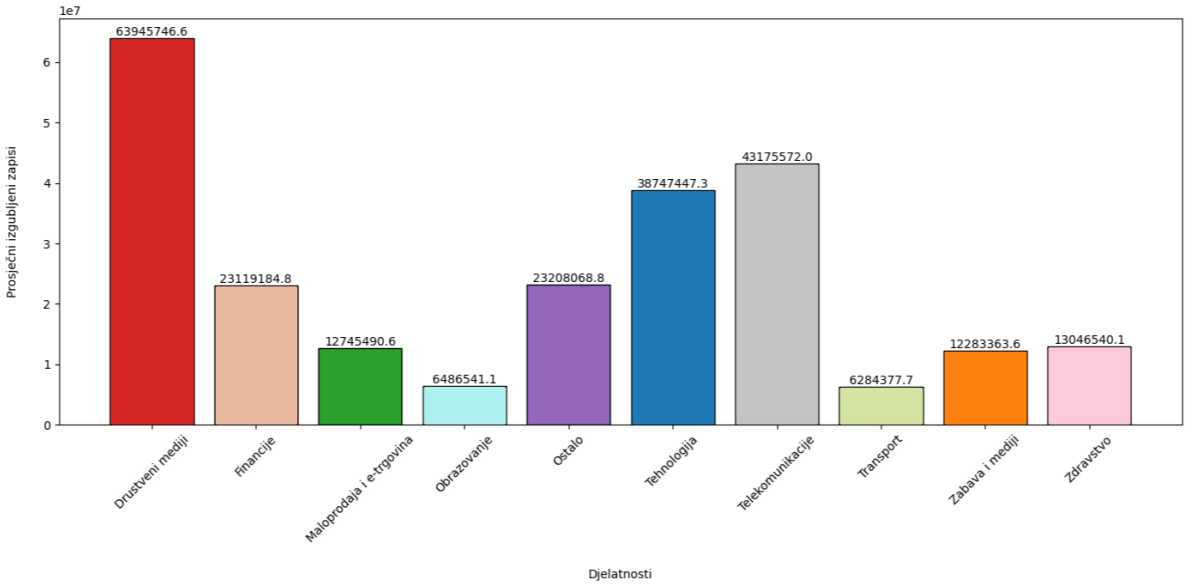



Izvor: Prikaz autora

U *Grafičkom prikazu 6.* su prikazane prosječne vrijednosti izgubljenih zapisa po specifičnim djelatnostima. Kao što je prethodno navedeno, broj izgubljenih zapisa nije izravno povezan s brojem napada, što je vidljivo iz činjenice da djelatnosti poput „Društveni mediji“ i „Telekomunikacije“ imaju znatno veći broj izgubljenih zapisa, iako djelatnosti „Tehnologija“ i „Zabava i mediji“ bilježe značajno veći broj napada u skupu podataka.

**Grafički prikaz 6.**

*Prosječni broj izgubljenih zapisa po djelatnosti*

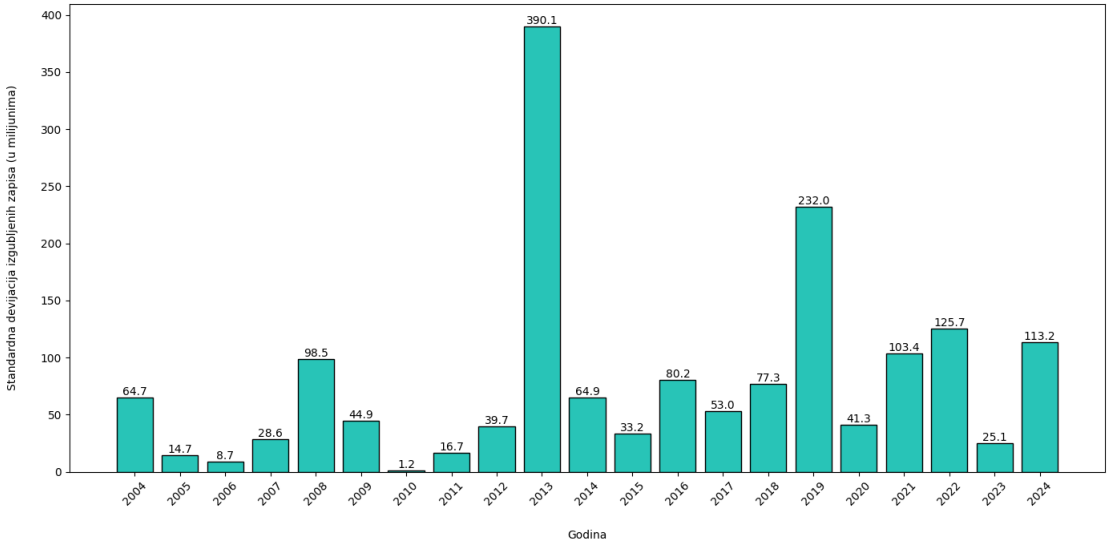



Izvor: Prikaz autora

Standardna devijacija prikazana u *Grafičkom prikazu 7*. koristi se kao dodatna metoda kontrole rezultata prikazanih u *Grafičkom prikazu 4.* Kao što je već prethodno navedeno, standardna devijacija je značajno veća u 2013. i 2019. godini jer ove godine uključuju veliki broj najvećih kibernetičkih napada u povijesti.

**Grafički prikaz 7.**

*Standardna devijacija izgubljenih zapisa po godinama*

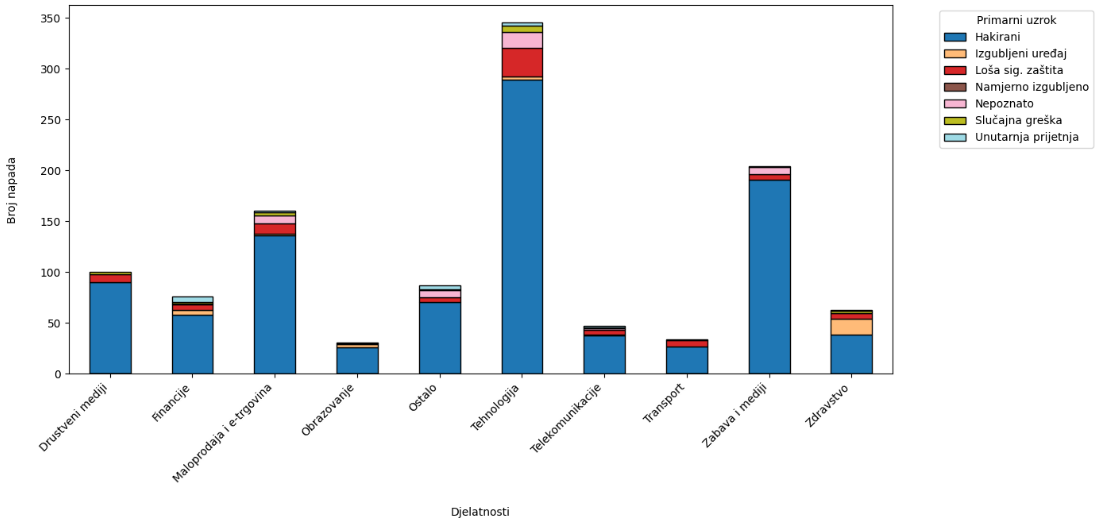



Izvor: Prikaz autora

Na kraju, provedena je analiza primarnih uzroka koji su omogućili provedbu kibernetičkih napada, a rezultati su prikazani u *Grafičkom prikazu 8*. Prevladavajući primarni uzrok je „hakirani“ što označava aktivnosti napadača kao ključni element bez kojeg ne bi bilo moguće uspješno provesti kibernetički napad, bez obzira na postojeće ranjivosti. Uzrok „loša sigurnosna zaštita“ usko je povezan s uzrokom „hakirani“ jer veliki broj kibernetičkih napada iskorištava postojeće ranjivosti za provedbu napada, što povećava vjerojatnost uspjeha. Konačno, djelatnost „zdravstvo“ sadrži značajan broj kibernetičkih napada koji su se temeljili na podacima iz izgubljenih uređaja.

**Grafički prikaz 8.**

*Primarni uzrok po djelatnostima*




Izvor: Prikaz autora

# 7. RASPRAVA

Analizom rezultata istraživanja i grafova prikupljeni su različiti podaci koji, u kombinaciji s teorijskim dijelom rada, omogućuju stvaranje opsežnije informacijske podloge s novim opažanjima. Iako je istraživanje ograničeno upotrebom namjernog uzorkovanja, što može uvesti pristranost u istraživanje, postavljeni kriteriji bili su nužni za analizu podataka te su omogućili izradu skupa podataka iz znatno raspršenih izvora.

Isprva, uočeno je da vremensko razdoblje od 2004. do 2010. godine sadrži značajno manje zabilježenih kibernetičkih napada, čak i nakon kombinacije različitih izvora informacija. Uzrok ove pojave može se objasniti činjenicom da je domena kibernetičke sigurnosti počela dobivati značajnu popularnost na globalnoj razini tek početkom 1990-ih godina, što karakterizira kibernetičke napade u navedenom razdoblju kao neistražene pojmove čija se važnost tek počela isticati (Aslan et al., 2023). Nadalje, u 2024. godini uočen je porast korištenja vrlo starih metoda izvedbe kibernetičkih napada, čije su prednosti nedostatak dostupnih informacija te mogućnost izbjegavanja detekcije (Google Cloud, 2023).

Obradom podataka o izgubljenim zapisima u kibernetičkim napadima, nije uočena izravna povezanost između broja napada i djelatnosti organizacije s brojem izgubljenih zapisa. Ovo opažanje ipak potvrđuje činjenicu da raznovrsne djelatnosti unutar privatnog sektora mogu biti ciljane kibernetičkim napadima, što može uzrokovati posljedice različite značajnosti. Organizacije čiji ključni poslovni procesi ovise o tehnologiji imaju najveći broj izgubljenih zapisa i najveći broj napada. Ovaj nalaz ističe razvoj tehnologije, koji je prethodno opisan kao jedan od uzroka kibernetičkih napada, jer doprinosi povećanju ovisnosti organizacija o tehnologiji, stvarajući više prilika koje kibernetički napadači mogu iskoristiti.

Konačno, utvrđeno je da je primarni uzrok uspješno provedenih kibernetičkih napada "hakiranje", što odgovara sigurnosnim izvještajima koji opisuju organizirane hakerske grupe kao jedan od najzastupljenijih uzroka uspješnih kibernetičkih napada (CrowdStrike, 2024; Office of the National Cyber Director, 2024; European Union Agency for Cybersecurity, 2023; Google Cloud, 2023; Verizon, 2024; World Economic Forum, 2024).

# 8. ZAKLJUČAK

U ovom radu analizirani su uzroci i karakteristike kibernetičkih napada u privatnom sektoru, s posebnim naglaskom na njihove motive, metode i posljedice. Kibernetički napadi predstavljaju sve veću prijetnju organizacijama zbog stalnog razvoja tehnologije i povećane ovisnosti o digitalnim sustavima. Iako kibernetički napadi postaju sve značajniji na globalnoj razini, informacije o njima su često raspršene i nedovoljno standardizirane. U radu su, koristeći različite izvore, ponuđena detaljna objašnjenja ključnih pojmova potrebnih za razumijevanje kibernetičkih napada i okruženja u kojem se događaju.

Analizom je utvrđeno da su ljudske greške, ranjivosti informatičkih sustava i ubrzani razvoj tehnologije ključni faktori koji doprinose uspješnosti kibernetičkih napada. Ljudski faktor, uključujući neadekvatnu obuku i nepažnju krajnjih korisnika, često je presudan u stvaranju ranjivosti koje napadači iskorištavaju. Uz to, razvoj novih tehnologija, poput umjetne inteligencije i računarstva u oblaku, stvorio je dodatne izazove u području kibernetičke sigurnosti.

Razmotreni su različiti motivi koji omogućuju dublje razumijevanje razloga zbog kojih se kibernetički napadi događaju, pri čemu je financijska dobit istaknuta kao dominantan cilj koji motivira napadače. Ovaj motiv često uključuje sporedne ciljeve, kao što su ideološki razlozi ili znatiželja. Također, istaknuti su uvjeti koji olakšavaju pojedincima da postanu kibernetički napadači, poput dostupnosti potrebnih alata i informacija te niskih financijskih prepreka za provedbu napada. Organizirane hakerske grupe identificirane su kao ključni akteri koji provode kibernetičke napade, a opisane su i psihološke karakteristike napadača koje ove grupe mogu iskoristiti za povećanje broja svojih članova.

U radu su također dane detaljne definicije zlonamjernih programa koji se koriste kao digitalni alati za provedbu kibernetičkih napada te su opisane različite metode napada. Ove metode iskorištavaju različite ranjivosti, od ljudskih slabosti putem socijalnog inženjeringa do tehnoloških napada poput napada uskraćivanjem usluge (DoS), koji preopterećuju sustave velikom količinom podataka. Opisane su i potencijalne posljedice kibernetičkih napada, koje osim izravnih financijskih troškova popravka sustava uključuju i mnoge neizravne troškove, poput gubitka dionika, pogoršanja reputacije brenda ili jačanja konkurencije. Na kraju su navedeni glavni principi kibernetičke sigurnosti i predložene opće sigurnosne mjere koje smanjuju vjerojatnost uspješnog napada.

Empirijsko istraživanje provedeno u ovom radu dodatno je potvrdilo teorijske uvide. Analizom 1147 slučajeva kibernetičkih napada identificirani su ključni obrasci koji pokazuju da su različite djelatnosti u privatnom sektoru česte mete kibernetičkih napada. Istraživanje je istaknulo značajne posljedice koje ovi napadi mogu uzrokovati te je naglašena potreba za većim ulaganjem u kibernetičku sigurnost

u svim djelatnostima privatnog sektora. Rezultati empirijskog istraživanja pokazuju da je proaktivan pristup ključan u smanjenju rizika te da je neophodno kontinuirano praćenje i prilagodba strategija sigurnosti u skladu s brzim razvojem tehnologije i promjenjivim krajolikom prijetnji.

Konačno, analizom perspektiva i obilježja različitih entiteta koji utječu na kibernetičke napade, ostvaren je primarni cilj rada, a to je pružanje sveobuhvatnih informacija o kibernetičkim napadima koje se mogu primijeniti u organizacijama privatnog sektora. Također, stvorena je široka informacijska podloga koja obuhvaća različite teme i koja može poslužiti kao početna točka za detaljnije istraživanje pojedinačnih aspekata kibernetičkih napada. Podaci iz ovog rada mogu olakšati pronalazak novih uvida koji možda ne bi bili uočljivi kada bi se istraživanje usmjerilo samo na specifični dio kibernetičke sigurnosti.

## LITERATURA


Abdi, A., Bennouri, H., & Keane, A. (2024). Cyber resilience, risk management, and security challenges in enterprise-scale cloud systems: Comprehensive review. *Proceedings of the 2024 13th Mediterranean Conference on Embedded Computing (MECO)* (str. 1-8). IEEE. https://doi.org/10.1109/MECO62516.2024.10577956

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet, 12*(10), 168. https://doi.org/10.3390/fi12100168

Alhebshi, R. M., Ahmed, N., Baleanu, D., Fatima, U., Dayan, F., Rafiq, M., Raza, A., Ahmad, M. O., & Mahmoud, E. E. (2023). Modeling of computer virus propagation with fuzzy parameters. *Computers, Materials & Continua, 74*(3), 5663-5678. https://doi.org/10.32604/cmc.2023.033319

Alkhalil, Z., Hewage, C., Liqaa, N., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*. https://doi.org/10.3389/fcomp.2021.563060

Amoo, O., Amoo, O., Osasona, F., Atadoga, A., Ayinla, B., Farayola, O., & Abrahams, T. (2024). Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive, 11*, 1304-1310. https://doi.org/10.30574/ijsra.2024.11.1.0217

Anu, P., & Vimala, S. (2017). A survey on sniffing attacks on computer networks. *Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2)* (str. 1-5). IEEE. https://doi.org/10.1109/I2C2.2017.8321914

Aslan, Ö., Aktug, S., Ozkan Okay, M., Yılmaz, A., & Akin, E. (2023*). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions*. *Electronics, 12*, 1-42. https://doi.org/10.3390/electronics12061333

Atmojo, Y. P., Susila, I. M. D., Hilmi, M. R., Rini, E. S., Yuningsih, L., & Hostiadi, D. P. (2021). A new approach for spear phishing detection. *Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)* (str. 49-54). IEEE. https://doi.org/10.1109/EIConCIT50028.2021.9431890

Black Kite. (2023). *Ransomware threat landscape report: Ransomware resurgence 2023 – Emerging trends, threat actors, and cybersecurity strategies*. Black Kite. https://blackkite.com/wp-content/uploads/2023/04/2023_Ransomware_Report_Black_Kite.pdf

Brotherston, L., & Berlin, A. (2017). *Defensive security handbook: Best practices for securing infrastructure*. O'Reilly Media.

Bull Jr., C. L. (2024). *Assignment 2.1: The 2016 Bangladesh Bank heist*. School of Professional & Continuing Education, University of San Diego. https://www.craigbullsecurity.com/uploads/1/4/8/2/148291237/assignment_2.1_-_the_2016_bangladesh_bank_heist_-_craig_bull.pdf

Campbell, N. A., Urry, L. A., Cain, M. L., Wasserman, S. A., Minorsky, P. V., & Reece, J. B. (2018). *Campbell biology* (11th ed.). Pearson Education Limited.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The economic impact of cyber-attacks* (CRS Report No. RL32331). Government and Finance Division, Congressional Research Service. https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf

Chai, W., & Rosencrance, L. (2024). *Hacker*. *TechTarget*. Pregledano 15. kolovoza 2024, s https://www.techtarget.com/searchsecurity/definition/hacker

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports, 5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Cloudflare. (2024). *What is a supply chain attack?* Pregledano 15. kolovoza 2024. s https://www.cloudflare.com/learning/security/what-is-a-supply-chain-attack/

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(6), 13-21. https://doi.org/10.22215/timreview/835

CrowdStrike. (2024). *2024 global threat report*. CrowdStrike. https://www.crowdstrike.com/global-threat-report/

De Becker, G. (2000). *The gift of fear: Survival signals that protect us from violence*. Bloomsbury Publishing.

Department of Defense. (2006). *National Military Strategy for Cyberspace Operations*. Washington, D.C.: Chairman of the Joint Chiefs of Staff.

Diogenes, Y., & Ozkaya, E. (2022). *Cybersecurity – Attack and defense strategies* (3rd ed.). Packt Publishing. https://www.packt.com

Duessel, P., Luo, S., Flegel, U., Dietrich, S., & Meier, M. (2020). Tracing privilege misuse through behavioral anomaly detection in geometric spaces. *Proceedings of the 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)* (str. 22-31). IEEE. https://doi.org/10.1109/SADFE51007.2020.00012

Dusane, P. S., & Pavithra, Y. (2020). Logic bomb: An insider attack. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(3), 926–931. https://doi.org/10.30534/ijatcse/2020/176932020

Đeraj, A. (2023). *Akademski kriminal u kontekstu kriminala bijelog ovratnika* (Završni rad). Sveučilište u Zagrebu, Pravni fakultet. https://urn.nsk.hr/urn:nbn:hr:199:894465

El Moussaid, N. E., & Toumanari, A. (2014). Web application attacks detection: A survey and classification. *International Journal of Computer Applications, 103*, 1-6. https://doi.org/10.5120/18123-9085

Elleithy, K. M., Blagovic, D., Cheng, W. K., & Sideleau, P. (2005). Denial of service attack techniques: Analysis, implementation and comparison. *Journal of Systemics, Cybernetics, and Informatics, 3*(1), 66–71.

European Union Agency for Cybersecurity, Lella, I., Ciobanu, C., Tsekmezoglou, E., Theocharidou, M., Magonara, E., Malatras, A., Svetozarov Naydenov, R., & Tsekmezoglou, E. (Ur.). (2023). *ENISA threat landscape 2023 – July 2022 to June 2023*. European Union Agency for Cybersecurity. https://data.europa.eu/doi/10.2824/782573

Freeman, G., Guo, J., & Jacob, E. (2011). Places for digital ecosystems, digital ecosystems in places. *Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES'11)* (str. 145-149). Association for Computing Machinery. https://doi.org/10.1145/2077489.2077516

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *Technology and Society Magazine, IEEE, 30*(1), 28–38. https://doi.org/10.1109/MTS.2011.940293

Garg, D., & Gill, R. (2023). Deepfake generation and detection - An exploratory study. *2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer*

*Engineering (UPCON)* (str. 888-893). IEEE. https://doi.org/10.1109/UPCON59197.2023.10434896

Gastellier-Prevost, S., & Laurent, M. (2011). Defeating pharming attacks at the client-side. *2011 5th International Conference on Network and System Security* (str. 33-40). IEEE. https://doi.org/10.1109/ICNSS.2011.6059957

Gautam, T. (2024). Study of password cracking methodologies. *International Journal of Fuzzy Logic and Design, 9*(1), 26–36.

Google Cloud. (2023). *Cybersecurity forecast 2024: Insights for future planning*. Google LLC. https://services.google.com/fh/files/misc/google-cloud-cybersecurity-forecast-2024.pdf

Google Cloud. (2024). *Artificial intelligence (AI) vs. machine learning (ML)*. Google LLC. https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning?hl=en

Gragido, W., Molina, D., Pirc, J., Selby, N., & Hay, A. (Technical Ed.). (2013). *Blackhatonomics: An inside look at the economics of cybercrime*. Syngress, an imprint of Elsevier.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence, 36*(1). https://doi.org/10.1080/08839514.2022.2037254

Harry, C. (2015). *A framework for categorizing disruptive cyber activity and assessing its impact* (CISSM Working Paper). Center for International Security Studies at Maryland, University of Maryland, School of Public Policy. https://cissm.umd.edu/sites/default/files/2019-07/CategorizingDisruptiveCyberActivity%20-%20080615.pdf

Heinbockel, W. J., Laderman, E. R., & Serrao, G. J. (2017). *Supply chain attacks and resiliency mitigations: Guidance for system security engineers* (MITRE Technical Report MTR170477). The MITRE Corporation. https://www.mitre.org/sites/default/files/2021-11/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf

Herley, C., & Florêncio, D. (2008). Protecting financial institutions from brute-force attacks. U S. Jajodia, P. Samarati, & S. Cimato (Ur.), *Proceedings of the IFIP TC 11 23rd International Information Security Conference. SEC 2008* (Vol. 278, str. 357–368). Springer. https://doi.org/10.1007/978-0-387-09699-5_45

Hossain, M., Khan, R., Noor, S. A., & Hasan, R. (2016). Jugo: A generic architecture for composite cloud as a service. *Proceedings of the 2016 IEEE 9th International Conference on Cloud Computing (CLOUD)* (str. 806-809). IEEE. https://doi.org/10.1109/CLOUD.2016.0112

IBM. (2024). *What is the Internet of Things (IoT)?* IBM. Pregledano 15. kolovoza 2024, s https://www.ibm.com/topics/internet-of-things.

IBM. (n.d.). *Što je virtualizacija?* IBM. Pregledano 15. kolovoza 2024, s https://www.ibm.com/topics/virtualization

IBM. (n.d.). *What is ETL?* IBM. Pregledano 15. kolovoza 2024, s https://www.ibm.com/topics/etl

Javaheri, D., Hosseinzadeh, M., & Rahmani, A. M. (2018). Detection and elimination of spyware and ransomware by intercepting kernel-level system routines. *IEEE Access, 6*, 78321–78332. https://doi.org/10.1109/ACCESS.2018.2884964

Kaspersky Lab. (2024). *Ransomware attacks and types – How encryption trojans differ*. Pregledano 15. kolovoza 2024, s https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Kaspersky Lab. (2024). *Threat landscape*. Encyclopedia Kaspersky. Pregledano 15. kolovoza 2024, s https://encyclopedia.kaspersky.com/glossary/threat-landscape/

Kaspersky Lab. (2024). *What is cryptocurrency and how does it work?* Kaspersky. Pregledano 15. kolovoza 2024, s https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.

Kim, D., & Solomon, M. G. (2018). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning.

Kosseff, J. (2020). *Cybersecurity law* (2nd ed.). John Wiley & Sons, Inc.

Kulshrestha, A., & Dubey, S. K. (2014). A literature review on sniffing attacks in computer network. *International Journal of Advanced Engineering Research and Science (IJAERS)*, *1*(2), 67-73. ISSN: 2349-6495.

Lewis, J., & Baker, S. (2013). *The economic impact of cybercrime and cyber espionage*. Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

Li, P., Salour, M., & Su, X. (2008). A survey of internet worm detection and containment. *IEEE Communications Surveys & Tutorials, 10*(1), 20-35. https://doi.org/10.1109/COMST.2008.4483668

Li, W., Badr, Y., & Biennier, F. (2012). Digital ecosystems: Challenges and prospects. In *Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES 2012)* (str. 117-122). Association for Computing Machinery. https://doi.org/10.1145/2457276.2457297

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lim, A. (2023, 22. kolovoza). *An executive view of key cybersecurity trends and challenges in 2023*. ISACA. Pregledano 15. kolovoza 2024, s https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023

Lim, A. (2024, 5. veljače). *The true cost of cyber attacks in 2024 and beyond*. ExpressVPN. Pregledano 15. kolovoza 2024, s https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

Lobo, D., Watters, P., & Wu, X.-W. (2010). A new procedure to help system/network administrators identify multiple rootkit infections. *Proceedings of the 2010 Second International Conference on Communication Software and Networks* (str. 124–128). IEEE. https://doi.org/10.1109/ICCSN.2010.14

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity, 7*(1), 1–8. https://doi.org/10.1093/cybsec/tyab021

Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News, 190*(1), 1-69. https://worldscientificnews.com/navigating-the-cyber-security-landscape-a-comprehensive-review-of-cyber-attacks-emerging-trends-and-recent-developments/

Malwarebytes. (2024). *What is a backdoor?* Pregledano 15. kolovoza 2024, s https://www.malwarebytes.com/backdoor

Mirza, A. M., Fernando, Y., Mergeresa, F., Wahyuni-Td, I. S., Ikhsan, R. B., & Fernando, E. (2023). Psychological risk, security risk and perceived risk of the cryptocurrency usage. In *Proceedings of the 2023 IEEE 9th International Conference on Computing, Engineering and Design (ICCED)* (str. 1-5). IEEE. https://doi.org/10.1109/ICCED60214.2023.10425190

Mitropoulos, D., Louridas, P., Polychronakis, M., & Keromytis, A. D. (2019). Defending against web application attacks: Approaches, challenges and implications. *IEEE Transactions on Dependable and Secure Computing, 16*(2), 188-203. https://doi.org/10.1109/TDSC.2017.2665620

Mohanta, A., & Saldanha, A. (2020). *Malware analysis and detection engineering: A comprehensive approach to detect and analyze modern malware* (1st ed.). Apress. https://doi.org/10.1007/978-1-4842-6193-4

Namanya, A. P., Cullen, A., Awan, I. U., & Disso, J. P. (2018). The world of malware: An overview. In *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)* (str. 420-427). IEEE. https://doi.org/10.1109/FiCloud.2018.00067

National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations* (NIST Special Publication No. 800-53, Rev. 4). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (n.d.). *Breach*. In *Computer Security Resource Center (CSRC) glossary*. Pregledano 15. kolovoza 2024, s https://csrc.nist.gov/glossary/term/breach

National Institute of Standards and Technology. (n.d.). *Cyber attack*. In *Computer Security Resource Center (CSRC) glossary*. Pregledano 15. kolovoza 2024, s https://csrc.nist.gov/glossary/term/cyber_attack

Nurse, J. R. C., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Ur.), *The Oxford handbook of cyberpsychology* (1st ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.36

Nwokedi, I., & Mathur, A. (2007). *A survey of malware detection techniques*. Purdue University. https://www.researchgate.net/publication/229008321_A_survey_of_malware_detection_techniques

Office of the National Cyber Director. (2024). *2024 report on the cybersecurity posture of the United States*. Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

Ogundare, E. (2024). *The human factor in cyber security*. https://www.researchgate.net/publication/379430784_THE_HUMAN_FACTOR_IN_CYBER_SECURITY

Özçelik, İ., & Brooks, R. R. (2020). *Distributed denial of service attacks: Real-world detection and mitigation*. CRC Press. https://doi.org/10.1201/9781315213125

Parsaei, A. (2024). Awareness and social engineering-based cyberattacks. *International Journal of Reliability, Risk and Safety: Theory and Application, 7*(1), 31-36. https://doi.org/10.22034/IJRRS.2024.7.1.4

Rashid, S., & Paul, S. P. (2013). Proposed methods of IP spoofing detection & prevention. *International Journal of Science and Research, 2*(8), 438–444.

Ribeiro, R., Mateus-Coelho, N., & Mamede, H. S. (2023). Improving social engineering resilience in enterprises: A systematic literature review. *ARIS2 - Advanced Research on Information Systems Security, 3*(1), 34-65. https://doi.org/10.56394/aris2.v3i1.30

Roopak, M., Parkinson, S., Tian, G., Ran, Y., Khan, S., & Chandrasekaran, B. (2024). *An unsupervised approach for the detection of zero-day DDoS attacks in IoT networks*. https://doi.org/10.22541/au.170526630.07302484/v1

Sabu, J., S, A., Gopan, A., G, S., & Murali, S. (2023). Advanced keylogger with keystroke dynamics. *Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT)* (str. 1598–1603). IEEE. https://doi.org/10.1109/ICICT57646.2023.10134044

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications (IJERA), 2*(2), 202–209. ISSN: 2248-9622

Samhi, J., Bissyandé, T. F., & Klein, J. (2022). TriggerZoo: A dataset of Android applications automatically infected with logic bombs. *Proceedings of the 19th International Conference on Mining Software Repositories (MSR '22)* (str. 459–463). Association for Computing Machinery. https://doi.org/10.1145/3524842.3528020

Selvan, A. J. A., & Fonceca, C. M. (2023). Cyber security culture in an IT company: An empirical study. *International Journal of Multidisciplinary Research and Growth Evaluation, 4*(2), 351-354. https://www.researchgate.net/publication/370059163_Cyber_security_culture_in_an_IT_company_An_empirical_study

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Soltes, E. (2016). *Why they do it: Inside the mind of the white-collar criminal*. PublicAffairs.

Sood, A. K., & Enbody, R. (2014). *Targeted cyber attacks: Multi-staged attacks driven by exploits and malware*. Syngress.

Squillace, J., & Cappella, J. (2024). Examining how targeted cyber attacks on critical supply chain networks can lead to economic collapse and civil unrest. *Proceedings of SoutheastCon 2024* (str. 1482-1489). IEEE. https://doi.org/10.1109/SoutheastCon52093.2024.10500029

Stallings, W., & Brown, L. (2024). *Computer security: Principles and practice* (5th ed.). Pearson Education, Inc.

Sujatha, G., Kanchhal, Y., & George, G. (2022). An advanced approach for detection of distributed denial of service (DDoS) attacks using machine learning techniques. *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)* (str. 821–827). IEEE. https://doi.org/10.1109/ICOSEC54921.2022.9951944

Suresh Kumar, S., Stephen, S., & Suhainul Rumysia, M. (2024). Rootkit detection using deep learning: A comprehensive survey. *Proceedings of the 2024 10th International Conference on Communication and Signal Processing (ICCSP)* (str. 365–370). IEEE. https://doi.org/10.1109/ICCSP60870.2024.10543963

Tanwar, V., & Ramkumar, K. R. (2023). A survey on the role of reverse engineering in security attacks. *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)* (str. 1-6). IEEE. https://doi.org/10.1109/RMKMATE59243.2023.10369068

TechTarget Contributor. (2024). *Web application (web app)*. TechTarget. https://www.techtarget.com/searchsoftwarequality/definition/Web-application-Web-app

Temara, S. (2024). The ransomware epidemic: Recent cybersecurity incidents demystified. *Asian Journal of Advanced Research and Reports, 18*(3), 1–16. https://doi.org/10.9734/ajarr/2024/v18i3610

The White House. (2023, ožujak). *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Truong, T. C., & Zelinka, I. (2019). A survey on artificial intelligence in malware as next-generation threats. *Mendel*, *25*(2), 27–34. https://doi.org/10.13164/mendel.2019.2.027

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M. A., & Rashid, A. (2018). Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications, 101,* 18-54. https://doi.org/10.1016/j.jnca.2017.10.016

Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016). Advanced persistent threats: Behind the scenes. *2016 Annual Conference on Information Science and Systems (CISS)* (str. 181–186). IEEE. https://doi.org/10.1109/CISS.2016.7460498

Verizon. (2024). *2024 data breach investigations report*. Verizon. https://verizon.com/dbir

Wang, Y., Liu, H., Li, Z., Su, Z., & Li, J. (2024). Combating advanced persistent threats: Challenges and solutions. *IEEE Network*. https://doi.org/10.1109/MNET.2024.3389734

World Economic Forum. (2024). *Global cybersecurity outlook 2024: Insight report*. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

World Economic Forum. (2024). *The Global Risks Report 2024* (19th ed.). World Economic Forum. https://www.weforum.org/publications/global-risks-report-2024/

Yilmaz, E., & Can, O. (2024). Unveiling shadows: Harnessing artificial intelligence for insider threat detection. *Engineering, Technology & Applied Science Research, 14*(2), 13341–13346. https://doi.org/10.48084/etasr.6911

Yu, Y., Yang, W., Ding, W., & Zhou, J. (2023). Reinforcement learning solution for cyber-physical systems security against replay attacks. *IEEE Transactions on Information Forensics and Security, 18*, 2583–2595. https://doi.org/10.1109/TIFS.2023.3268532

Zeng, Y. (2022). AI empowers security threats and strategies for cyber attacks. *Procedia Computer Science, 208*, 170-175. https://doi.org/10.1016/j.procs.2022.10.025

Zhang, L., Yu, S., Wu, D., & Watters, P. (2011). A survey on latest botnet attack and defense. *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (str. 53–60). IEEE. https://doi.org/10.1109/TrustCom.2011.11

## SAŽETAK

Ovaj rad istražuje uzroke i karakteristike kibernetičkih napada u privatnom sektoru, uključujući motive, metode i posljedice ovih napada. Kibernetički napadi predstavljaju sve veću prijetnju za organizacije zbog rastuće ovisnosti o tehnologiji. Unatoč njihovoj globalnoj važnosti, informacije o kibernetičkim napadima često su raspršene i nestandardizirane. Cilj ovog rada je pružiti sveobuhvatnu informacijsku podlogu koja obuhvaća različite aspekte kibernetičkih napada, omogućujući organizacijama u privatnom sektoru bolje razumijevanje i pripremu za ove prijetnje.

Metode istraživanja uključivale su temeljitu analizu literature i empirijsko istraživanje na temelju sekundarnih podataka o 1147 slučajeva kibernetičkih napada u privatnom sektoru. Rezultati istraživanja ističu da su ljudske greške, ranjivosti informacijskih sustava i ubrzani razvoj tehnologije ključni faktori koji doprinose uspješnosti kibernetičkih napada. Financijski motivi identificirani su kao najdominantniji, dok su organizirane hakerske grupe prevladavajući akteri. Istraživanje također pokazuje da je proaktivan pristup ključan za smanjenje rizika i uspješnu obranu od kibernetičkih prijetnji.



Ključne riječi: kibernetički napadi, sigurnosni propusti, kibernetička sigurnost

## SUMMARY

This paper investigates the causes and characteristics of cyber-attacks in the private sector, including the motives, methods, and consequences of these attacks. Cyber-attacks pose an increasing threat to organizations due to their growing reliance on technology. Despite their global significance, information on cyber-attacks is often scattered and non-standardized. The aim of this paper is to provide a comprehensive informational foundation that covers various aspects of cyber-attacks, enabling private sector organizations to better understand and prepare for these threats.

The research methods included a thorough literature review and empirical research based on secondary data from 1,147 cases of cyber-attacks in the private sector. The research findings highlight that human errors, vulnerabilities in information systems, and rapid technological development are key factors contributing to the success of cyber-attacks. Financial motives were identified as the most dominant, while organized hacker groups were found to be the prevailing actors. The research also demonstrates that a proactive approach is crucial for reducing risks and successfully defending against cyber threats.

Keywords: cyber-attacks, security breaches, cybersecurity

## PRILOZI

DavDoan. (2024). *WikiDataBreachAnalysis* [Dataset]. GitHub. https://github.com/DavDoan/WikiDataBreachAnalysis/blob/main/CleanData.csv

Gojoyuno. (2024). *Cyber breach analysis dataset* [Dataset]. Kaggle. https://www.kaggle.com/datasets/gojoyuno/cyber-breach-analysis-dataset

information is beautiful. (2024). *World's biggest data breaches & hacks* [Dataset]. information is beautiful. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

TheDevastator. (2022). *Data breaches: A comprehensive list* [Dataset]. Kaggle. https://www.kaggle.com/datasets/thedevastator/data-breaches-a-comprehensive-list

## POPIS GRAFIČKIH PRIKAZA