Napredne metode i strategije u kibernetičkoj sigurnosti: Prilagođavanje u suvremenom IT okruženju

Krajačić, Marta

VELEUČILIŠTE SUVREMENIH INFORMACIJSKIH TEHNOLOGIJA

STRUČNI PRIJEDIPLOMSKI STUDIJ INFORMACIJSKIH TEHNOLOGIJA

Marta Krajačić

ZAVRŠNI RAD

NAPREDNE METODE I STRATEGIJE U KIBERNETIČKOJ SIGURNOSTI: PRILAGOĐAVANJE U SUVREMENOM IT OKRUŽENJU

Veleučilište suvremenih informacijskih tehnologija
10000 Zagreb, Ulica Vjekoslava Klaića 7

Studij:	Stručni prijediplomski studij informacijskih tehnologija smjer baze podataka i web dizajn
Student:	**Marta Krajačić**
Matični broj:	2018057

Zadatak završnog rada

Predmet:	Računalne mreže
Naslov:	**Napredne metode i strategije u kibernetičkoj sigurnosti: Prilagođavanje u suvremenom IT okruženju**
Zadatak:	Analizirati postojeće metode i strategije kibernetičke sigurnosti, identificirati njihove slabosti te predložiti napredne tehnike i rješenja za unapređenje sigurnosnih sustava u suvremenim IT okruženjima. Razviti praktični projekt koji implementira odabrane sigurnosne mjere, testira njihovu efikasnost u simuliranim uvjetima te analizira i dokumentira rezultate i moguća poboljšanja.
Mentor:	dr. sc. Damir Delija, prof. struč. stud.
Zadatak uručen kandidatu:	3.10.2023.
Rok za predaju rada:	29.10.2024.
Rad predan:	_____

Povjerenstvo:

Marijan Čančarević, v. pred.	član predsjednik	_____
dr. sc. Damir Delija, prof. struč. stud.	mentor	_____
Edmond Krusha, v. pred.	član	_____

SADRŽAJ

1. UVOD

Kibernetička sigurnost danas je neizostavna tema koja postaje sve važnija s obzirom na rastuću učestalost prijetnji kao što su hakiranje, krađa identiteta i infekcije malware-om. Ovi napadi predstavljaju ozbiljnu prijetnju ne samo velikim korporacijama, već i pojedincima i njihovim osjetljivim podacima. Očuvanje integriteta informacijskih sustava i zaštita privatnosti korisnika ključni su aspekti kibernetičke sigurnosti, koja se temelji na načelima zaštite podataka i resursa od neautoriziranog pristupa i napada.

Kako se osobne i poslovne aktivnosti sve više premještaju na digitalne platforme, sigurnost na internetu postaje imperativ za sve – od pojedinaca do velikih organizacija. Kibernetička sigurnost, stoga, ne samo da postaje nužnost, već zahtijeva neprekidno praćenje, prilagođavanje i inovacije kako bi se očuvala stabilnost i povjerenje u digitalnim okruženjima.

U ovom radu, osim što ćemo razmotriti razne metode kibernetičke sigurnosti, detaljno ćemo analizirati implementaciju Zero Trust modela. Ovaj model, koji zahtijeva stalnu provjeru korisnika bez obzira na njihovu lokaciju ili ulogu unutar organizacije, postaje sve važniji u modernim sigurnosnim strategijama. Iako Zero Trust model značajno poboljšava sigurnost, mnoge organizacije još uvijek nisu u potpunosti implementirale potrebne mjere, što ih čini ranjivima na napade.

Povećanje broja državom sponzoriranih kibernetičkih napada također predstavlja značajan problem. Takvi napadi, usmjereni na ključne infrastrukturne sektore kao što su energetika, zdravstvo i financijski sektor, često imaju političke i strateške ciljeve. Države poput Rusije i Sjeverne Koreje često su povezane s ovim vrstama aktivnosti, što dodatno komplicira globalni sigurnosni krajobraz.

Sigurnost lanca opskrbe postaje još jedno ključno pitanje. Napadači sve više koriste slabosti trećih strana kako bi pristupili sustavima, što naglašava potrebu za poboljšanjem sigurnosnih protokola unutar cijelog lanca opskrbe.

Rasprostranjenost IoT (Internet of Things) uređaja dodatno povećava rizike. IoT uređaji, koji su sve prisutniji u industrijskim i privatnim okruženjima, često su nesigurni i predstavljaju idealne mete za napade. Ovi uređaji mogu biti iskorišteni za pokretanje DDoS napada, krađu podataka ili prekid rada, što zahtijeva sveobuhvatan pristup sigurnosti tih sustava.

Konačno, stroži regulatorni okviri, poput NIS2 direktive u Europskoj uniji, prisiljavaju organizacije na usvajanje rigoroznijih sigurnosnih mjera. Ovo uključuje unaprjeđenje unutarnjih procedura, bolje upravljanje sigurnosnim incidentima i kontinuiranu edukaciju zaposlenika.

Ovi izazovi jasno pokazuju da kibernetička sigurnost nije statična, već dinamično područje koje zahtijeva stalne inovacije i prilagodbu. Samo usvajanjem holističkog pristupa, koji uključuje najnovije tehnologije, strože regulative i edukaciju zaposlenika, moguće je osigurati dugoročnu sigurnost digitalne infrastrukture i održati povjerenje u digitalnom svijetu.

2. TEORIJSKE OSNOVE KIBERNETIČKE SIGURNOSTI

Teorijske osnove kibernetičke sigurnosti oblikovale su se kroz desetljeća tehnološkog napretka i evolucije računalnih sustava, počevši od ranih godina računalne povijesti pa sve do modernih vremena u kojima su kibernetičke prijetnje postale sastavni dio globalne sigurnosne strategije. Današnje razumijevanje kibernetičke sigurnosti temelji se na ključnim konceptima i metodologijama koje omogućuju zaštitu digitalnih resursa od rastućeg spektra prijetnji.

2.1. Osnovni koncepti kibernetičke sigurnosti

Kibernetička sigurnost odnosi se na korištenje različitih tehnologija, praksi i metoda kako bi se zaštitile mreže, podaci i sustavi od kibernetičkih prijetnji. Ovi ključni koncepti čine temelj za razumijevanje načina na koji se informacije štite u digitalnom svijetu. U ovom dijelu rada analizirat ćemo i definirati ključne pojmove i principe koji čine osnovu kibernetičke sigurnosti. Jedan od koncepata na koji ćemo se posebno osvrnuti u ovom radu je Zero Trust Model, koji se temelji na ideji da se nikome ne vjeruje automatski, bez obzira na to odakle dolazi pristup, već se svaki korisnik i uređaj mora neprestano provjeravati. U prilogu slijedi analiza i definicija nekih od osnovnih koncepata kibernetičke sigurnosti.

- Povjerljivost (Confidentiality)

  Povjerljivost se odnosi na osiguravanje da su osjetljivi podaci dostupni samo onima koji imaju pravo pristupa. Čuvanje povjerljivosti ključan je element u sprječavanju neovlaštenog pristupa informacijama. To se postiže kroz metode kao što su šifriranje, upravljanje pristupom i autentifikacija. Šifriranje pretvara podatke u format koji je nečitljiv bez ispravne autorizacije. Višefaktorska autentifikacija (MFA) dodaje dodatni sloj sigurnosti, zahtijevajući od korisnika da potvrde svoj identitet na više načina.
- Integritet (Integrity)

  Integritet osigurava da podaci ostanu točni i nepromijenjeni tijekom cijelog svog životnog ciklusa. To znači da informacije ne smiju biti neovlašteno izmijenjene, bilo slučajno ili namjerno. Alati poput digitalnih potpisa i kontrola verzija omogućuju osiguravanje da se podaci ne mogu mijenjati bez da to bude zabilježeno. Na primjer, prilikom prijenosa podataka, kriptografske metode pomažu otkriti sve promjene koje su nastale tijekom prijenosa, čuvajući tako njihov integritet.
- Dostupnost (Availability)

  Dostupnost podataka i sustava osigurava da korisnici mogu pristupiti informacijama kada god im zatrebaju. Cilj je osigurati da sustavi ostanu operativni unatoč prijetnjama,

poput kibernetičkih napada ili tehničkih kvarova. Strategije za očuvanje dostupnosti uključuju korištenje sigurnosnih kopija, distribuiranih mreža i zaštitu od DDoS napada. Napadi uskraćivanja usluge (DoS/DDoS) mogu privremeno onesposobiti sustave, ali uz pomoć sustava za balansiranje opterećenja i redovnih sigurnosnih kopija, rizici se mogu minimizirati.

- Autentifikacija (Authentication)

  Autentifikacija je proces kojim se potvrđuje identitet korisnika. Ovaj postupak osigurava da samo ovlašteni korisnici mogu pristupiti resursima ili podacima. Primjeri autentifikacije uključuju lozinke, biometrijske podatke (poput otisaka prstiju ili prepoznavanja lica) te višefaktorsku autentifikaciju (MFA), koja kombinira više načina provjere identiteta.

- Autorizacija (Authorization)

  Autorizacija određuje prava i ovlasti korisnika unutar sustava. Nakon što je korisnik autentificiran, autorizacija mu omogućuje pristup određenim resursima i radnjama unutar sustava. Autorizacija osigurava da korisnici imaju samo onaj pristup koji im je potreban, čime se smanjuje rizik od zloupotrebe informacija.

- Neodricanje (Non-repudiation)

  Neodricanje osigurava da ni pošiljatelj ni primatelj ne mogu poreći da su poslali ili primili određene informacije. Ovaj koncept je posebno važan u pravnim i financijskim transakcijama. Digitalni potpisi i kriptografski algoritmi omogućuju dokaz da su transakcije ili komunikacije zaista izvršene.

- Praćenje i revizija (Monitoring and Auditing)

  Praćenje i revizija ključni su alati za praćenje aktivnosti unutar sustava i otkrivanje nepravilnosti. Sustavi za otkrivanje upada (IDS) i sustavi za prevenciju upada (IPS) pomažu u prepoznavanju sumnjivih aktivnosti u stvarnom vremenu. Revizija pak omogućuje analizu povijesnih podataka kako bi se osigurala usklađenost sa sigurnosnim pravilima i otkrile potencijalne ranjivosti.

- Sigurnosne politike (Security Policies)

  Sigurnosne politike definiraju smjernice i postupke koje organizacija mora slijediti kako bi zaštitila svoje informacijske sustave. To uključuje pravila o korištenju lozinki, upravljanje pristupom, sigurnosnim kopijama podataka i postupanje u slučaju sigurnosnih incidenata. Dobro definirane sigurnosne politike ključne su za učinkovitu zaštitu podataka i resursa te za usklađenost s regulativama.

- Upravljanje prijetnjama (Threat Management)

  Upravljanje prijetnjama obuhvaća identificiranje, procjenu i sprječavanje prijetnji prije nego što postanu ozbiljan sigurnosni problem. Procjene ranjivosti i penetracijska testiranja koriste se za otkrivanje potencijalnih slabosti u sustavu, dok redovite sigurnosne zakrpe (patch management) pomažu eliminirati te ranjivosti prije nego što ih napadači iskoriste.
- Zaštita krajnjih točaka (Endpoint Security)

  Zaštita krajnjih točaka odnosi se na osiguranje pojedinačnih uređaja, poput računala, pametnih telefona i IoT uređaja, koji su povezani na mrežu. To uključuje korištenje antivirusnih programa, firewallova i sustava za otkrivanje zlonamjernih softvera, kako bi se spriječilo da krajnji uređaji postanu slaba točka u mreži.

Zero Trust Model blisko je povezan s ključnim principima kibernetičke sigurnosti, poput povjerljivosti, integriteta, dostupnosti, autentifikacije, autorizacije i upravljanja prijetnjama. Povjerljivost, koja jamči da su osjetljivi podaci dostupni samo onima koji imaju pravo pristupa, pojačava se kroz stalnu provjeru identiteta i višefaktorsku autentifikaciju. Za razliku od tradicionalnih sustava koji automatski vjeruju svima unutar mreže, Zero Trust zahtijeva kontinuiranu provjeru i autorizaciju za svaki pristup. Također osigurava integritet podataka strogim kontrolama i praćenjem promjena, dok dostupnost održava stalnom provjerom pristupa i dodjelom samo nužnih privilegija. Upravljanje prijetnjama temelji se na neprestanom praćenju i brzom otkrivanju potencijalnih napada, a zaštita krajnjih točaka dodatno je pojačana sigurnosnim provjerama svakog uređaja prije nego što mu se odobri pristup. Na taj način, Zero Trust objedinjuje sve ove elemente u koherentan i učinkovit sustav zaštite prilagođen suvremenim prijetnjama.

3. PREGLED KIBERNETIČKIH PRIJETNJI I METODOLOGIJA

Kibernetičke prijetnje danas dolaze iz raznih smjerova – od zlonamjernog softvera do složenih napada na ključne infrastrukturne sustave. Ti napadi mogu uključivati hakere izvana, unutarnje prijetnje unutar samih organizacija te sve učestalije napade na opskrbne lance, poznate kao "supply chain" napadi. Kako bi se organizacije mogle obraniti od ovih prijetnji, potrebno je primijeniti raznolike i sveobuhvatne sigurnosne metodologije. One uključuju procjenu rizika, identifikaciju ranjivosti te implementaciju adekvatnih zaštitnih mjera.

Prijetnje postaju sve sofisticiranije, osobito s primjenom novih tehnologija poput umjetne inteligencije. AI omogućava napadačima stvaranje prilagođenih phishing napada, kreiranje deepfake sadržaja, pa čak i manipulaciju podacima, što čini te napade izuzetno teško prepoznatljivima tradicionalnim sustavima zaštite. Takvi sofisticirani napadi koriste napredne algoritme i strojnim učenjem prilagođavaju svoje strategije, što dodatno naglašava potrebu za razvijenijim sigurnosnim pristupima.

Organizacije se danas oslanjaju na složene metodologije za upravljanje prijetnjama, kao što su višeslojna zaštita (Defense in Depth), kontinuirano praćenje mrežnog prometa i sustava te procjena potencijalnih ranjivosti. Zero Trust model postaje sve popularniji jer nudi sigurnosni pristup koji podrazumijeva stalnu provjeru identiteta korisnika i kontrolu pristupa, čime se smanjuje rizik od neovlaštenih napada unutar organizacije.

Nadalje, kroz analizu ključnih prijetnji koje su prisutne u današnjem digitalnom svijetu te metodologija koje su razvijene kako bi se te prijetnje prepoznale i spriječile, bolje ćemo razumjeti s kakvim izazovima se organizacije suočavaju. Metodologije koje ćemo dalje prikazati pomažu u postavljanju okvira za proaktivnu zaštitu te nude najbolju praksu u suočavanju s kibernetičkim prijetnjama. Posebna pažnja bit će posvećena naprednim modelima kao što je Zero Trust, koji uvelike doprinose modernim sigurnosnim strategijama.

U nastavku slijedi detaljna analiza metodologija koje se koriste za učinkovito upravljanje kibernetičkim prijetnjama.

3.1. Upravljanje rizicima u kibernetičkoj sigurnosti

Upravljanje rizicima je metodologija koja omogućuje organizacijama da identificiraju, procijene i smanje rizike koji ugrožavaju njihove sustave, podatke i mreže. Kako kibernetičke prijetnje nastavljaju evoluirati, tako i metodologije upravljanja rizicima moraju biti prilagodljive i u stalnoj promjeni. Danas se suočavamo s prijetnjama koje sve češće koriste napredne tehnologije, poput umjetne inteligencije (AI), kako bi zaobišle tradicionalne sigurnosne sustave. Stoga je važno primjenjivati sveobuhvatan pristup koji uključuje

kontinuiranu procjenu rizika, detekciju ranjivosti te implementaciju zaštitnih mjera koje su u skladu s najnovijim tehnološkim trendovima.

Upravljanje rizicima obično započinje s identifikacijom rizika, što znači prepoznavanje potencijalnih ranjivosti u sustavu, poput zastarjele softverske infrastrukture ili nedovoljno educirane zaposlenike. Nakon identifikacije, sljedeći korak je procjena rizika, kojom se utvrđuje vjerojatnost ostvarivanja prijetnje i potencijalni učinak na organizaciju. Na temelju tih podataka, organizacije definiraju prioritete zaštite i razvijaju planove kako bi se minimizirali rizici.

Među najvažnijim koracima upravljanja rizicima je implementacija zaštitnih mjera. Ovdje je naglasak na primjeni tehnoloških alata poput šifriranja, višefaktorske autentifikacije, ali i na razvoju sigurnosnih politika unutar organizacija, uključujući edukaciju zaposlenika. Posljednji, ali ne manje važan korak, je kontinuirano praćenje i revizija. Budući da se prijetnje stalno razvijaju, organizacije moraju neprekidno prilagođavati svoje sigurnosne mjere kako bi ostale korak ispred napadača.

3.1.1. Obrana u dubini (Defense in Depth)

Obrana u dubini (Defense in Depth, DiD) je pristup kibernetičkoj sigurnosti koji se temelji na ideji da nijedna sigurnosna mjera nije savršena i da je potrebno imati više slojeva zaštite kako bi se napadačima otežao pristup sustavima. Svaki sloj predstavlja dodatnu prepreku koju napadači moraju savladati kako bi stigli do osjetljivih podataka ili kritične infrastrukture. Ovaj pristup često se uspoređuje s utvrdom – baš kao što se srednjovjekovni dvorci branili s više slojeva zaštite, od jarka i zidova do stražara, tako i današnji sustavi koriste niz sigurnosnih mjera kako bi spriječili napade.

Jedan od prvih slojeva u ovoj strategiji je perimetralna zaštita, koja uključuje vatrozide (firewalle) i mrežne filtre. Njihova funkcija je kontrolirati sav promet koji ulazi i izlazi iz mreže, tako da neovlašteni korisnici nemaju pristup osjetljivim dijelovima sustava. Nakon toga dolazi mrežna segmentacija, koja razdvaja mrežu u manje dijelove. Time se sprječava da napadač, čak i ako probije vanjski sloj, može lako prodrijeti u cijeli sustav – pristup svakom segmentu mreže je strogo kontroliran.

Također, sigurnost krajnjih točaka igra ključnu ulogu u zaštiti uređaja poput računala, mobitela i IoT uređaja koji se povezuju na mrežu. Korištenjem antivirusnog softvera, enkripcije podataka i redovitih ažuriranja softvera, organizacije osiguravaju da su svi povezani uređaji zaštićeni. Tu je i sigurnost aplikacija, koja se fokusira na zaštitu web i softverskih aplikacija putem vatrozida

za aplikacije, sigurnosnih testiranja i pravovremenih zakrpa, sprječavajući napade poput SQL injekcija.

Cijeli koncept obrane u dubini temelji se na tri ključna područja zaštite: fizičkoj, administrativnoj i tehničkoj. Fizička zaštita odnosi se na stvari poput zaključanih prostorija i sigurnosnih kamera koje štite podatkovne centre i druge ključne dijelove infrastrukture. Administrativna zaštita obuhvaća sigurnosne politike, pravilnike i edukaciju zaposlenika, dok tehnička zaštita uključuje vatrozide, antivirusni softver i enkripciju podataka – sve što direktno štiti digitalne aspekte organizacije.

Današnja tehnologija, poput računalstva u oblaku i rada na daljinu, zahtijeva modernizaciju ove strategije. Zero Trust pristup, gdje se nikome ne vjeruje automatski, postaje sve popularniji. Ovaj pristup osigurava stalnu verifikaciju i praćenje korisnika, što dodatno smanjuje rizike napada. U kombinaciji s obrambenim slojevima, organizacije postaju znatno otpornije na napade.

Jedan od glavnih razloga zašto je obrana u dubini toliko učinkovita je što napadač, kako bi ostvario svoj cilj, mora proći kroz više slojeva zaštite. To napade čini dugotrajnijima i složenijima, povećavajući šanse da ih sustav otkrije i zaustavi. Ova strategija također zahtijeva kontinuiranu prilagodbu – organizacije moraju redovito procjenjivati nove prijetnje i osigurati da njihovi sigurnosni slojevi ostanu učinkoviti i ažurirani.

Na kraju, obrana u dubini nije samo kombinacija sigurnosnih alata, već sveobuhvatan pristup koji integrira različite oblike zaštite kako bi sustavi i podaci ostali sigurni. Kroz slojevitu zaštitu organizacije povećavaju otpornost na napade i osiguravaju da, čak i ako jedan sloj zakaže, drugi slojevi nastave štititi ključne dijelove sustava. Ovaj pristup postao je jedna od najpouzdanijih i najefikasnijih strategija u modernoj kibernetičkoj sigurnosti.

3.1.2. NIST-ov okvir za kibernetičku sigurnost

NIST-ov okvir za kibernetičku sigurnost (CSF- Cybersecurity Framework), razvijen je na Nacionalnom institutu za standarde i tehnologiju, dizajniran je na da bude dovoljno fleksibilan kako bi se mogao prilagoditi različitim vrstama organizacija, bez obzira na veličinu ili sektor u kojem djeluju. Sastoji se od tri glavne komponente: okvir jezgre, okvir implementacijskih razina i profil okvira.

Okvir jezgre je dio koji sadrži pet osnovnih funkcija: Identificirati, Zaštititi, Otkriti, Reagirati i Oporaviti se. Svaka funkcija pomaže organizacijama prepoznati prijetnje, implementirati sigurnosne mjere, reagirati na incidente i vratiti se u normalno poslovanje. Funkcija

"Identifikacija" pomaže prepoznati imovinu i potencijalne ranjivosti, "Zaštita" osigurava provođenje mjera kao što su kontrola pristupa i enkripcija podataka, dok funkcije "Otkrivanje" i "Reagiranje" osiguravaju brzo prepoznavanje i odgovaranje na sigurnosne prijetnje. Zadnja funkcija "Oporavak" omogućuje organizacijama da se brzo oporave nakon incidenta.

Okvir implementacijskih razina pomaže organizacijama u određivanju njihove trenutne razine razvijenosti u pogledu sigurnosti. Postoje četiri razine: od djelomične, gdje sigurnosne mjere nisu u potpunosti implementirane, do adaptivne, gdje organizacija kontinuirano prilagođava svoje sigurnosne mjere na temelju novih prijetnji i naučenih lekcija.

Profil okvira omogućuje organizacijama da prilagode sigurnosne mjere svojim specifičnim potrebama. Organizacija može stvoriti "trenutni profil", koji odražava sadašnju sigurnosnu razinu, i "ciljani profil", koji predstavlja sigurnosne ciljeve koje žele postići. Uspoređivanjem ovih profila organizacije mogu vidjeti gdje imaju nedostatke i na čemu trebaju raditi.

Implementacija NIST CSF-a obuhvaća nekoliko bitnih koraka:

1. Procjena rizika: Ovaj početni korak podrazumijeva detaljnu analizu svih resursa koje organizacija koristi, kao i prepoznavanje potencijalnih prijetnji i ranjivosti koje bi mogle ugroziti te resurse. Sustavi za upravljanje imovinom, poput CMDB-a (Configuration Management Database), omogućuju organizacijama mapiranje svih digitalnih resursa – poput podataka, aplikacija, servera i mreža – te identifikaciju osjetljivih dijelova sustava koji zahtijevaju posebnu pažnju. Na temelju ovih podataka, organizacija može odrediti gdje postoje najveće sigurnosne praznine i koji resursi zahtijevaju najviši stupanj zaštite

2. Tehnološka zaštita: Nakon identifikacije resursa i ranjivosti, implementiraju se sigurnosne mjere koje štite sustav od neovlaštenog pristupa i potencijalnih prijetnji. Jedan od ključnih aspekata zaštite je multifaktorska autentifikacija (MFA), koja osigurava da samo ovlašteni korisnici mogu pristupiti osjetljivim podacima. MFA koristi više oblika verifikacije (npr. lozinke i mobilne potvrde) kako bi povećala sigurnost pristupa. Uz to, sustavi za upravljanje identitetima (IAM), kao što su Okta ili Azure AD, upravljaju i nadziru korisničke pristupe unutar organizacije, osiguravajući da ovlaštenja budu pravilno dodijeljena i kontrolirana.

3. Enkripcija podataka igra ključnu ulogu u zaštiti osjetljivih informacija. Alati poput BitLockera (za enkripciju diskova) i TLS/SSL certifikata (za zaštitu podataka tijekom prijenosa) osiguravaju da, čak i ako napadači uspiju pristupiti podacima, ne mogu ih pročitati bez dešifriranja. Vatrozidi i IDS/IPS sustavi (Intrusion Detection and

Prevention Systems), poput Cisco ASA i Palo Alto Networks, pružaju mrežnu zaštitu, prepoznajući i blokirajući neovlašteni mrežni promet i pokušaje proboja.

4. Stalno praćenje: Kontinuirano praćenje mreže ključno je za pravovremeno otkrivanje prijetnji. SIEM (Security Information and Event Management) rješenja, poput Splunka i IBM QRadara, prikupljaju sigurnosne podatke iz različitih izvora unutar organizacije, analiziraju ih u stvarnom vremenu i identificiraju moguće prijetnje ili anomalije. Ovi alati omogućuju organizacijama da odmah reagiraju na sumnjive aktivnosti, smanjujući potencijalnu štetu koja bi mogla nastati kao rezultat kibernetičkih napada.

5. Odgovor na incidente: Kada se dogodi sigurnosni incident, brzina reakcije je ključna. Platforme za SOAR (Security Orchestration, Automation, and Response), poput Palo Alto Cortex XSOAR, automatiziraju i koordiniraju odgovor na incidente. SOAR sustavi omogućuju organizacijama da automatski poduzmu korake poput izolacije zaraženih sustava, obavještavanja relevantnih timova i dokumentiranja incidenata radi kasnije analize. Automacija ubrzava proces odgovora, smanjuje ljudske pogreške i minimizira štetu.

6. Oporavak: Nakon incidenta, ključna je faza oporavka, koja osigurava da se podaci i sustavi vrate u prethodno stanje. Alati za sigurnosne kopije i oporavak podataka, poput Veeama i Acronisa, osiguravaju da se izgubljeni ili oštećeni podaci brzo obnove, čime se omogućuje kontinuitet poslovanja. Ovaj korak uključuje i analizu incidenta kako bi se identificirale slabosti u sustavu i poduzele mjere za njihovo otklanjanje u budućnosti.

7. NIST CSF nije statičan proces. Organizacije kontinuirano evaluiraju učinkovitost svojih sigurnosnih mjera i prilagođavaju ih kako bi ostale zaštićene od novih prijetnji.

3.1.3. Napredni sustavi za otkrivanje prijetnji (IDS/IPS)

Napredni sustavi za otkrivanje prijetnji (IDS/IPS) imaju značajnu ulogu u zaštiti mreža i sustava od različitih kibernetičkih napada. IDS (sustav za otkrivanje upada, engl. Intrusion Detection System) i IPS (sustav za sprječavanje upada, engl. Intrusion Prevention System) omogućuju organizacijama ne samo prepoznavanje prijetnji već i zaštitu od njih, uz mogućnost reagiranja u stvarnom vremenu.

IDS funkcionira kao sustav koji pasivno nadzire mrežni promet i analizira aktivnosti kako bi prepoznao sumnjive ili neovlaštene radnje. Kada prepozna nepravilnosti, sustav generira

upozorenje za administratore, koji tada poduzimaju potrebne korake. IDS sustavi mogu biti mrežni (NIDS), gdje nadziru promet na cijeloj mreži, ili na poslužitelju (HIDS), gdje nadziru specifične uređaje ili aplikacije. IPS, s druge strane, ide korak dalje od IDS-a jer ne samo da prepoznaje prijetnje, već aktivno reagira na njih. To znači da IPS može odmah blokirati sumnjivi promet ili spriječiti napad prije nego što napravi štetu sustavu.

IDS sustavi koriste dva osnovna pristupa: prepoznavanje uzoraka ,gdje se koriste unaprijed definirana pravila za prepoznavanje poznatih napada, i prepoznavanje anomalija, gdje sustav prati neuobičajeno ponašanje u mreži kako bi prepoznao nove ili sofisticirane prijetnje. IPS koristi iste metode, no s dodatnom funkcijom automatske reakcije, kao što su blokiranje sumnjivog prometa ili ograničavanje pristupa.

Kada govorimo o implementaciji IDS/IPS sustava, ona može biti softverska ili hardverska.

Softverska rješenja uključuju IDS/IPS sustave koji se instaliraju kao aplikacije na poslužiteljima ili mrežnim uređajima. Ove aplikacije nadziru mrežni promet, analiziraju podatke koji prolaze kroz mrežu te prepoznaju potencijalne prijetnje. Njihova prednost je fleksibilnost i mogućnost integracije u postojeće sustave.

Hardverska rješenja odnose se na namjenske uređaje, koji se fizički postavljaju unutar mrežne infrastrukture. Ti uređaji djeluju kao filteri, analizirajući svaki paket podataka koji prolazi kroz mrežu, te automatski poduzimaju mjere ako prepoznaju prijetnju. Takvi uređaji su često postavljeni na strateškim točkama mreže, između rutera i internih sustava, kako bi imali pregled nad prometom koji ulazi i izlazi iz mreže.Kada se implementiraju IDS/IPS sustavi, oni ne zahtijevaju fizičke čipove, već su to uređaji ili softverska rješenja koja se integriraju s mrežom kako bi kontinuirano nadzirali promet. Na primjer, uređaj može biti smješten između mrežnog rutera i ključnih internih sustava, što omogućava analizu svakog paketa podataka u stvarnom vremenu.

U tehnologijama koje se koriste za implementaciju IDS/IPS sustava, ističe se DPI metoda ili dubinska inspekcija paketa (engl. Deep Packet Inspection) koja omogućava detaljnu analizu svakog paketa unutar mrežnog prometa, uključujući i sadržaj paketa. IDS/IPS sustavi također se često integriraju sa SIEM (engl. Security Information and Event Management) rješenjima, kao što su Splunk ili IBM QRadar, kako bi analizirali i korelirali podatke u stvarnom vremenu te automatski generirali upozorenja. Osim toga, sve češće koriste umjetnu inteligenciju i strojno učenje kako bi prepoznali nove obrasce prijetnji i prilagodili sigurnosne mjere za otkrivanje i sprječavanje novih vrsta napada.

Ova rješenja omogućuju organizacijama ne samo prepoznavanje prijetnji, već i aktivnu zaštitu od njih u stvarnom vremenu, osiguravajući stalnu zaštitu mreža i sustava.

3.1.4. Zero Trust sigurnosni model

Zero Trust je sigurnosni model koji je postao neophodan u današnjim IT okruženjima zbog promjena poput sve češćeg rada na daljinu i korištenja oblaka. Osnovna ideja ovog modela je "nikada ne vjeruj, uvijek provjeri". Tradicionalni sigurnosni modeli povjeravaju pristup korisnicima ili uređajima unutar mreže, no Zero Trust odbacuje tu pretpostavku i zahtijeva stalnu provjeru svih korisnika i uređaja, neovisno o njihovoj lokaciji.

U tradicionalnim modelima, nakon što korisnik ili uređaj uđe u mrežu, često mu se automatski dodjeljuje povjerenje i slobodan pristup mnogim resursima. Ovaj pristup predstavlja rizik, jer napadači koji jednom probiju vanjski sigurnosni sloj mogu se slobodno kretati unutar mreže. Zero Trust sprječava takve scenarije zahtijevajući autentifikaciju i autorizaciju za svaki pristup, bez obzira na mjesto korisnika.

Jedan od ključnih elemenata Zero Trust modela je mikrosegmentacija. To znači da se mreža dijeli na manje dijelove ili segmente, gdje svaki segment ima strogo kontrolirani pristup. Ako napadač uspije probiti jedan segment, ne može lako doći do drugih dijelova mreže, čime se znatno smanjuje potencijalna šteta.

Drugi važan princip je najmanje privilegije. Korisnicima i uređajima dodjeljuje se samo minimalan pristup potreban za obavljanje zadataka. Tako, čak i ako je napadač kompromitirao nečiji račun, šteta se može kontrolirati jer kompromitirani korisnik nema pristup svemu.

Višefaktorska autentifikacija (MFA) je također ključan element Zero Trust modela. MFA koristi kombinaciju lozinki, biometrijskih podataka i potvrda putem mobilnih uređaja kako bi osigurala identitet korisnika. To otežava napadačima pristup čak i ako imaju korisničke vjerodajnice.

Kontinuirano praćenje aktivnosti korisnika i uređaja još je jedna važna karakteristika Zero Trust modela. Sustavi stalno prate obrasce ponašanja i aktivnosti te reagiraju na svaku sumnjivu ili neuobičajenu aktivnost. Na taj način moguće je brzo prilagoditi sigurnosne mjere na temelju promjena u ponašanju korisnika.

Implementacija Zero Trust modela

Implementacija Zero Trust modela zahtijeva više tehničkih koraka i slojevit pristup. Prvi korak je identifikacija kritičnih resursa unutar organizacije, kao što su podaci, sustavi i aplikacije. Ovo uključuje mapiranje svih digitalnih resursa i određivanje tko treba imati pristup tim resursima. Mreža se tada mikrosegmentira korištenjem tehnologija poput SDN (Software-Defined Networking) i VLAN-ova za razdvajanje mrežnog prometa na manje, kontrolirane segmente.

Ovo sprječava napadače da se lateralno kreću unutar mreže ako uspiju kompromitirati jedan segment.

Drugi važan tehnički korak je implementacija višefaktorske autentifikacije (MFA). Korištenjem alata poput Microsoft Azure AD ili Okta, svaki korisnik mora proći dodatne razine autentifikacije, uključujući lozinke, biometrijske podatke ili mobilne potvrde. Osim toga, sustavi za Identity and Access Management (IAM) centraliziraju upravljanje identitetima, dok Privileged Access Management (PAM) rješenja osiguravaju strogu kontrolu nad privilegiranim računima i njihovim pristupom osjetljivim podacima.

Kontinuirano praćenje aktivnosti korisnika i uređaja osigurava se korištenjem SIEM i NDR alata. SIEM (Security Information and Event Management) sustavi kao što su Splunk i IBM QRadar prate sigurnosne događaje u stvarnom vremenu i koreliraju ih kako bi prepoznali anomalije ili prijetnje. NDR (Network Detection and Response) alati poput Darktrace nadziru mrežni promet, detektirajući neobične obrasce i potencijalne napade. Ovi alati omogućuju organizacijama da brzo prepoznaju i reagiraju na prijetnje prije nego što se prošire.

Također, primjena principa najmanjih privilegija osigurava da korisnici i uređaji imaju samo osnovne dozvole potrebne za obavljanje svojih zadataka. Korištenje RBAC (Role-Based Access Control) sustava omogućuje upravljanje pravima pristupa na temelju korisničkih uloga unutar organizacije, smanjujući mogućnost zloupotrebe privilegija.

Na kraju, automatizacija odgovora na prijetnje putem SOAR (Security Orchestration, Automation, and Response) sustava omogućuje organizacijama brzo reagiranje na incidente. SOAR alati poput Palo Alto Cortex XSOAR automatski izoliraju zaražene sustave, šalju obavijesti sigurnosnim timovima i dokumentiraju incidente, čime se minimizira potencijalna šteta.

Zero Trust pruža dinamičnu sigurnost za organizacije, osobito u složenim IT okruženjima koja uključuju rad na daljinu i korištenje oblaka. Implementacijom mikro segmentacije, višefaktorske autentifikacije i kontinuiranog praćenja, organizacije mogu značajno smanjiti rizik od napada i osigurati bolju kontrolu nad pristupom kritičnim resursima.

3.1.5. Kriptografija i šifriranje

Kriptografija je proces zaštite podataka s pomoću matematičkih metoda koje osiguravaju povjerljivost, integritet i autentičnost informacija. Osnovni cilj kriptografije je onemogućiti pristup podacima neovlaštenim osobama, kako tijekom prijenosa, tako i tijekom pohrane podataka. U suvremenom IT okruženju, kriptografija ima ključnu ulogu u osiguravanju sigurnih komunikacija, zaštiti podataka i očuvanju privatnosti.

Jedan od temeljnih elemenata kriptografije je šifriranje. Šifriranje se koristi za pretvaranje razumljivih podataka (tzv. čistog teksta) u nečitljiv niz podataka (šifrat), koji može dešifrirati samo ovlaštena osoba ili sustav. Postoje dvije glavne vrste kriptografije:

1. Simetrično šifriranje: U simetričnom šifriranju koristi se jedan ključ za šifriranje i dešifriranje podataka. Ova metoda je brza i učinkovita, što ju čini pogodnom za šifriranje velikih količina podataka. Međutim, glavni izazov simetričnog šifriranja je sigurno dijeljenje ključa između dviju strana, jer svaka strana mora imati isti ključ za dešifriranje podataka. Ako ključ padne u ruke napadača, sigurnost podataka je ugrožena. Najpoznatiji primjer simetričnog algoritma je AES (Advanced Encryption Standard), koji je široko korišten zbog svoje sigurnosti i brzine.

2. Asimetrično šifriranje: Za razliku od simetričnog šifriranja, asimetrično šifriranje koristi par ključeva – jedan javni i jedan privatni ključ. Javni ključ koristi se za šifriranje podataka, dok se privatni koristi za njihovo dešifriranje. Velika prednost ovog pristupa je što se javni ključ može slobodno dijeliti, dok privatni ključ ostaje tajan. Tako, čak i ako netko dođe do javnog ključa, ne može dešifrirati podatke bez privatnog ključa. Asimetrično šifriranje pruža višu razinu sigurnosti, ali je nešto sporije u usporedbi sa simetričnim metodama. Primjer asimetrične kriptografije je RSA algoritam, koji se koristi u različitim sigurnosnim aplikacijama, uključujući digitalne potpise i SSL/TLS protokole za osiguravanje internetskih veza.

Osim šifriranja, kriptografija obuhvaća i druge tehnike koje dodatno povećavaju sigurnost podataka:

- Digitalni potpisi: Digitalni potpisi služe kao dokaz autentičnosti i integriteta podataka. Koriste se kako bi se osiguralo da je određena poruka ili dokument došao od vjerodostojnog pošiljatelja te da nije promijenjen tijekom prijenosa. Digitalni potpisi često se koriste u elektroničkoj trgovini, digitalnim certifikatima i pravno valjanoj elektroničkoj komunikaciji.

- Hash funkcije: Hash funkcije koriste se za generiranje jedinstvenih "otisaka" podataka. Ove funkcije pretvaraju podatke u fiksnu duljinu šifriranih kodova, bez obzira na veličinu izvornog podatka. Ako se podaci i najmanje promijene, hash funkcija će generirati potpuno drugačiji kod, čime se lako može otkriti svaka promjena ili manipulacija podacima. Primjeri popularnih hash funkcija su SHA-256 i MD5.

- Kriptografski protokoli: Uključuju protokole poput SSL/TLS koji omogućuju sigurne internetske veze, osiguravajući da su podaci šifrirani tijekom prijenosa. Ovi protokoli koriste kombinaciju simetričnih i asimetričnih metoda kako bi omogućili siguran prijenos podataka, primjerice u komunikacijama putem web preglednika.

Kriptografija je ključna za osiguranje različitih oblika komunikacija i prijenosa podataka u IT sustavima. Osim osiguravanja sigurnosti financijskih transakcija (npr. kod digitalnih valuta), koristi se i u VPN-ovima, aplikacijama za sigurno slanje poruka (npr. WhatsApp koristi end-to-end enkripciju), elektroničkom bankarstvu te svim vrstama elektroničke trgovine i privatnih podataka.
S obzirom na važnost i osjetljivost podataka u modernom svijetu, kriptografija ostaje temeljna tehnologija za zaštitu privatnosti, integriteta i sigurnosti podataka.

3.1.6. Sigurnost u oblaku

Sigurnost u oblaku postaje sve značajniji aspekt kibernetičke sigurnosti s obzirom na to da se sve više organizacija odlučuje za korištenje cloud usluga radi povećane fleksibilnosti, smanjenih troškova i lakšeg pristupa resursima. Međutim, korištenje oblaka također donosi izazove u vezi s osiguranjem podataka, aplikacija i infrastrukture, pa je stoga neophodno usvojiti niz mjera koje će zaštititi osjetljive informacije. Organizacije moraju implementirati sveobuhvatne sigurnosne strategije kako bi se smanjili rizici od neovlaštenog pristupa, kibernetičkih napada te gubitka podataka.
Jedan od temeljnih aspekata sigurnosti u oblaku je šifriranje podataka. Ova mjera osigurava da podaci pohranjeni ili preneseni putem oblaka budu zaštićeni i nečitljivi neovlaštenim korisnicima, čak i ako dođe do proboja sigurnosnih mjera. Šifriranje podataka može se primijeniti u različitim fazama – tijekom prijenosa (data in transit) i tijekom pohrane (data at rest), čime se dodatno smanjuje mogućnost neovlaštenog pristupa. Primjena end-to-end šifriranja omogućuje da podaci ostanu zaštićeni od izvora do odredišta, bez mogućnosti presretanja ili neovlaštenog čitanja. To je posebno važno u kontekstu korištenja oblaka jer osjetljivi podaci prolaze kroz više mrežnih točaka prije nego što dođu do krajnjeg korisnika.
Osim šifriranja, ključna je kontrola pristupa i autorizacija. Oblak se temelji na tome da podaci budu dostupni s bilo kojeg mjesta i uređaja, što je pogodnost, ali i rizik. Zbog toga se koriste stroge mjere autentifikacije, poput višefaktorske autentifikacije (MFA), gdje se pristup odobrava tek nakon što korisnik prođe nekoliko razina provjere identiteta. Time se značajno smanjuje rizik od neovlaštenog pristupa, čak i ako su kompromitirane lozinke. Višefaktorska

autentifikacija nadopunjuje se naprednim sustavima za upravljanje identitetima (IAM), koji omogućuju centralizirano upravljanje korisnicima i kontrolu nad njihovim pravima pristupa. Upravo pravilno definiranje uloga i prava korisnika u oblaku ključno je za zaštitu osjetljivih podataka.

Praćenje i nadzor aktivnosti u oblaku omogućuju organizacijama da u stvarnom vremenu prepoznaju prijetnje i reagiraju na njih prije nego što naprave štetu. Korištenjem specifičnih alata za praćenje, organizacije mogu detektirati anomalije u mrežnom prometu te identificirati potencijalne prijetnje. Ovi alati koriste napredne tehnologije poput umjetne inteligencije i strojnog učenja kako bi analizirali ogromne količine podataka i prepoznali neuobičajene obrasce ponašanja. Time se omogućuje pravovremeno otkrivanje sumnjivih aktivnosti, kao što su pokušaji neovlaštenog pristupa ili prijenos velikih količina podataka bez ovlaštenja. Integracija ovih sustava u infrastrukturu oblaka omogućuje brzu reakciju na prijetnje te minimiziranje potencijalne štete.

Sigurnosne politike u oblaku također igraju ključnu ulogu u zaštiti podataka. Svaka organizacija mora definirati jasna pravila i postupke za upravljanje podacima, uključujući pravila za pohranu, pristup i dijeljenje podataka. Te politike moraju biti u skladu s propisima poput GDPR-a ili HIPAA-e, koji propisuju kako se osobni podaci trebaju čuvati i koristiti. Usluge oblaka često nude alate koji pomažu organizacijama da osiguraju usklađenost s ovim propisima, što je od iznimne važnosti za zaštitu privatnosti i povjerljivosti podataka.

Uz sve navedene mjere, dodatne sigurnosne prakse, poput izrade sigurnosnih kopija i planova za oporavak od katastrofa (Disaster Recovery), pomažu u osiguravanju kontinuiteta poslovanja čak i u slučaju sigurnosnih incidenata. Redovita izrada sigurnosnih kopija podataka smanjuje rizik od trajnog gubitka podataka u slučaju kibernetičkog napada ili tehničkog kvara. Također, korištenje virtualnih privatnih oblaka (VPC) omogućuje stvaranje privatnih, izoliranih mrežnih okruženja unutar javnih oblaka, što dodatno povećava sigurnost i kontrolu nad mrežnim prometom.

Sigurnost u oblaku omogućuje organizacijama da u potpunosti iskoriste prednosti koje im pružaju udaljeni resursi i infrastruktura, uz istodobnu zaštitu podataka od kibernetičkih napada i gubitka podataka. Kombinacijom šifriranja, stroge kontrole pristupa, praćenja aktivnosti u stvarnom vremenu te postavljanja jasnih sigurnosnih politika, organizacije mogu osigurati sigurno i efikasno poslovanje u oblaku, čime smanjuju rizik od prijetnji i povećavaju sigurnost svojih podataka.

Ovo su samo neke od brojnih metodologija za sprječavanje i upravljanje kibernetičkim

prijetnjama. Postoje i druge poput FAIR-a (Factor Analysis of Information Risk), koja se koristi za kvantitativnu procjenu rizika u informacijskoj sigurnosti, omogućujući organizacijama da donesu bolje odluke o upravljanju rizicima. OSSTMM (Open Source Security Testing Methodology Manual) nudi strukturirani pristup za sigurnosno testiranje fizičkih, ljudskih i mrežnih sustava. SOC 2 je standard koji se fokusira na sigurnost, dostupnost, povjerljivost i integritet podataka za organizacije koje upravljaju podacima drugih tvrtki. PCI DSS (Payment Card Industry Data Security Standard) koristi se za zaštitu podataka o platnim karticama, posebno u industrijama koje obrađuju, pohranjuju ili prenose te osjetljive informacije. Ove metodologije dodatno proširuju mogućnosti zaštite od kibernetičkih prijetnji i pomažu organizacijama da bolje upravljaju sigurnosnim rizicima.

Kombinacija svih navedenih metodologija, tehnologija i strategija omogućava organizacijama da ne samo prepoznaju i spriječe prijetnje već i da se brzo oporave nakon incidenta, čime se smanjuje potencijalna šteta i osigurava dugoročna zaštita podataka i sustava. S obzirom na brzinu razvoja novih prijetnji, kontinuirana prilagodba i modernizacija sigurnosnih pristupa ključna je za ostanak korak ispred napadača.

3.2. TIPOVI KIBERNETIČKIH NAPADA

Nakon detaljne analize tehnologija i metoda za zaštitu, vrijeme je za dio od kojega se štitimo, a to su kibernetički napadi.

Kibernetički napadi mogu se podijeliti na različite tipove ovisno o izvoru napada i razini tehničke sofisticiranosti napadača. Postoje unutarnji i vanjski napadi, ovisno o tome dolazi li prijetnja iz same organizacije ili od vanjskih aktera. Unutarnji napadi često uključuju osobe koje već imaju ovlašten pristup sustavima, dok vanjski napadi dolaze od vanjskih prijetnji, često uz pomoć naprednih alata i metoda. Ovisno o vještinama napadača, napadi mogu biti strukturirani, gdje iskusni kriminalci ciljano koriste sofisticirane tehnike, ili nestrukturirani, koji dolaze od amatera bez jasnog plana. Svaki tip napada predstavlja ozbiljnu prijetnju, a organizacije i pojedinci trebali bi biti spremni suočiti se s ovim rizicima putem naprednih sigurnosnih mjera i tehnologija.

3.2.1. Zlonamjerni softver(Malware)

Malware, ili zlonamjerni softver, postao je jedan od najsloženijih i najopasnijih oblika prijetnji u svijetu kibernetičke sigurnosti. Ovi programi su kreirani s ciljem da oštete, ometu ili neovlašteno pristupe računalima, mrežama i podacima, a kako tehnologija napreduje, tako i malware postaje sve sofisticiraniji. Od ranih virusa koji su se širili putem floppy diskova do

današnjih sofisticiranih napada koji ciljaju velike korporacije i državne institucije, malware je evoluirao u prijetnju koja se ne može ignorirati.

Najčešći tipovi malwarea

- Virusi su prvi poznati oblik zlonamjernog softvera. Oni se šire tako što se vežu uz legitimne programe i datoteke, a jednom aktivirani mogu oštetiti podatke ili usporiti sustav. Oni se često prenose putem e-pošte ili preuzimanja s interneta. Kada se jednom "zaraze" sustavi, virusi mogu lako prenositi zlonamjerne kodove na druge uređaje.
- Crvi (worms) djeluju slično virusima, ali za razliku od njih, mogu se samostalno širiti mrežom bez interakcije korisnika. Crvi preopterećuju mrežne resurse i često uzrokuju velike štete. Na primjer, Morrisov crv iz 1988. godine zarazio je tisuće računala širom svijeta, naglašavajući kako brzo ovakvi napadi mogu paralizirati čitave mreže.
- Ransomware je postao jedna od najvećih prijetnji za organizacije. Ovaj tip malwarea šifrira podatke žrtve i traži otkupninu za povratak pristupa. Napadi poput WannaCry i NotPetya iz 2017. godine uzrokovali su globalne prekide rada, a WannaCry je posebno pogodio bolnice, uzrokujući velike gubitke i ozbiljne probleme u pružanju zdravstvene usluge.
- Spyware je zlonamjerni softver koji prati aktivnosti korisnika bez njihovog znanja. On može prikupljati osjetljive podatke, uključujući lozinke i informacije o kreditnim karticama, te ih prosljeđivati napadačima. Ovaj tip malwarea je posebno opasan jer može tiho djelovati duže vrijeme, neprimjetno narušavajući privatnost.
- Trojanski konji su malware koji se pretvara da je legitimni softver, varajući korisnike da ga instaliraju. Kada se instalira, trojanac omogućava napadačima pristup računalima i mrežama, često bez znanja korisnika.

Evolucija malwarea

Tijekom godina, malware je postao sve sofisticiraniji. U posljednje vrijeme svjedočimo rastu Ransomware-as-a-Service (RaaS) modela, gdje kriminalne organizacije prodaju ili iznajmljuju ransomware alate. Ovaj model omogućava napadačima, čak i onima s minimalnim tehničkim znanjem, da pokreću napade.

Jedan od najnovijih oblika malwarea je BlackCat ransomware (poznat i kao ALPHV), koji koristi napredne tehnike kako bi ciljao velike organizacije. U 2023. godini, ova skupina je izvela niz napada, uključujući onemogućavanje NCR Aloha POS sustava, čime su restorani ostali bez funkcionalnih blagajni, te napad na grad Dallas, koji je paralizirao IT sustave gradske uprave i policije.

3.2.2. Phishing

Phishing predstavlja jedan od najučestalijih i najrazornijih oblika kibernetičkih napada, a njegova učinkovitost temelji se na manipulaciji ljudima kako bi nehotice otkrili osjetljive podatke. Ova vrsta napada uglavnom se oslanja na socijalni inženjering, gdje napadači iskorištavaju povjerenje korisnika ili njihovu nepažnju kako bi dobili pristup informacijama poput lozinki, brojeva kreditnih kartica ili drugih osjetljivih podataka. Phishing napadi, koji se često provode putem e-pošte ili lažnih web stranica, koriste tehniku imitacije stvarnih organizacija ili pojedinaca kako bi uvjerili korisnike da predaju svoje podatke ili obave određene akcije koje idu u korist napadača.

Jedan od najpoznatijih primjera phishing napada dogodio se između 2013. i 2015. godine, kada su napadači uspješno prevarili tehnološke gigante, poput Googlea i Facebooka, koristeći sofisticirane phishing kampanje. U ovom slučaju, napadači su poslali lažne račune za plaćanje, predstavljajući se kao legitimni dobavljači. Kao rezultat toga, tvrtke su izvršile isplate napadačima, što je rezultiralo financijskim gubitkom od preko 100 milijuna dolara. Ovaj napad pokazuje koliko su phishing kampanje sofisticirane i kako čak i najveće korporacije mogu postati žrtve ako ne primijene odgovarajuće sigurnosne mjere.

Phishing dolazi u različitim oblicima, od kojih su neki ciljaniji i opasniji. Spear phishing predstavlja ciljane napade na određene pojedince ili organizacije, pri čemu napadači koriste personalizirane informacije kako bi poruke izgledale legitimno. Whaling je posebna vrsta spear phishinga koja je usmjerena na visoke dužnosnike ili članove uprave unutar organizacija. S druge strane, clone phishing uključuje kreiranje kopija legitimnih e-poruka kako bi korisnici vjerovali da je riječ o stvarnim zahtjevima, no linkovi ili privici unutar poruka usmjeravaju na zlonamjerne stranice.

Zaštita od phishinga zahtijeva višeslojni pristup. Prva linija obrane leži u edukaciji korisnika, gdje je ključna svijest o prijetnjama. Obučeni korisnici mogu lakše prepoznati sumnjive poruke i poduzeti korake kako bi izbjegli prevaru. Osim toga, korištenje antivirusnih i anti-phishing alata osigurava dodatni sloj zaštite jer ovi alati mogu blokirati sumnjive poruke ili spriječiti pristup lažnim web stranicama. Višefaktorska autentifikacija (MFA) pruža dodatnu zaštitu jer zahtijeva više koraka za prijavu, čime se smanjuje mogućnost da napadač dobije pristup sustavu, čak i ako je kompromitirao lozinku korisnika.

S tehničkog aspekta, provjera URL adresa i SSL certifikata također su jednostavne, ali učinkovite mjere. Lažne web stranice često koriste URL-ove koji su slični legitimnim, s blagim razlikama u slovima, dok SSL certifikati pružaju dodatnu sigurnost provjerom autentičnosti

web stranica. Korištenje ovih tehnika značajno smanjuje šanse da korisnici postanu žrtve phishing napada.

Utjecaj phishinga na organizacije može biti razoran. Financijski gubici, krađa podataka i ugrožen ugled organizacija predstavljaju samo neke od posljedica uspješnih phishing napada. U današnjem digitalnom svijetu, gdje su podaci ključni resurs, nužno je poduzeti sve dostupne mjere kako bi se spriječili ovi napadi. Osim tehničkih rješenja, ključna je kontinuirana obuka zaposlenika kako bi bili u stanju prepoznati prijetnje. Kombinacija modernih tehnologija, kao što su MFA i antivirusni alati, uz edukaciju i svijest korisnika, najbolja je obrana protiv phishing napada.

U konačnici, phishing ostaje jedan od najčešće korištenih oblika kibernetičkih napada zbog svoje jednostavnosti i učinkovitosti. No, uz odgovarajuće sigurnosne mjere i svijest o prijetnjama, organizacije mogu smanjiti rizik od ovih napada i zaštititi svoje podatke i sustave.

3.2.3. DDoS (Distribuirani napadi uskraćivanja usluge)

DDoS (Distributed Denial of Service) napadi predstavljaju jednu od najraširenijih i najučinkovitijih vrsta kibernetičkih napada čiji je cilj preplaviti ciljani sustav ili mrežu velikom količinom lažnog prometa. Rezultat je preopterećenje sustava, zbog čega postaje neupotrebljiv za legitimne korisnike. Ovi napadi često koriste tzv. botnet mreže, koje se sastoje od zaraženih uređaja kao što su računala, pametni telefoni i IoT uređaji, poput kamera ili printera. Napadači koriste te zaražene uređaje za generiranje golemog volumena lažnog prometa koji onemogućuje rad ciljanog sustava ili mreže.

Primjer jednog od najvećih i najsloženijih DDoS napada dogodio se u listopadu 2016. godine, kada je tvrtka Dyn, koja upravlja internetskim uslugama, bila meta masivnog napada. Ovaj napad je imao dalekosežne posljedice jer su zbog njega velike web stranice poput Twittera, Netflixa, Reddita i CNN-a postale nedostupne. Napadači su koristili mrežu zaraženih IoT uređaja (kamere, printeri), koje su preplavili prometom kako bi onesposobili sustav. U ovom slučaju, korišten je Mirai botnet, koji je iskorištavao loše sigurnosne postavke na IoT uređajima i pretvarao ih u alate za napad.

Slično tomu, GitHub, popularna platforma za razvoj softvera, također je bila meta jednog od najvećih zabilježenih DDoS napada u 2018. godini. Napad je dosegao vrhunac prometa od 1,35 Tbps, što ga čini jednim od najsnažnijih napada ikad zabilježenih. Iako je napad trajao samo 20 minuta, bio je dovoljno snažan da izazove privremenu nedostupnost GitHubove usluge. No, zahvaljujući naprednim tehnikama za sprječavanje DDoS napada, tim GitHub uspio je brzo

obnoviti svoje usluge. Ovi slučajevi pokazuju koliko su DDoS napadi postali ozbiljan sigurnosni problem, osobito zbog brzog rasta IoT uređaja, koji su često slabo zaštićeni.

DDoS napadi funkcioniraju na način da napadači kompromitiraju veliki broj uređaja i pretvaraju ih u botnet mrežu. Ovi uređaji, pod kontrolom napadača, koordinirano šalju zahtjeve prema ciljanim serverima ili mrežama, stvarajući preopterećenje. Postoji nekoliko različitih vrsta DDoS napada. Volumetrijski napadi pokušavaju zagušiti propusnost mreže ogromnom količinom lažnog prometa, dok napadi na aplikacijski sloj (Layer 7) ciljaju specifične aplikacije, poput web stranica, kako bi ih preopteretili, bez potrebe za velikim prometom. Također, napadi poput SYN flooda koriste TCP protokol kako bi stvorili polovično otvorene veze i onemogućili sustav u obradi novih zahtjeva.

Za obranu od DDoS napada, organizacije koriste niz tehnoloških rješenja koja omogućuju filtriranje i ograničavanje prometa prije nego što on dosegne ciljani sustav. Rješenja poput Cloudflare, Akamai ili AWS Shield koriste tehnike za filtriranje i raspodjelu prometa kako bi smanjili rizik od preopterećenja. Ova rješenja koriste Content Delivery Network (CDN) sustave koji distribuiraju promet na globalnoj razini i time smanjuju pritisak na pojedine servere. Osim toga, primjena tehnika poput rate limitinga, gdje se ograničava broj zahtjeva po korisniku u određenom vremenskom razdoblju, također pomaže u zaštiti od ovakvih napada. Organizacije također koriste Deep Packet Inspection (DPI) tehnologiju koja analizira promet i filtrira zlonamjerne pakete podataka prije nego što dođu do cilja.

DDoS napadi mogu imati razorne posljedice po organizacije, uključujući financijske gubitke, narušeni ugled i gubitak povjerenja korisnika. Zbog toga je od iznimne važnosti implementirati napredne sustave zaštite i kontinuirano nadzirati promet kako bi se prepoznale i spriječile potencijalne prijetnje. Kombinacija proaktivnih sigurnosnih mjera i naprednih alata za detekciju omogućuje organizacijama da smanje učinak DDoS napada i osiguraju kontinuitet poslovanja.

3.2.4. SQL Injekcija

SQL injekcija (SQL-i) jedna je od najučestalijih tehnika napada na web aplikacije koja se koristi za iskorištavanje ranjivosti u komunikaciji s bazama podataka. Ova metoda napada omogućuje napadačima da umjesto uobičajenih korisničkih unosa u aplikaciju ubace zlonamjerne SQL naredbe kako bi pristupili bazi podataka. Posljedice mogu biti razorne, od krađe osjetljivih podataka do uništenja baze. Unatoč tome što SQL injekcija postoji već desetljećima, ona i dalje predstavlja značajan problem jer mnoge aplikacije, zbog lošeg dizajna ili neadekvatnih sigurnosnih mjera, ostaju ranjive.

SQL injekcija omogućuje napadačima da ostvare širok raspon zlonamjernih aktivnosti. Najčešće se koristi za krađu osjetljivih podataka poput lozinki, brojeva kreditnih kartica, email adresa i drugih osobnih podataka. No, može poslužiti i za dobivanje administratorskih privilegija, što napadaču omogućuje potpunu kontrolu nad aplikacijom. U nekim slučajevima napadači čak koriste SQL injekcije kako bi manipulirali bazama podataka, što im omogućuje neovlašteno mijenjanje ili brisanje podataka.

Jedan od najpoznatijih primjera ovakvog napada dogodio se 2008. godine kada je Heartland Payment Systems, procesor za kreditne kartice, pretrpio masivni napad. Napadači su uspjeli iskoristiti ranjivosti u sustavu kako bi pristupili bazi podataka i ukrali oko 130 milijuna brojeva kreditnih i debitnih kartica. Ovaj slučaj je jasan pokazatelj koliko su ovakvi napadi opasni i kako mogu rezultirati ogromnim financijskim gubicima. Slično se dogodilo i u napadu na Yahoo! Voices 2012. godine, kada je oko pola milijuna email adresa i lozinki kompromitirano zbog ranjivosti uzrokovanih lošom zaštitom baze podataka.

Još jedan noviji slučaj zabilježen je 2023. godine kada je grupa hakera pod nazivom ResumeLooters iskoristila SQL injekciju kako bi provalila na više od 65 web stranica, uključujući stranice za zapošljavanje i trgovine. Ukradeni su milijuni osobnih podataka koji su kasnije prodani na tamnom webu. Ovaj napad je pokazao da, unatoč napretku tehnologije, SQL injekcija i dalje ostaje velika prijetnja, posebno za web aplikacije koje nisu dovoljno osigurane.

Zaštita od SQL injekcija zahtijeva kombinaciju tehničkih mjera i dobrih sigurnosnih praksi. Prvi korak u zaštiti je korištenje parametriziranih upita. Ova tehnika osigurava da se korisnički unos ne može interpretirati kao SQL naredba, već se obrađuje kao običan tekst. Tako se eliminira mogućnost da napadač umetne zlonamjerne naredbe u bazu podataka. Korištenje ORM alata (Object-Relational Mapping), poput Hibernatea ili Entity Frameworka, također smanjuje rizik jer ovi alati automatski generiraju SQL upite i štite aplikaciju od direktnih napada.

Također, filtriranje i validacija unosa izuzetno su važne mjere zaštite. Svi podaci koje aplikacija prima od korisnika moraju biti provjereni i očišćeni od potencijalno zlonamjernih unosa. Na primjer, ograničavanje vrste podataka koje aplikacija prihvaća ili korištenje white-lista za validaciju unosa mogu značajno smanjiti mogućnost napada. Uz to, redovita sigurnosna ažuriranja ključna su za osiguranje aplikacije jer mnoge ranije verzije softvera imaju poznate ranjivosti koje napadači mogu iskoristiti.

SQL injekcija i dalje predstavlja jednu od najvećih prijetnji za web aplikacije, osobito zbog toga što mnoge aplikacije još uvijek ne primjenjuju odgovarajuće sigurnosne mjere. Redovito ažuriranje sustava, implementacija tehnika kao što su parametrizirani upiti i validacija podataka

te korištenje ORM alata može značajno smanjiti rizik od ovih napada i zaštititi osjetljive podatke

Ovo su samo neki od brojnih napada s kojima se susrećemo, a s porastom primjene umjetne inteligencije (AI), ove prijetnje postaju sve sofisticiranije. Umjetna inteligencija omogućava napadačima da automatiziraju napade, prilagođavaju phishing kampanje i koriste deepfake tehnologije kako bi zavarali čak i najnaprednije sigurnosne sustave. AI također pomaže u razvoju novih alata za otkrivanje i prevenciju prijetnji, poput naprednih sustava za analizu podataka u stvarnom vremenu.

Sve veći izazov predstavlja brzina kojom se kibernetičke prijetnje razvijaju. Organizacije se moraju neprestano prilagođavati ovim prijetnjama primjenom višeslojnih sigurnosnih strategija, kontinuiranog praćenja sustava i edukacije zaposlenika. Kombinacijom tradicionalnih metoda zaštite, poput enkripcije i vatrozida, te naprednih alata koji koriste AI, organizacije mogu značajno smanjiti rizik od kibernetičkih napada i osigurati sigurnost svojih sustava i podataka.

4. PRAKTIČNI RAD - IMPLEMENTACIJA ZERO TRUST MODELA U OFFICE 365 OKRUŽENJU

Tijekom ovog praktičnog rada implementirala sam Zero Trust model unutar Office 365 okruženja, prateći definirane korake kako bih osigurala maksimalnu zaštitu podataka, korisnika i uređaja. Proces je započeo sveobuhvatnom procjenom sigurnosnih potreba organizacije, zatim identifikacijom ključnih resursa koje je bilo potrebno zaštititi, te konačno, implementacijom odgovarajućih alata i tehnologija iz Office 365 paketa.

4.1. Procjena sigurnosnih potreba organizacije

Prvi korak u implementaciji Zero Trust modela unutar Office 365 bila je temeljita procjena sigurnosnih potreba organizacije. Ovaj proces poslužio je kao polazna točka za definiranje ključnih sigurnosnih zahtjeva te identificiranje najvažnijih resursa koje je bilo potrebno zaštititi. Provela sam ovu procjenu korak po korak, s ciljem razumijevanja gdje se nalaze potencijalne ranjivosti te kako ih mogu adresirati kroz implementaciju Zero Trust modela.

4.1.1. Korak 1: Pregled postojećih sigurnosnih mjera i infrastrukture

Započela sam s detaljnim pregledom postojećih sigurnosnih mehanizama i infrastrukture organizacije. To je uključivalo provjeru trenutnih tehnologija za autentifikaciju korisnika, zaštitu podataka i upravljanje pristupom. Ispitala sam i koje se sigurnosne politike primjenjuju, od načina na koji se upravlja korisničkim lozinkama, do zaštite podataka u prijenosu i pohrani.

Teorijski, Zero Trust model zahtijeva uklanjanje implicitnog povjerenja unutar mreže. Tradicionalne sigurnosne postavke često pretpostavljaju da su svi unutar mrežnog perimetra pouzdani, no Zero Trust zahtijeva stalnu provjeru svakog korisnika i uređaja. Analitički, ustanovljeno je da postojeći sustavi unutar organizacije nemaju potrebnu razinu nadzora nad unutarnjim korisnicima, što znači da je bilo potrebno uvesti strože sigurnosne mehanizme za kontinuiranu verifikaciju.

4.1.2. Korak 2: Identifikacija osjetljivih podataka i ključnih sustava

Nakon pregleda infrastrukture, fokusirala sam se na identifikaciju osjetljivih podataka i glavnih sustava unutar organizacije. Ovo je bilo ključno jer sam morala odrediti koji podaci zahtijevaju najvišu razinu zaštite, poput financijskih informacija, osobnih podataka zaposlenika, te strateških poslovnih dokumenata. Također sam identificirala kritične IT sustave i aplikacije bez kojih organizacija ne bi mogla nesmetano funkcionirati, poput e-mail

platformi, sustava za upravljanje projektima i CRM aplikacija.

Zero Trust stavlja poseban naglasak na zaštitu osjetljivih podataka i kontrolu pristupa. Organizacije moraju imati jasnu sliku o tome što se smatra najosjetljivijim resursima kako bi se odgovarajuće sigurnosne mjere usmjerile na ta područja. Uvidjela sam da je najveći rizik ugrožavanje financijskih podataka i osobnih informacija zaposlenika, pa sam to stavila u fokus buduće implementacije sigurnosnih alata.

4.1.3. Korak 3: Procjena prijetnji i rizika

Kako bismo bolje razumjeli s čime se organizacija suočava, povedena je procjenu prijetnji i rizika. Identificirala sam vanjske i unutarnje prijetnje, poput phishing napada, ransomware napada i moguće zloupotrebe privilegiranih pristupnih prava. S obzirom na sve veći trend rada na daljinu, posebnu pažnju posvetila sam uređajima izvan kontrole organizacije (BYOD – Bring Your Own Device), koji predstavljaju dodatni sigurnosni rizik.

Zero Trust model polazi od pretpostavke da prijetnje mogu doći s bilo kojeg mjesta – izvan ili unutar organizacije. Svaka veza mora biti tretirana kao potencijalni sigurnosni rizik, a pristup podacima i resursima mora biti strogo kontroliran. Zaključujemo da su phishing napadi i neosigurani uređaji najveći sigurnosni izazovi za organizaciju, te se usmjeravamo na rješavanje tih problema u daljnjim koracima.

4.1.4. Korak 4: Usklađivanje s regulativama

Nakon procjene prijetnji, analizirala sam koliko su trenutni sigurnosni procesi organizacije usklađeni s važećim regulativama poput GDPR-a (Opća uredba o zaštiti podataka, engl. General Data Protection Regulation). S obzirom na to da organizacija obrađuje osobne podatke svojih zaposlenika i klijenata, bilo je ključno osigurati da svi podaci budu pravilno zaštićeni i pohranjeni u skladu s propisima. Posebna pažnja posvećena je pitanjima privatnosti, šifriranju podataka i pravilnom upravljanju osjetljivim informacijama.

Zero Trust model mora biti usklađen s regulatornim zahtjevima, osobito u pogledu zaštite osobnih podataka. Usuglašenost s regulativama kao što je GDPR osigurava da organizacija ne samo da štiti svoje podatke, već i izbjegava pravne posljedice u slučaju sigurnosnih incidenata. Identificirana su područja koja zahtijevaju bolju kontrolu nad podacima, osobito u vezi s pohranjivanjem i šifriranjem osjetljivih informacija.

4.1.5. Korak 5: Definiranje sigurnosnih ciljeva

Na temelju provedenih analiza, definirala sam sigurnosne ciljeve koji će voditi daljnju implementaciju Zero Trust modela. Glavni ciljevi uključivali su:

- Osiguravanje potpune zaštite osjetljivih podataka kroz šifriranje i ograničavanje pristupa samo onima kojima je to potrebno.
- Uvođenje višefaktorske autentifikacije (MFA) kako bi se osiguralo da samo ovlašteni korisnici mogu pristupiti osjetljivim resursima.
- Primjena uvjetnih pravila pristupa kako bi se dodatno osigurala kontrola nad pristupom podacima iz različitih mrežnih okruženja i uređaja.
- Kontinuirano praćenje aktivnosti unutar sustava i revizija svih pristupnih događaja, kako bi se pravovremeno reagiralo na potencijalne prijetnje.

Jasno definiranje ciljeva omogućuje organizaciji da sustavno primjenjuje sigurnosne mjere i prati napredak prema boljoj zaštiti. Fokusirala sam se na zaštitu osjetljivih podataka i kontrolu pristupa, kao ključne točke za osiguranje stabilnosti i sigurnosti organizacijskog IT okruženja.

4.2. Identifikacija ključnih podataka, korisnika i uređaja

Nakon procjene sigurnosnih potreba, sljedeći važan korak bio je identificirati ključne podatke, korisnike i uređaje unutar organizacije. Ovaj korak je važan jer omogućuje da precizno utvrdimo što i tko treba najvišu razinu zaštite. Jasno razumijevanje ovih elemenata omogućilo je učinkovitu primjenu sigurnosnih mjera i postavilo temelje za Zero Trust model, koji se temelji na tome da nitko i ništa nije automatski pouzdano. U nastavku je objašnjeno kako sam pristupila identifikaciji svakog od tih elemenata i čemu to služi.

4.2.1. Identifikacija ključnih podataka

Prvi korak bio je kategorizirati sve podatke koje organizacija koristi prema njihovoj osjetljivosti. Na ovaj način jasno se definira koji podaci zahtijevaju najvišu razinu zaštite, a koji podaci imaju nižu razinu rizika.

Kategorije identificiranih podataka uključivale su:

- Financijski podaci: Podaci poput izvještaja o prihodima i rashodima, troškovima i općim financijskim bilancama. Ovi podaci su vrlo osjetljivi jer bi njihov gubitak ili neovlašteni pristup mogao ozbiljno ugroziti poslovanje.

- Osobni podaci zaposlenika i klijenata: Identifikacija osobnih podataka, kao što su imena, adrese, kontakt informacije, brojevi računa i zdravstveni podaci. Kako bi bili usklađeni s GDPR-om, bilo je potrebno osigurati da ovi podaci budu pod strogom zaštitom.
- Poslovni i strateški dokumenti: To su dokumenti koji sadrže važne poslovne planove, strategije, kao i intelektualno vlasništvo. Ovi dokumenti zahtijevaju najvišu razinu povjerljivosti kako bi se zaštitila konkurentska prednost organizacije.
- Podaci o klijentima: Uključuje povjerljive informacije o klijentima, poput narudžbi i povijesti suradnje. Ovi podaci su važni jer ugroženost istih može utjecati na povjerenje klijenata u poslovanje.

Identifikacija ključnih podataka pomaže nam da znamo gdje primijeniti najstrože mjere zaštite, poput šifriranja podataka i ograničenja pristupa. Na primjer, osobni podaci korisnika i financijski dokumenti dobili su najvišu razinu zaštite jer bi njihovo curenje moglo izazvati ozbiljne posljedice. Kroz ovaj proces postavljeni su jasni prioriteti kako bismo znali gdje i kako usmjeriti resurse za zaštitu podataka.

4.2.2. Identifikacija korisnika

Sljedeći korak bio je identificirati tko sve pristupa tim podacima. Svaki korisnik unutar organizacije ima različitu razinu pristupa, ovisno o svojoj ulozi, pa je bilo važno definirati tko smije pristupiti kojem dijelu sustava. Na ovaj način se uspostavljaju pravila o pristupu i osigurava se da korisnici imaju samo onaj pristup koji im je potreban za obavljanje svakodnevnih zadataka.

Kategorije korisnika koje smo identificirali:

- Privilegirani korisnici: To su korisnici poput IT administratora i menadžera koji imaju proširene ovlasti za pristup osjetljivim sustavima i podacima. Ovi korisnici često postaju mete napada jer mogu imati pristup cijelom sustavu, pa smo za njih postavili strože sigurnosne mjere.
- Obični korisnici: Zaposlenici koji koriste sustav samo za obavljanje svakodnevnih zadataka. Njihov pristup je ograničen na specifične resurse koji su im potrebni, što znači da nemaju pristup osjetljivim podacima ako im to nije potrebno.

- Vanjski suradnici: Ako organizacija surađuje s vanjskim partnerima ili suradnicima, njihov pristup mora biti strogo kontroliran. Dobili su pristup samo onim dijelovima sustava koji su nužni za obavljanje posla, uz postavljanje dodatnih ograničenja i nadzora.

Kategorizacija korisnika omogućuje nam da primijenimo načelo najmanjih privilegija. To znači da svaki korisnik ima samo onoliko pristupa koliko mu je nužno potrebno za obavljanje posla. Tako se smanjuje mogućnost zloupotrebe ili neovlaštenog pristupa osjetljivim podacima. Za privilegirane korisnike uvađaju se dodatni slojevi zaštite, uključujući višefaktorsku autentifikaciju i strože nadzorne politike.

4.2.3. Identifikacija uređaja

U sklopu Zero Trust modela, svaki uređaj koji pristupa mreži mora biti poznat i siguran. Zato je bilo važno identificirati sve uređaje koje korisnici koriste za pristup sustavu, kako bismo osigurali da samo provjereni uređaji imaju pristup mrežnim resursima.

Kategorije uređaja koje smo identificirali:

- Korporativni uređaji: To su uređaji koji su u vlasništvu organizacije, poput računala, laptopa i pametnih telefona. Ovi uređaji su pod kontrolom IT odjela i na njih se primjenjuju stroga sigurnosna pravila.
- Privatni uređaji (BYOD): Zaposlenici ponekad koriste vlastite uređaje za poslovne svrhe, a ovi uređaji predstavljaju veći rizik jer nisu pod punom kontrolom organizacije. Postavili smo dodatne mjere zaštite, poput uvjetnog pristupa, kako bismo osigurali da se privatni uređaji koriste samo pod određenim uvjetima.
- IoT uređaji: Također smo identificirali uređaje povezane s mrežom, poput printera ili drugih uređaja povezanih s internetom, kako bismo ih uključili u sigurnosni sustav.

Identifikacija uređaja omogućuje nam da postavimo sigurnosne politike koje ograničavaju pristup samo na uređaje koji su sigurni i usklađeni s pravilima organizacije. Na primjer, privatni uređaji zaposlenika mogu pristupiti mreži samo ako ispunjavaju sigurnosne zahtjeve, poput instalacije antivirusnog softvera ili korištenja VPN-a. Ovo je važno jer smanjuje rizik od neovlaštenog pristupa putem nesigurnih ili kompromitiranih uređaja.

4.3. Proces implementacije

Nakon što sam identificirala ključne podatke, korisnike i uređaje, prešla sam na

implementaciju sigurnosnih alata unutar Office 365. Ovi alati omogućili su primjenu Zero Trust modela, pružajući zaštitu na više razina. Kroz detaljno planiranje i tehničku provedbu, osigurala sam da svaki alat bude pravilno konfiguriran kako bi pružio maksimalnu razinu sigurnosti. U nastavku slijedi tehnički opis svake implementacije.

4.3.1. Microsoft Defender za Office 365

Microsoft Defender za Office 365 je alat za zaštitu e-pošte, datoteka i aplikacija unutar Office 365 okruženja. Njegova glavna funkcija je detekcija i blokiranje naprednih prijetnji poput phishing napada, ransomware napada i zlonamjernog softvera.

Tehnička implementacija:

- Konfiguracija zaštite e-pošte: Microsoft Defender postavlja se tako da automatski skenira sve dolazne i odlazne poruke unutar Exchange Online servisa. Unutar administrativne konzole definiraju se pravila koja filtriraju sumnjive privitke i blokiraju poruke koje sadrže potencijalno zlonamjerne poveznice. Kako bih dodatno zaštitila korisnike od zlonamjernih sadržaja, koristila sam funkcionalnosti Safe Links i Safe Attachments. Funkcionalnost Safe Links osigurava zaštitu korisnika skeniranjem svih poveznica unutar e-poruka i dokumenata u stvarnom vremenu. Poveznice se provjeravaju svaki put kad ih korisnik klikne, osiguravajući da se blokira pristup zlonamjernim ili phishing web-stranicama. Tako Safe Links kontinuirano pruža zaštitu od zlonamjernih poveznica, čak i ako se prijetnja pojavi nakon što je e-poruka isporučena. S druge strane, Safe Attachments pruža zaštitu skeniranjem svih privitaka prije nego što ih korisnici otvore. Privitci se šalju u sigurno virtualno okruženje (sandbox) gdje se testiraju na prisutnost zlonamjernog softvera. Ako je privitak zaražen, blokira se pristup korisnicima, čime se sprječava otvaranje opasnih datoteka. Ove funkcionalnosti zajedno osiguravaju sveobuhvatnu zaštitu e-poruka, filtrirajući zlonamjerne poveznice i privitke, smanjujući rizik od napada unutar Office 365 okruženja.
- Automatsko blokiranje prijetnji: Postavila sam pravilo prema kojem Microsoft Defender automatski blokira pristup svim dokumentima koji sadrže zlonamjerni softver, osiguravajući da korisnici ne mogu otvoriti ili preuzeti sumnjive datoteke koje bi mogle ugroziti sigurnost sustava. Ovaj proces uključuje trenutnu detekciju zlonamjernih sadržaja unutar dokumenata, gdje Defender identificira potencijalno opasan softver poput virusa, ransomwarea ili trojanaca i odmah sprječava daljnju

interakciju korisnika s takvim datotekama. Administratori automatski primaju obavijesti o svim sumnjivim aktivnostima ili zlonamjernim datotekama, što im omogućuje brzu reakciju i dodatne sigurnosne provjere. Defender također automatski prebacuje sve sumnjive datoteke i e-poruke u karantenu, gdje su privremeno izolirane od ostatka sustava. Time se omogućuje daljnja analiza od strane sigurnosnog tima, koji zatim može odlučiti o sljedećim koracima – bilo da se datoteka trajno blokira, ukloni ili ponovno omogući ako se utvrdi da je sigurna. Ovaj sustav automatske blokade i karantene značajno smanjuje rizik od širenja zlonamjernog softvera unutar organizacije, osiguravajući da svaki potencijalni incident bude temeljito istražen i obrađen prije nego što može nanijeti štetu.

- Smanjenje lažno pozitivnih rezultata: Uvela sam pravila za smanjenje broja lažno pozitivnih prijetnji koristeći tehnologije kao što su strojno učenje i analiza uzoraka ponašanja korisnika. Ova pravila osmišljena su kako bi sustav mogao preciznije razlikovati stvarne prijetnje od uobičajenih korisničkih aktivnosti koje su možda netočno označene kao sumnjive. Primjenom strojnog učenja, sustav automatski prepoznaje obrasce u ponašanju korisnika, poput učestalih prijava s određenih uređaja ili pristupa određenim podacima, te na temelju tih podataka prilagođava sigurnosne postavke kako bi smanjio broj lažno pozitivnih detekcija. Na primjer, ako korisnik često pristupa određenim dokumentima s iste lokacije i uređaja, sustav može prilagoditi svoja pravila kako ne bi stalno označavao takvo ponašanje kao sumnjivo. Administratori su također dobili prilagođene alate za upravljanje karantenom i filtriranje sumnjivih e-poruka. Ovi alati omogućuju im da brzo pregledaju izolirane datoteke i e-poruke, te da na temelju dodatne analize donesu odluke o njihovom vraćanju ili trajnom uklanjanju. Tako je moguće bolje upravljati potencijalnim prijetnjama, a ujedno osigurati da ne dolazi do nepotrebnih prekida u radu zbog lažno označenih prijetnji.

Microsoft Defender osigurao je naprednu zaštitu od prijetnji i omogućio siguran protok informacija unutar organizacije. Pravilnom konfiguracijom, značajno sam smanjila mogućnost phishing napada i infekcije zlonamjernim softverom putem e-pošte i privitaka.

4.3.2. Uvjetni pristup (Conditional Access)

Uvjetni pristup (Conditional Access) omogućava definiranje pravila koja određuju tko može

pristupiti određenim resursima, na temelju različitih uvjeta poput lokacije, uređaja i sigurnosnih postavki. Ovo je ključan alat Zero Trust modela jer osigurava kontrolu pristupa na temelju usklađenosti uređaja i korisničkih postavki.

Tehnička implementacija:

- Postavljanje uvjetnih pravila: Korištenjem Azure Active Directory (AAD), definirala sam pravila koja uvjetuju pristup Office 365 aplikacijama i podacima. Pristup osjetljivim podacima dozvoljen je samo s uređaja koji zadovoljavaju sigurnosne standarde, kao što su instaliran antivirusni softver i ažuriran operativni sustav. Uvjetni pristup implementirala sam za sve ključne aplikacije, poput SharePointa i OneDrivea.
- Lokacijska ograničenja: Uvjetni pristup konfigurirala sam tako da blokira prijave s određenih zemljopisnih lokacija ili nepoznatih IP adresa. Korisnicima je dozvoljen pristup osjetljivim podacima samo unutar korporativne mreže ili putem VPN-a. Ova pravila uvela sam kako bih spriječila napade putem kompromitiranih uređaja iz neovlaštenih lokacija.
- Provjera usklađenosti uređaja: Korištenjem Microsoft Intune, konfigurirala sam pravila za provjeru usklađenosti uređaja. Uređaji koji ne zadovoljavaju sigurnosne standarde, poput zastarjelog antivirusnog softvera ili nedostatka enkripcije, automatski su blokirani pri pokušaju pristupa mrežnim resursima. Implementirala sam Mobile Device Management (MDM) kako bih osigurala kontrolu nad mobilnim uređajima.

Uvjetni pristup osigurao je da samo provjereni korisnici s usklađenih uređaja mogu pristupiti osjetljivim podacima i aplikacijama, što je značajno smanjilo rizik od neovlaštenog pristupa i kompromitacije podataka.

4.3.3. Višefaktorska autentifikacija (MFA)

Višefaktorska autentifikacija (MFA) jedan je od najvažnijih sigurnosnih slojeva u Zero Trust modelu jer dodaje dodatni faktor provjere prilikom prijave korisnika, smanjujući rizik od neovlaštenog pristupa čak i ako su lozinke kompromitirane.

Tehnička implementacija:

- Omogućavanje MFA za sve korisnike: Koristeći Azure Active Directory (Azure AD), konfigurirala sam višefaktorsku autentifikaciju (MFA) kako bi svi korisnici unutar organizacije morali koristiti dodatni sloj sigurnosti prilikom prijave. Prvo se koristi

tradicionalna lozinka, nakon čega se zahtijeva dodatni faktor autentifikacije, poput jednokratnog koda (OTP) poslanog putem mobilne aplikacije, SMS-a ili telefonskog poziva. Za tehničku implementaciju, kreirala sam pravila unutar Azure AD administrativne konzole koja definiraju vrste autentifikacijskih faktora prihvaćenih za MFA te sam omogućila sinkronizaciju sa svim korisničkim računima unutar Office 365. Ova metoda osigurava višeslojnu sigurnost i zaštitu od neovlaštenih pristupa, čak i u slučajevima kada je lozinka kompromitirana.

- Dodatni slojevi zaštite za privilegirane korisnike Posebnu pažnju posvetila sam korisnicima s višim privilegijama, poput administratora i zaposlenika koji imaju pristup osjetljivim podacima i resursima unutar organizacije. Za te korisnike, konfigurirala sam obaveznu MFA pri svakoj prijavi, bez obzira na lokaciju ili uređaj s kojeg pristupaju. Također sam uključila dodatne slojeve zaštite koristeći biometrijske podatke (npr. otisak prsta ili prepoznavanje lica) kao drugi faktor autentifikacije. Korištenjem Azure AD Conditional Access značajke, postavila sam pravila koja ovim korisnicima omogućuju pristup samo ako su ispunjeni strogi uvjeti usklađenosti uređaja i sigurnosnih politika, čime sam smanjila mogućnost zloupotrebe privilegiranih računa.Samoposlužno resetiranje lozinke (Self-service password reset): Implementirala sam funkcionalnost koja omogućava korisnicima da samostalno resetiraju lozinke koristeći MFA, čime sam smanjila administrativno opterećenje i poboljšala sigurnost.

Višefaktorska autentifikacija je osigurala dodatnu razinu sigurnosti, smanjujući rizik od kompromitiranja korisničkih računa i omogućila siguran pristup korisnicima čak i s udaljenih lokacija.

4.3.4. Azure Active Directory (AAD) i Role-Based Access Control (RBAC)

Azure Active Directory (AAD) omogućuje centralizirano upravljanje identitetima i pristupima unutar Office 365, dok Role-Based Access Control (RBAC) osigurava da korisnici imaju pristup samo onim resursima koji su im potrebni za obavljanje svojih poslova.

Tehnička implementacija:

- Kreiranje korisničkih grupa i uloga: U Azure Active Directory (AAD) kreirala sam korisničke grupe temeljene na odjelima i funkcijama unutar organizacije, kako bih pojednostavila upravljanje pravima pristupa. Ovaj proces uključuje definiranje uloga

prema poslovnim zahtjevima svakog odjela. Na primjer, IT odjel dobio je proširene privilegije za administraciju sustava, dok su financijski odjeli dobili ograničen pristup aplikacijama i podacima potrebnim za njihove zadatke, poput pristupa financijskim izvještajima ili alatima za upravljanje budžetom. Implementacija ovih pravila u AAD-u omogućila je jednostavnije upravljanje korisničkim pravima i pristupima kroz cijeli sustav Office 365. Pomoću RBAC-a, definirala sam precizna pravila pristupa koja osiguravaju da korisnici imaju pristup samo onim resursima koji su im potrebni, čime se minimizira mogućnost zloupotrebe privilegija. Pravila pristupa temeljena na ulogama smanjuju rizik od pogrešaka i povećavaju sigurnost, jer su pristupi strogo kontrolirani i automatski prilagođeni temeljem korisničke grupe i funkcije.

- Privileged Identity Management (PIM): Kako bih dodatno zaštitila osjetljive resurse i korisnike s višim privilegijama, aktivirala sam Privileged Identity Management (PIM) unutar Azure AD-a. PIM omogućuje upravljanje privilegiranim korisnicima i njihovim pristupima, pružajući dodatnu razinu kontrole nad ovlaštenjima. Ovaj alat osigurao je da korisnici s višim privilegijama, poput IT administratora ili financijskih menadžera, imaju pristup osjetljivim resursima samo kada je to potrebno, na privremenoj osnovi. Tehnička implementacija uključivala je konfiguriranje PIM-a tako da se privilegirani pristup dodjeljuje samo na zahtjev, uz vremenski ograničen pristup određenim resursima. Nakon isteka tog perioda, korisnicima se automatski ukidaju dodatne privilegije, čime se smanjuje rizik od zlonamjernih aktivnosti ili pogrešaka uzrokovanih nepotrebnim pristupom. Također, omogućena je dvostruka autentifikacija za privilegirane korisnike kako bi se osigurala dodatna sigurnost prilikom svakog pokušaja pristupa osjetljivim podacima.

Centralizirano upravljanje identitetima i pristupima omogućilo mi je učinkovitu kontrolu nad korisničkim pristupima i smanjilo rizik od neovlaštenog korištenja privilegiranih računa.

4.3.5. Microsoft Information Protection (MIP)

Microsoft Information Protection (MIP) omogućava klasifikaciju i zaštitu osjetljivih podataka unutar Office 365, što je ključno za zaštitu povjerljivih informacija unutar organizacije.

Tehnička implementacija:

- Klasifikacija podataka: Korištenjem MIP-a, postavila sam automatske oznake za klasifikaciju dokumenata na temelju njihovog sadržaja, što uključuje prepoznavanje

osjetljivih podataka poput financijskih informacija, osobnih identifikacijskih podataka (PII), brojeva kreditnih kartica i medicinskih podataka. Ova klasifikacija temelji se na unaprijed definiranim pravilima unutar Microsoft 365 Compliance Centra, gdje sam konfigurirala uvjete za klasifikaciju dokumenata. Na primjer, postavila sam da se dokumenti koji sadrže ključne riječi ili obrasce (npr. obrasci za identifikacijske brojeve ili osjetljive financijske podatke) automatski označe kao "Povjerljivi" ili "Visoko povjerljivi". MIP-ova funkcionalnost automatske klasifikacije omogućila mi je primjenu oznaka na dokumente u stvarnom vremenu, čak i bez intervencije korisnika. Oznake su povezane s pravilima za zaštitu, kao što su automatsko šifriranje i sprječavanje prijenosa podataka izvan organizacije. Implementirala sam senzore za osjetljive podatke, koji prepoznaju različite obrasce i fraze specifične za industriju, poput brojeva osobnih iskaznica ili medicinskih zapisa, te prema njima klasificiraju podatke.

- Automatska zaštita podataka: Primijenila sam pravila za automatsko šifriranje podataka korištenjem Azure Information Protection (AIP). To omogućuje automatsko šifriranje dokumenata koji sadrže osjetljive informacije, poput financijskih izvještaja, pravnih dokumenata ili osobnih podataka, što ih čini nečitljivima za neovlaštene korisnike. Šifriranje je konfigurirano tako da se automatski aktivira u trenutku kada dokument postane klasificiran kao "Povjerljiv" ili "Visoko povjerljiv" .Pravila za sprječavanje gubitka podataka (DLP) integrirala sam unutar MIP-a kako bih osigurala da povjerljivi dokumenti ne mogu biti dijeljeni ili slani izvan organizacije bez odobrenja. DLP pravila automatski skeniraju e-poruke i datoteke za osjetljive podatke te sprječavaju korisnike da te podatke dijele putem e-maila, OneDrivea ili drugih dijeljenih platformi bez odobrenja. Ako korisnik pokuša poslati zaštićeni dokument izvan organizacije, pravilo DLP automatski blokira prijenos ili zahtijeva dodatnu autorizaciju.Konfigurirala sam Conditional Access pravila unutar Azure AD-a kako bih dodatno osigurala da samo autorizirani korisnici i uređaji mogu pristupiti osjetljivim podacima. Primjenom detaljnih uvjeta pristupa osigurano je da pristup povjerljivim dokumentima bude omogućen samo korisnicima koji prolaze višefaktorsku autentifikaciju (MFA), dok pristupi iz nepoznatih ili neuobičajenih lokacija budu automatski blokirani.

MIP je osigurao da su svi povjerljivi podaci unutar organizacije pravilno klasificirani i zaštićeni, čime sam smanjila rizik od neovlaštenog dijeljenja i curenja podataka.

Tehnička implementacija ovih alata u Office 365 omogućila mi je da osiguram cjelovitu zaštitu podataka, korisnika i uređaja unutar organizacije. Korištenjem alata poput Microsoft Defendera, MFA, uvjetnog pristupa, AAD-a i MIP-a, uspješno sam primijenila Zero Trust model, što je omogućilo značajno poboljšanje sigurnosti organizacije i zaštitu od naprednih prijetnji. Ovi alati su neophodni za održavanje visoke razine sigurnosti u složenom okruženju poput Office 365, a pravilna implementacija osigurala je da su svi resursi organizacije zaštićeni na odgovarajući način.

4.4. Praćenje i dogovor na incidente

Praćenje i odgovor na sigurnosne incidente igraju značajnu ulogu u primjeni Zero Trust modela u Office 365. U ovom koraku, implementirala sam alate i postavila procese koji omogućuju kontinuirano praćenje mrežnih aktivnosti i pravovremeni odgovor na sigurnosne prijetnje. Praćenje je ključan element Zero Trust modela jer omogućuje stalnu provjeru i nadzor svih korisnika, uređaja i aplikacija. Ujedno, učinkovito upravljanje incidentima osigurava brz odgovor na potencijalne prijetnje kako bi se minimizirale moguće štete.

4.4.1. Implementacija sustava za praćenje

Kako bih osigurala kontinuirano praćenje svih aktivnosti unutar Office 365, implementirala sam alate koji omogućuju nadzor nad svim događajima unutar sustava. Alati za praćenje pružaju uvid u aktivnosti korisnika, promjene u postavkama sigurnosti, prijave s različitih lokacija i druge ključne događaje.

Tehnička implementacija:

- Microsoft Defender for Identity: Ovaj alat implementirala sam kako bi omogućio kontinuirano praćenje korisničkog ponašanja i otkrivanje anomalija. Defender for Identity nadzire pristup osjetljivim podacima i ponašanje korisnika unutar mreže te identificira potencijalno sumnjive aktivnosti poput neobičnih prijava ili neuobičajenog preuzimanja podataka.
- Microsoft Cloud App Security (MCAS): Postavila sam MCAS za praćenje cloud aplikacija koje korisnici koriste unutar Office 365. MCAS omogućava detaljno praćenje korištenja aplikacija, aktivnosti prijava, dijeljenja datoteka i pristupa podacima. Na temelju pravila koja sam definirala, MCAS automatski označava

sumnjive aktivnosti poput neuobičajenog volumena preuzimanja datoteka ili pristupa s novih uređaja.

- Microsoft Sentinel: Za centralizirano praćenje i upravljanje sigurnosnim događajima, implementirala sam Microsoft Sentinel kao platformu za prikupljanje podataka iz različitih izvora, uključujući Defender, MCAS i druge alate. Sentinel omogućava analizu prikupljenih podataka, identifikaciju obrazaca prijetnji i automatski generira alarme u slučaju potencijalnih sigurnosnih incidenata.

Korištenjem ovih alata osigurala sam stalno praćenje svih korisničkih i mrežnih aktivnosti, što je ključan aspekt Zero Trust modela. Ova vrsta nadzora omogućila mi je brzu detekciju sumnjivih događaja, kao što su neovlaštene prijave ili neobično ponašanje korisnika, i pravovremenu reakciju na potencijalne sigurnosne incidente.

4.4.2. Definiranje pravila za generiranje alarma

Nakon postavljanja sustava za praćenje, konfigurirala sam specifična pravila za generiranje alarma u slučaju detekcije neobičnih ili sumnjivih aktivnosti. Pravila su prilagođena prema specifičnim sigurnosnim potrebama organizacije i uključuju različite scenarije poput sumnjivih prijava, pokušaja pristupa osjetljivim podacima i neovlaštenih promjena postavki.

Tehnička implementacija:

- Automatsko generiranje alarma: Definirala sam alarme za razne aktivnosti koje ukazuju na potencijalne prijetnje, poput prijava iz nepoznatih ili nesigurnih lokacija, promjene privilegija korisnika, kao i neovlaštenih pokušaja pristupa podacima. Na primjer, ako se detektira prijava s uređaja koji nije ranije korišten ili iz geografske lokacije izvan organizacije, sustav automatski generira alarm.
- Integracija s Microsoft Sentinelom: Koristeći Microsoft Sentinel, konfigurirala sam automatizirane odgovore na incidente. Sentinel prikuplja podatke iz Defendera i drugih alata, kreira "playbooks" koji automatski pokreću odgovore na specifične prijetnje, poput blokiranja korisničkog računa ili izolacije uređaja u slučaju sumnje na kompromitaciju.

Zašto je ovo važno? Automatizacija generiranja alarma omogućila mi je brzu detekciju prijetnji bez potrebe za stalnim ljudskim nadzorom. Postavljanjem preciznih pravila osigurala sam da sustav sam prepozna potencijalno opasne situacije i odmah obavijesti sigurnosne timove, čime sam smanjila vrijeme reakcije na incidente.

4.4.3. Odgovor na incidente

U sklopu Zero Trust modela, od iznimne je važnosti da postoji jasan plan za odgovor na incidente kako bi se minimizirala šteta u slučaju sigurnosnih prijetnji. Nakon što je identificiran potencijalni incident, postavila sam sustav za brzu reakciju i rješavanje problema, koristeći automatske odgovore i intervenciju sigurnosnih timova.

Tehnička implementacija:

- Izolacija sumnjivih uređaja: U slučaju otkrivanja neovlaštenog pristupa ili kompromitiranih uređaja, implementirala sam automatski mehanizam koji odmah izolira sumnjive uređaje iz mreže kako bi se spriječila daljnja kompromitacija. Microsoft Defender za krajnje točke (Endpoint) automatski izolira uređaje koji pokazuju znakove zlonamjernog softvera ili neuobičajenog ponašanja.
- Blokiranje kompromitiranih korisničkih računa: Korištenjem Azure AD-a, implementirala sam pravila za automatsko blokiranje ili onemogućavanje korisničkih računa u slučaju pokušaja neovlaštenih prijava. Tako napadač koji je kompromitirao korisnički račun odmah biva spriječen u daljnjim radnjama, dok se računu može pristupiti samo nakon dodatne provjere.
- Odgovor putem Sentinel playbooks-a: Sentinel playbooks omogućili su da se nakon detekcije incidenta automatski pokrenu unaprijed definirani odgovori, poput automatske obavijesti sigurnosnih timova, blokiranja pristupa podacima i izolacije mrežnih resursa.

Zašto je ovo važno? Brz i automatiziran odgovor na incidente ključan je za smanjenje utjecaja sigurnosnih prijetnji. Automatskim izoliranjem sumnjivih uređaja i blokiranjem kompromitiranih korisničkih računa, uspjela sam brzo reagirati i minimizirati potencijalnu štetu prije nego što se incident proširi.

4.5. Upravljanje incidentima i revizija

Osim brzog odgovora na incidente, ključno je imati jasan proces za upravljanje incidentima i kasniju reviziju. Ovaj proces omogućava analizu svakog incidenta, procjenu što se dogodilo i definiranje mjera za sprječavanje sličnih incidenata u budućnosti.

Tehnička implementacija:

- Zapisivanje svih incidenata: Svaki incident automatski se bilježi unutar Sentinel sustava, zajedno s detaljima o tome tko je bio uključen, koji su podaci bili ugroženi i kako je došlo do incidenta. Ovi podaci su ključni za kasniju analizu i prilagodbu sigurnosnih mjera.
- Post-incident analiza: Nakon svakog incidenta, provodim post-mortem analizu kako bih utvrdila što je uzrokovalo incident i koje mjere je potrebno dodatno prilagoditi. Ove informacije koristim za prilagodbu pravila uvjetnog pristupa, MFA postavki i drugih sigurnosnih parametara.
- Revizija korisničkog ponašanja: Na temelju podataka prikupljenih od Microsoft Defendera, MCAS-a i Sentinela, redovito provodim reviziju korisničkog ponašanja. Ovaj proces omogućava uočavanje obrazaca koji bi mogli ukazivati na buduće prijetnje, što omogućuje unaprijed definirane reakcije i prilagodbu sigurnosnih postavki.

Upravljanje incidentima omogućuje ne samo brzu reakciju na sigurnosne prijetnje, već i učenje iz svakog incidenta kako bi se sustav kontinuirano poboljšavao. Na ovaj način, organizacija postaje otpornija na buduće prijetnje jer se pravila i alati stalno prilagođavaju novim izazovima.

4.6. Rezultati i koristi

Implementacija Zero Trust modela unutar Office 365 donijela je konkretne rezultate i značajne koristi za sigurnost organizacije. Kroz sve faze implementacije – od identifikacije ključnih podataka, korisnika i uređaja, do praćenja i odgovora na incidente – postigli smo višu razinu zaštite, smanjili sigurnosne rizike i unaprijedili kontrolu nad mrežnim resursima. U ovom dijelu prikazujemo postignute rezultate i koristi koje su proizašle iz ove implementacije.

4.6.1. Povećana razina sigurnosti podataka

Jedan od najvažnijih rezultata bio je značajan porast sigurnosti osjetljivih podataka. Implementacijom alata poput Microsoft Defendera, uvjetnog pristupa i Microsoft Information Protectiona (MIP), uspjeli smo zaštititi podatke od neovlaštenog pristupa i curenja.

Rezultati:

- Smanjenje rizika od neovlaštenog pristupa: Korištenjem višefaktorske autentifikacije (MFA) i uvjetnog pristupa, osigurali smo da samo verificirani korisnici i uređaji mogu pristupiti osjetljivim podacima. Ova mjera je značajno smanjila broj potencijalnih incidenata vezanih uz neovlaštene pristupe.
- Zaštita povjerljivih podataka: Implementacija MIP-a omogućila je pravilnu klasifikaciju podataka i primjenu automatskog šifriranja na osjetljive dokumente, čime je spriječeno curenje povjerljivih informacija. Osjetljivi podaci, poput financijskih izvještaja i osobnih podataka zaposlenika, sada su bolje zaštićeni i manje podložni zloupotrebama.

Koristi: Viša razina sigurnosti podataka osigurala je usklađenost s regulativama poput GDPR-a i smanjila rizik od financijskih i reputacijskih šteta povezanih s curenjem podataka. Također, organizacija je sada bolje zaštićena od naprednih prijetnji poput ransomwarea i phishing napada.

4.6.2. Poboljšana kontrola pristupa

Korištenje Role-Based Access Control (RBAC) i uvjetnog pristupa omogućilo je detaljniju i precizniju kontrolu nad time tko ima pristup određenim podacima i resursima. Postavljanjem jasnih pravila o pristupu, osigurali smo da korisnici imaju samo one ovlasti koje su im potrebne za obavljanje svakodnevnih zadataka.

Rezultati:

- Bolja segmentacija pristupa: Korištenjem RBAC-a, postigli smo da su administratori, financijski odjeli i vanjski suradnici ograničeni na samo one resurse koji su relevantni za njihove poslove. Ovo je minimiziralo mogućnost zloupotrebe privilegija i neovlaštenog pristupa osjetljivim podacima.
- Zaštita od napada iznutra: Uvođenjem strožih pravila pristupa, smanjili smo mogućnost zloupotrebe povlastica i spriječili napade iznutra, odnosno napade koji dolaze od ovlaštenih korisnika koji bi mogli zloupotrijebiti svoj pristup.

Koristi: Precizna kontrola pristupa omogućila je organizaciji da smanji rizik od zloupotreba i da u stvarnom vremenu upravlja pristupima. Ovo je povećalo sigurnost bez narušavanja produktivnosti zaposlenika, jer im je pristup bio prilagođen njihovim poslovnim potrebama.

4.6.3. Brži odgovor na sigurnosne incidente

Implementacija sustava za praćenje putem Microsoft Defendera, Cloud App Security (MCAS) i Microsoft Sentinela omogućila je brzo prepoznavanje prijetnji i pravovremeni odgovor na incidente. Automatizirani sustavi za praćenje detektirali su sumnjive aktivnosti u stvarnom vremenu i omogućili sigurnosnim timovima brzu reakciju.

Rezultati:

- Smanjeno vrijeme reakcije: Korištenje automatiziranih alarma i Sentinel playbooks-a značajno je smanjilo vrijeme potrebno za reakciju na sigurnosne incidente. Incidenti poput neovlaštenih prijava ili pokušaja pristupa osjetljivim podacima odmah su prepoznati i riješeni.
- Učinkovitija izolacija prijetnji: Automatizacija je omogućila brzu izolaciju sumnjivih uređaja i korisničkih računa, čime je spriječeno širenje prijetnji unutar mreže.

Koristi: Brži i automatiziran odgovor na incidente smanjio je potencijalne štete koje bi mogli uzrokovati napadači. Organizacija sada ima bolju kontrolu nad sigurnosnim događajima, a napadi su svedeni na minimum prije nego što su uspjeli izazvati ozbiljnije posljedice.

4.6.4. Smanjeni broj sigurnosnih incidenata

Nakon primjene Zero Trust modela, došlo je do značajnog smanjenja broja sigurnosnih incidenata unutar organizacije. Korištenjem više slojeva sigurnosti, automatiziranih pravila i stalnog praćenja, broj potencijalnih prijetnji i stvarnih incidenata značajno je smanjen.

Rezultati:

- Pad u broju phishing napada: Korištenjem MFA-a i Microsoft Defendera, blokirali smo većinu phishing napada prije nego što su stigli do korisnika. Time smo smanjili rizik od krađe identiteta i kompromitiranja korisničkih računa.
- Manji broj kompromitiranih uređaja: Korištenjem pravila uvjetnog pristupa i provjere usklađenosti uređaja, značajno smo smanjili broj uređaja koji su kompromitirani zbog zlonamjernog softvera ili neadekvatnih sigurnosnih postavki.

Koristi: Smanjenje broja incidenata omogućilo je organizaciji da se usredotoči na poslovne ciljeve bez stalnih prekida uzrokovanih sigurnosnim prijetnjama. Također, smanjeni broj napada i prijetnji smanjio je opterećenje na IT timove i sigurnosno osoblje.

4.6.5. Unaprijeđena usklađenost s regulativama

Korištenjem alata za zaštitu podataka poput MIP-a i Defendera, organizacija je uskladila svoje poslovanje s važećim zakonskim propisima poput GDPR-a i drugih industrijskih standarda.

Rezultati:

- Bolja zaštita osobnih podataka: Implementacija MIP-a omogućila je pravilnu zaštitu osobnih podataka zaposlenika i klijenata, čime je osigurana usklađenost s GDPR-om.
- Automatizirana pravila usklađenosti: Definirali smo pravila koja automatski primjenjuju mjere zaštite i šifriranja na osjetljive dokumente, čime smo smanjili mogućnost nenamjernog kršenja pravila usklađenosti.

Koristi: Osiguranje usklađenosti s regulativama smanjilo je rizik od pravnih posljedica i novčanih kazni te osiguralo povjerenje klijenata i partnera. Automatizacija pravila usklađenosti također je smanjila administrativne troškove povezane s ručnim procesima zaštite podataka.

Primjena Zero Trust modela unutar Office 365 rezultirala je znatnim povećanjem sigurnosti, boljom kontrolom nad pristupom i bržim odgovorom na sigurnosne incidente. Korištenjem alata kao što su Microsoft Defender, MFA, uvjetni pristup, MIP i Sentinel, organizacija je značajno smanjila broj sigurnosnih prijetnji, poboljšala zaštitu podataka i osigurala usklađenost s regulativama. Ovi rezultati omogućili su organizaciji da djeluje sigurnije, učinkovitije i pouzdanije u današnjem izazovnom kibernetičkom okruženju.

5. ZAKLJUČAK

Kroz ovaj rad proučeni su ključni aspekti kibernetičke sigurnosti, počevši od teorijskih osnova pa sve do praktične primjene u stvarnom okruženju. U uvodnom dijelu analizirane su suvremene prijetnje s kojima se organizacije danas suočavaju, kao i sve složenije tehnike koje napadači koriste kako bi kompromitirali podatke i sustave. Rast prijetnji poput hakiranja, phishinga i ransomware napada pokazuje koliko je važno kontinuirano ulagati u zaštitu informacija i prilagođavati sigurnosne strategije promjenjivom digitalnom okruženju.

Teorijski dio rada dao je uvid u temeljne koncepte kibernetičke sigurnosti, uključujući povjerljivost, integritet, dostupnost i autentifikaciju. Ovi principi čine osnovu svakog sigurnosnog okvira, a Zero Trust model pokazao se kao ključan u modernim IT sustavima, osobito onima koji koriste oblak i podržavaju rad na daljinu. Zero Trust model, koji se temelji na stalnoj provjeri identiteta i ograničenju pristupa na osnovi najmanjih privilegija, posebno je važan za organizacije koje teže potpunoj kontroli nad pristupom podacima i sustavima.

U pregledu kibernetičkih prijetnji i metodologija analizirana je rastuća sofisticiranost napada te kako nove tehnologije, poput umjetne inteligencije, omogućuju napadačima razvoj naprednijih tehnika. Upravljanje rizicima, segmentacija mreže i višefaktorska autentifikacija pokazale su se ključnima u suzbijanju ovih prijetnji. Zero Trust model nudi robustan okvir za postizanje višeslojne zaštite, čime se smanjuje površina napada i poboljšava sigurnosna postavka organizacija.

Praktična implementacija Zero Trust modela unutar Office 365 okruženja donijela je konkretne rezultate, poboljšala zaštitu podataka i omogućila preciznu kontrolu pristupa. Kroz procjenu sigurnosnih potreba, identifikaciju ključnih podataka i korisnika te implementaciju alata poput Microsoft Defendera i višefaktorske autentifikacije, postignuta je viša razina sigurnosti i smanjenje rizika od neovlaštenog pristupa. Posebno važan dio bila je kontinuirana revizija i praćenje svih aktivnosti unutar sustava, čime je omogućena brza reakcija na incidente.

Rezultati ove implementacije pokazuju da je Zero Trust model donio mnogobrojne koristi, uključujući smanjenje sigurnosnih incidenata, bolju zaštitu osjetljivih podataka i jaču usklađenost s regulativama poput GDPR-a. Sigurnosna infrastruktura sada omogućuje

organizaciji da se učinkovitije nosi s prijetnjama i osigura stabilan i pouzdan rad svojih sustava.

Preporuke za buduće istraživanje uključuju dublju analizu sigurnosnih izazova vezanih uz IoT uređaje te daljnji razvoj sigurnosnih politika koje bi obuhvatile nove tehnologije i metode napada. Također, važno je kontinuirano prilagođavati sigurnosne mjere u skladu s promjenama u kibernetičkom krajoliku i održavati visoku razinu edukacije zaposlenika. Na taj način organizacije mogu ostati otporne na sve složenije prijetnje.

LITERATURA

1. Johnson, T. A., (2020), *Cybersecurity: Protecting Critical Infrastructures from Cyber Attacks and Cyber Warfare*, CRC Press.
2. Cox, C., (2020), *Everyday Cybersecurity: A Practical Approach to Understanding Cybersecurity, Security Awareness, and Protecting Your Personal Information and Identity*, Z-lib.org.
3. Anderson, B., (2021), *Theory and Application of Zero Trust Security: A Brief Overview*
4. Imperva, (2021), *Cybersecurity Risk Management*, https://www.imperva.com/learn/data-security/cybersecurity-risk-management/ (pristupljeno 01.09.2024.)
5. CyberArk, (2021), *What is Defense in Depth?*, https://www.cyberark.com/what-is/defense-in-depth/ (pristupljeno 03.09.2024..)
6. SecureWorld, (2021), *Zero Trust Implementation Challenges*, https://www.secureworld.io/industry-news/zero-trust-implementation-challenges (pristupljeno 04.09.2024.)
7. Cyberight, (2021), *Zero Trust Pillars*, https://www.cyberight.com/zero-trust-pillars (pristupljeno 07.09. 2024.)
8. SoftwareLab, (2021), *SoftwareLab Report: Security Solutions*, https://www.softwarelab.com/ (pristupljeno 08.09. 2024.)

SAŽETAK

Ovaj završni rad istražio je ključne izazove kibernetičke sigurnosti s fokusom na implementaciju Zero Trust modela u Office 365 okruženju. Rad je započeo analizom rastućih prijetnji poput ransomwarea i phishinga, te ukazao na potrebu višeslojnog pristupa sigurnosti. Teorijski dio obuhvatio je ključne koncepte povjerljivosti, integriteta i dostupnosti, dok je praktični dio pokazao uspješnu primjenu Zero Trust principa.

Kroz implementaciju alata kao što su višefaktorska autentifikacija (MFA), Microsoft Defender i Microsoft Information Protection (MIP), postignuta je veća sigurnost podataka i smanjen rizik od neovlaštenog pristupa. Automatizirani sustavi omogućili su brže reakcije na sigurnosne incidente, dok su napredni alati za upravljanje identitetima (PIM) dodatno osigurali osjetljive resurse. Zaključno, ovaj rad naglašava važnost proaktivnog pristupa kibernetičkoj sigurnosti, primjenom Zero Trust modela koji značajno smanjuje rizike, poboljšava zaštitu podataka i osigurava usklađenost s regulativama poput GDPR-a.

SUMMARY

This paper explored the key challenges of cybersecurity with a focus on the implementation of the Zero Trust model in the Office 365 environment. The work began by analyzing the growing threats such as ransomware and phishing, highlighting the need for a layered approach to security. The theoretical part covered the key concepts of confidentiality, integrity, and availability, while the practical part demonstrated the successful application of Zero Trust principles. Through the implementation of tools such as multi-factor authentication (MFA), Microsoft Defender, and Microsoft Information Protection (MIP), greater data security was achieved, and the risk of unauthorized access was reduced. Automated systems enabled faster responses to security incidents, while advanced identity management tools (PIM) provided additional protection for sensitive resources. In conclusion, this thesis emphasizes the importance of a proactive approach to cybersecurity, applying the Zero Trust model, which significantly reduces risks, improves data protection, and ensures compliance with regulations such as GDPR.