ALFA BK UNIVERZITET

FAKULTET INFORMACIONIH TEHNOLOGIJA

DEFENSE IN DEPTH STRATEGIJA INFORMACIONE SIGURNOSTI ZA PREDUZEĆA MALE I SREDNJE VELIČINE U BIH

doktorska disertacija

Mentor:

Doc. dr Aleksandar Zakić

Kandidat:

Alen Kamiš

br. ind. 2021/5902

Beograd 2026. godine

ALFA BK UNIVERSITY

FACULTY OF INFORMATION TEHNOLOGY

DEFENSE IN DEPTH STRATEGY FOR INFORMATION SECURITY FOR SMALL AND MEDIUM ENTERPRISES IN BOSNIA AND HERZEGOVINA

PhD Thesis

Mentor:

Prof. Aleksandar Zakić, PhD

Candidate:

Alen Kamiš

2021/5902

Belgrade 2026. godine

IZJAVA MENTORA O PROCJENI ORIGINALONOSTI I SAGLASNOSTI ZA PREDAJU

URAĐENE DOKTORSKE DISERTACIJE

Ovim izjavljujem da sam nakon pregledanog rukopisa doktorske disertacije saglasan/na da kandidat Alen Kamiš može da preda Službi za posljediplomske studije Univerziteta urađenu doktorsku disertaciju pod nazivom:

DEFENSE IN DEPTH STRATEGIJA INFORMACIONE SIGURNOSTI ZA PREDUZEĆA MALE I SREDNJE VELIČINE U BIH

radi organizacije njene ocjene i odbrane, i da ista sadrži originalan naučni doprinos koji se sastoji od:

- razvoja i formalizacije modela procjene informacione bezbjednosti za mala i srednja preduzeća zasnovanog na Defense in Depth strategiji,
- definisanja i implementacije Indeksa informacione bezbjednosti (IIB) kao kvantitativnog pokazatelja nivoa sigurnosne zrelosti organizacija,
- integracije IIB indeksa u model procjene sajber rizika, čime je omogućena objektivna i mjerljiva evaluacija stanja i unapređenja informacione bezbjednosti,
- primjene statističkih metoda, uključujući hi-kvadrat test, radi empirijske validacije povezanosti između nivoa informacione bezbjednosti i organizacionih karakteristika preduzeća,
- razvoja metodološkog okvira za unapređenje informacione bezbjednosti MSP u Bosni i Hercegovini kroz implementaciju ključnih slojeva Defense in Depth strategije, uključujući firewall zaštitu, višefaktorsku autentifikaciju i mehanizme nadzora,
- empirijskog istraživanja koje pruža originalne rezultate o trenutnom stanju i nivou zrelosti informacione bezbjednosti u MSP sektoru u Bosni i Hercegovini.

Na osnovu izvršene procjene, konstatujem da doktorska disertacija predstavlja originalno naučno djelo, rezultat samostalnog istraživačkog rada kandidata, te da ispunjava sve uslove propisane važećim pravilima za pokretanje postupka ocjene i javne odbrane doktorske disertacije.

Beograd, 01.04.2026. godine

Doc.dr Aleksandar Zakić

_____

(potpis mentora)

Komisija

za pregled, ocjenu i javnu odbranu doktorske disertacije

_____

Dr Milan Gligorijević, redovni profesor, predsednik

FIT, Alfa BK Univerzitet, Beograd,

_____

Dr Aleksandar Zakić, docent, mentor

FIT, Alfa BK Univerzitet, Beograd,

_____

Dr Slaviša Trajković, redovni profesor, član

Ekonomski fakultet, Univerzitet u Prištini, Kosovska Mitrovica

_____

Dr Jelena Stojanović, docent, član

FMRN, Alfa BK Univerzitet, Beograd,

_____

Dr Lidija Beko, redovni profesor, član

Rudarsko-geološki fakultet, Univerzitet u Beogradu, Beograd,

Datum usmene odbrane:

Zahvalnica

Izražavam svoju duboku i iskrenu zahvalnost poštovanim profesorima na visokom nivou profesionalnosti, stručnosti i posvećenosti tokom mojih doktorskih studija. Njihovo znanje, akademska podrška i konstruktivan pristup značajno su doprinijeli mom naučnom i profesionalnom razvoju, kao i uspješnoj realizaciji ove doktorske disertacije.

Posebnu i neizmjernu zahvalnost dugujem svom mentoru, doc. dr Aleksandru Zakiću, na kontinuiranom stručnom vođenju, nesebičnoj podršci, kao i na pravovremenim, preciznim i izuzetno vrijednim savjetima i smjernicama. Njegova stručnost, akademsko iskustvo i posvećenost naučnoistraživačkom radu bili su od presudnog značaja za kvalitet, jasnoću i naučni doprinos ove doktorske disertacije.

Posebno se zahvaljujem svojim roditeljima na trajnoj podršci, razumijevanju i vrijednostima koje su mi usadili, a koje su predstavljale temelj mog obrazovanja i ličnog razvoja.

Iskrenu zahvalnost dugujem svojoj supruzi Lejli i mojoj djeci na strpljenju, razumijevanju i bezuslovnoj podršci tokom cjelokupnog trajanja doktorskih studija. Njihova podrška, ohrabrenje bili su neprocjenjiv izvor snage i motivacije tokom ovog zahtjevnog, ali izuzetno značajnog životnog i akademskog puta.

DEFENSE IN DEPTH STRATEGIJA INFORMACIONE SIGURNOSTI ZA PREDUZEĆA MALE I SREDNJE VELIČINE U BIH

Rezime: Ova studija pokušava da pronađe odgovore na najveće izazove u pogledu informacione sigurnosti malih i srednjih kompanija, ne samo u BiH, već cijelog svijeta.

Svrha rada je da menadžmentu preduzeća (prvenstveno IKT menadžeru) ponudi rješenja problema u organizaciji, upravljanju i optimizaciji poslovanja putem implementacije pojačane informacione sigurnosti sa ciljem postizanja pozitivnih poslovnih rezultata i konkurentnosti sa sve jačom konkurencijom otvorenog globalnog tržišta. Svi primjećujemo da je sve više preduzeća koja su bila kompromitovana ili su bila žrtve računarskih napada. Napadima se nanosi šteta preduzećima prvenstveno u materijalnom smislu (iznuda novca ili nedostupnost online servisa i sl.), ali također saznanjem da je to preduzeće bilo izloženo i kompromitovano, dolazi i do gubitka povjerenja kupaca, što proizvodi i manji profit kompanije.

Defense in Depth je strategija informacione sigurnosti koja kreira više barijernu zaštitu sa ciljem osiguravanja informacionih sistema sa što manjom mogućnošću izloženosti i nedostupnosti IKT sistema. Strategija pokušava da, kroz primjenu pojačanih metoda fizičke, hardverske, softverske zaštite i propisivanjem procedura i propisa za kompanije, smanji uticaj pokušaja napada i nedostupnosti IKT servisa preduzeća.

Defense in Depth kroz strategiju informacione sigurnosti bavi se fizičkom, mrežnom, endpoint sigurnošću i višefaktorskom autorizacijom kontrole pristupa. Pored ovih hardversko - softverskih strategija da bi se implementirala potrebne su sigurnosne politike i procedure koje pomažu i kod kontrole procesa. Politike i procedure veoma su korisne kod implementacije i konkurisanja preduzeća za izdavanja industrijskih standarda (npr. ISO 9000 ili ISO 27001). Također, kroz Defense in Depth strategiju obezbjeđuje se oporavak i zaštita podataka (Backup and Recovery). I na kraju ova strategija bavi se i nadgledanjem i otkivanjem potencijalnih sigurnosnih prijetnji u IKT sistemu.

Može se reći da ova Defense in Depth strategija informacione sigurnosti ima značajan uticaj na unapređenje poslovnih procesa, optimizaciju i smanjenje mogućnosti nedostupnosti IKT sistema čime se ostvaruju pozitivni rezultati poslovanja.

Ključne riječi: Informaciona sigurnost, Defense in Depth, računarski napadi

Naučna oblast: Informacione i komunikacione tehnologije

Uža naučna oblast: Informaciona sigurnost, računarske nauke

UDK:

DEFENSE IN DEPTH STRATEGY FOR INFORMATION SECURITY FOR SMALL AND MEDIUM ENTERPRISES IN BOSNIA AND HERZEGOVINA

Abstract: This study aims to find answers to the greatest challenges in information security for small and medium-sized enterprises, not only in Bosnia and Herzegovina but globally. The purpose of the paper is to offer the company's management (primarily the ICT manager) solutions to organizational, management, and business optimization problems through the implementation of enhanced information security, with the goal of achieving positive business results and maintaining competitiveness in the increasingly strong competition of the global open market.

We are all noticing that more and more companies have been compromised or have fallen victim to cyberattacks. These attacks cause harm to businesses, primarily in material terms (extortion, unavailability of online services, etc.), but also through the loss of trust from customers upon learning that the company has been exposed and compromised, leading to reduced profits.

Defense in Depth is an information security strategy that creates multi-layered protection aimed at securing information systems with minimal exposure and unavailability of ICT systems. The strategy seeks to reduce the impact of attack attempts and ICT service downtime for businesses by applying enhanced methods of physical, hardware, and software protection, as well as establishing procedures and regulations for companies.

Through its information security strategy, Defense in Depth addresses physical, network, endpoint security, and multi-factor authorization for access control. In addition to these hardware and software strategies, security policies and procedures are essential for implementation, as they help with process control. Policies and procedures are also highly useful when companies are applying for industry standards (e.g., ISO 9000 or ISO 27001). Furthermore, through the Defense in Depth strategy, data recovery and protection (Backup and Recovery) are ensured. Finally, this strategy involves monitoring and detecting potential security threats within ICT systems.

It can be said that the Defense in Depth information security strategy has a significant impact on improving business processes, optimizing operations, and reducing the likelihood of ICT system downtime, which in turn results in positive business outcomes.

Keywords: Information security, Defense in Depth, cyberattacks

Scientific area: Information and Communication Technologies

Narrower scientific field: Information Security, Computer Science

UDK:

Sadržaj

Popis skraćenica

ABAC - Attribute-Based Access Control (Kontrola pristupa zasnovana na atributima)
ACL - Access Control Lists (Pravila kontrole pristupa)
AES - Advanced Encryption Standard (enkripcijski standard)
AI - Artificial Intelligence (Vještačka inteligencija)
API - Application Programming Interface (Aplikacijski programski interfejs)
APS - Automation and Process System (Sistem za automatizaciju i upravljanje procesima)
APT - Advanced Persistent Threat (Napredna trajna prijetnja)
ATP - Advanced Threat Protection (Napredna zaštita od prijetnji)
BCP - Business Continuity Plan (Plan kontinuiteta poslovanja)
BIA - Business Impact Analysis (Analiza uticaja na poslovanje)
CERT - Computer Emergency Response Team (Tim za hitni odgovor na računarske sigurnosne incidente)
CMM - Cybersecurity Capacity Maturity Model for Nations (Model zrelosti kapaciteta sajber sigurnosti za države)
COBIT - Control Objectives for Information and Related Technologies (Framework za upravljanje i kontrolu IT)
CPU - Central Processing Unit (Procesor)
CSF - Cybersecurity Framework
CSIRT - Computer Security Incident Response Team (Tim za odgovor na sigurnosne incidente u informacionim sistemima)
CSRF - Cross-Site Request Forgery (Napad putem krivotvorenja zahtjeva između web stranica)
CVE - Common Vulnerabilities and Exposures (Zajednička lista sigurnosnih ranjivosti i izloženosti)
DAST - Dynamic application security testing (Dinamičko sigurnosno testiranje aplikacije)
DDoS - Distributed Denial of Service (Distribuirani napad uskraćivanja usluge)
DMZ - Demilitarized Zone (demilitarizovana zona)
DoS - Denial of Service (Napad uskraćivanja usluge)
DPI - Deep Packet Inspection (Dubinsku inspekciju paketa)
EMS - Element Management System (Sistem za upravljanje elementima)
ENISA - European Union Agency for Cybersecurity (Agencija Evropske unije za sajber sigurnost)
ERP - Enterprise Resource Planning (Sistema za planiranje resursa preduzeća)
FIRST - Forum of Incident Response and Security Teams (Forum timovi za odgovor na sigurnosne incidente)
GDPR - General Data Protection Regulation (Opšta uredba o zaštiti podataka)
HAIS-Q - Human Aspects of Information Security Questionnaire (Upitnik o ljudskim aspektima informacijske sigurnosti)
HSM - Hardware Security Module (Hardverski sigurnosni modul)
HTTP - HyperText Transfer Protocol (osnovni web protokol)

IAM - Identity and Access Management (Upravljanje identitetima i pristupom)
ICCP - Inter-Control Center Communications Protocol (Protokolza komunikaciju između kontrolnih centara)
ICS - Industrial Control System (Industrijski sistemi kontrole)
ICT - IKT - Informacijsko-komunikacijska tehnologija
IDS - Intrusion Detection System (Sistemi za detekciju upada)
IIB - Indeks informacione bezbjednosti
ILM - Identity Lifecycle Management (Upravljanje životnim ciklusom identiteta)
IMS - Identity Management Systems (Sistemi za upravljanje identitetima)
IP - Internet protocol (Internet protokol)
IP/MAC - Internet Protocol Address / Media Access Control Address
IPS - Intrusion Prevention System (Sistemi za preveniciju upada)
ISACA - Information Systems Audit and Control Association (Udruženje za reviziju i kontrolu informacionih sistema)
ISMS - Information Security Management System (Sistem upravljanja sigurnošću informacija)
ITU - International Telecommunication Union (Međunarodna unija za telekomunikacije)
LAN - Local Area Network (Lokalna mreža)
LDAP - Lightweight Directory Access Protocol (Lagani protokol za pristup direktorijumu)
MFA - Multi-Factor Authentication (Višefaktorska autentifikacija)
MITRE ATT&CK - MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE baza taktika, tehnika i znanja o napadima)
ML - Machine Learning (Mašinsko učenje)
MoU - Memorandum of Understanding (Memorandume o razumijevanju)
MSP - Mala i srednja preduzeća
MTD - Maximum Tolerable Downtime (Maksimalno dozvoljeno vrijeme prekida rada)
MTTD - Mean Time to Detect (Prosječno vrijeme detekcije)
MTTR - Mean Time to Respond (Prosječno vrijeme odgovora)
NAT - Network Address Translation (Prevođenje mrežnih adresa)
NIST - Nacionalni Institut za Standardizaciju i Tehnologiju Sjedinjenih Američkih Država
OSSIM – Open Source Security Information Management (Open-source sistem za upravljanje sigurnosnim informacijama)
OT – Operational Technology (Operativna tehnologija)
OTP – One-time password (Jednokratna šifra)
OWASP - Open Web Application Security Project (Otvoreni projekat za sigurnost web aplikacije)
PAM - Privileged Access Management (Upravljanje privilegovanim pristupom)
PBAC - Policy-Based Access Control (Kontrola pristupa zasnovana na sigurnosnim politikama)
PKI – Public Key Infrastructure (Infrastruktura javnog ključa)
RaaS - Ransomware-as-a-Service (Ransomware virus kao servis)
RADIUS/TACACS+ - Remote Authentication Dial-In User Service/ Terminal Access Controller Access-Control System Plus (Protokoli za autorizaciju/autentifikaciju)

RBAC - Role-Based Access Control (Kontrola pristupa zasnovana na ulogama)
RPO - Recovery Point Objective (Vremenski period potreban za oporavak podataka)
RSA – Rivest–Shamir–Adleman (Enkripcijski protokol)
RTO - Recovery Time Objective (Procjena vremena oporavka)
SaaS - Software as a Service (Software kao servis)
SAST - Static application security testing (Statičko sigurnosno testiranje aplikacije)
SCA - Software Composition Analysis (Analiza sastava softvera)
SCADA - Supervisory Control and Data Acquisition (Sistem za nadzor i prikupljanje podataka)
SIEM - Security Information and Event Management (Sistemi za nadzor događaja i njihovu korelaciju)
SLA - Service Level Agreement (Ugovor o nivou usluge)
SOAR - Security Orchestration, Automation and Response (Orkestracija, automatizacija i odgovor na sigurnosne incidente)
SoD - Separation of Duties (Razdvajanje odgovornosti)
SQL - Structured Query Language (Baza podataka)
SSL/TLS - Secure Sockets Layer / Transport Layer Security (Sigurnosni protokol koji šifrira komunikaciju između klijenta i servera.)
TCP/IP - Transmission Control Protocol / Internet Protocol (osnovni mrežni protokol)
TEE - trusted execution environments (zatvorena procesorska okruženja),
UAM - Unified Access Management (Unificirano upravljanje pristupom)
VLAN - Virtual Local Area Network (Virtualna lokalna mreža)
VolP - Voice over Internet Protocol („Telefoniranje“ preko Internet protokola)
VPN - Virtual Private Network
WAF - Web Application Firewall (Firewall za web aplikacije)
WEP - Wired Equivalent Privacy (Wireless sigurnosni protokol)
XSS - Cross-Site Scripting (Napad ubacivanjem zlonamjerne skripte u web stranicu)

1. Uvod

Analiza problema informacione sigurnosti u malim i srednjim preduzećima (u daljem tekstu: MSP) u Bosni i Hercegovini ne može se odvojiti od šireg konteksta globalnih trendova u sajber bezbjednosti. Posmatrajući dešavanja na međunarodnom nivou, primjećuje se da je informacija postala najvrjedniji resurs organizacija, čija je zaštita pod stalnim pritiskom tehnoloških promjena, umrežavanja sistema i sve većeg broja sofisticiranih napada (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Ovo nameće potrebu da upravljanje bezbjednosnim rizicima postaje integralni dio poslovne strategije, jer svaka slabost u sistemu može ugroziti kontinuitet poslovanja. Jedan od osnovnih izazova prepoznat je u različitim nivoima svijesti o riziku. Istraživanja pokazuju da dio organizacija procjenjuje opasnost od sajber napada kao stvarnu i visoku, ali ne reaguje adekvatnim mjerama zaštite, dok drugi segment uopšte ne prepoznaje posljedice potencijalnog ugrožavanja podataka (Almoaigel & Abuabid, 2023). Takva neujednačenost se javlja čak i među kompanijama koje posjeduju tehničke resurse, što sugeriše da pitanje edukacije zaposlenih o sajber bezbjednosti nosi jednaku važnost kao i implementacija tehničkih rješenja. Posebno je problematično kada menadžment ne uključuje zaposlene u razvoj sigurnosne strategije – gotovo trećina ispitanih firmi priznala je da takva participacija izostaje (Scholl & Schuktomow, 2021). Razlike u pristupu bezbjednosti djelimično se mogu objasniti organizacionom strukturom i definisanim odgovornostima unutar nacionalnog konteksta. Obrazac saradnje često nedostaje u zemljama gdje formalne CERT/CSIRT (Computer Emergency Response Team, u daljem tekstu: CERT/Computer Security Incident Response Team, u daljem tekstu: CSIRT) strukture nisu razvijene na državnom nivou, pa jedini oslonac predstavljaju lokalni ili sektor-specifični timovi. Unutar globalne prakse prepoznata je potreba za povezivanjem tehničkog aspekta zaštite sa jasno definisanim planom kontinuiteta rada ključnih infrastrukturnih sistema. Upravljanje kontinuitetom rada podatkovnih centara uključuje koordinaciju sa korporativnim partnerima, definisanje modela podrške, planiranje sukcesije ključnih funkcija i delegiranje ovlaštenja tokom kriznih situacija (el-Khameesy & Mohamed, 2013). Ovakav pristup zahtijeva proaktivno planiranje kako bi se ublažile posljedice incidenata koji bi mogli ugroziti rad organizacije. Istraživanja sajber prijetnji u vladinim informacionim sistemima dodatno naglašavaju složenost okruženja MSP-a kada su izloženi istovjetnim izazovima kao velike institucije – od masovnih kampanja phishing-a do napada koji traju duže vrijeme i iza kojih stoje države

(Judijanto, et al., 2023). Ovi scenariji otkrivaju ranjivosti koje male firme često zanemaruju misleći da nisu primarne mete takvih napada, što ih zapravo može učiniti pogodnijim za kompromitovanje zbog odsustva adekvatne zaštite. Rizik povezan sa ljudskim faktorom ostaje stalna tema istraživanja sajber bezbjednosti. Safitri i Darjat (Safitri & Darjat, 2024) ukazuju na to da kompetencije zaposlenih direktno utiču na otpornost sistema – treninzi prilagođeni nivou znanja pojedinaca omogućavaju smanjenje grešaka koje napadači mogu iskoristiti. Svijest o sopstvenoj ulozi u održavanju sigurnosti rijetko dolazi spontano, potrebno ju je graditi uz kontinuirano praćenje ponašanja korisnika. Veoma specifičan oblik ugrožavanja predstavlja socijalni inženjering, jer povezuje psihološke manipulacije sa tehničkim metodama zaobilaženja zaštitnih mehanizama. Kombinovanjem različitih metoda napada povećava se vjerovatnoća uspjeha socijalni inženjering kampanje, a dokazano je da bivši zaposleni predstavljaju ozbiljan faktor rizika, bilo kroz nenamjerne propuste ili svjesno sabotažno djelovanje (Scholl & Schuktomow, 2021). U takvim okolnostima integrisanje analize ponašanja zaposlenih sa postojećim tehničkim kontrolama može smanjiti broj uspješnih incidenata. Sa praktičnog stanovišta održavanja funkcionisanja mreža tokom i nakon incidenta od presudnog značaja su procedure odgovora na incidente koje svi zaposleni moraju poznavati unaprijed. Bez jasnih protokola reagovanja svaki pokušaj očuvanja integriteta sistema postaje improvizacija sa velikim šansama za neuspjeh. Napadi preko zajedničkih komunikacionih protokola dodatno komplikuju situaciju jer mogu koristiti legitimne kanale pristupa između servera i internih baza podataka kao most ka kompromitovanju unutrašnjih servisa (Kuipers & Fabro, 2006). Ovi elementi nagovještavaju koliko je važno periodično revidirati ravnotežu između željene funkcionalnosti poslovnog procesa i zahtjeva bezbjednosti sistema. Istraživanja (Shekh, 2024) pokazuju da mjerenje rizika od socijalni inženjering napada koristeći nove AI metodologije, mora biti dio stalnog procesa upravljanja rizikom kako bi se identifikovali posredni efekti ranjivosti koji se ne vide na prvi pogled. Korištenje modela zasnovanih na digitalnim dokazima daje mogućnost preciznijeg mapiranja uzročno-posljedičnih veza između aktivnosti unutar firme i ranjivosti kojima prijeti iskorištavanje kroz socijalni inženjering tehnike. Takav mozaik faktora ukazuje da problem informacione sigurnosti nije samo tehničko pitanje nego mnogo širi fenomen koji zahtijeva povezivanje tehnoloških alata, obrazovnog pristupa zaposlenima, jasno definisanog institucionalnog okvira i konstruktivne saradnje između javnog i privatnog sektora, bez čega MSP ostaju

izložena širokom spektru prijetnji koje mogu paralizovati njihove aktivnosti ili uzrokovati trajnu štetu po reputaciju kompanije.

1.1. Predmet istraživanja

Ovo istraživanje ima za cilj analizirati primjenu Defense in Depth strategije informacione sigurnosti u MSP. Kroz rad će se identifikovati ključni aspekti ove strategije i procijeniti njihova efikasnost u zaštiti sistema i podataka od sajber prijetnji. Također, istraživanje će se fokusirati na izazove i prepreke u implementaciji Defense in Depth strategije, kao i na važnost obuke i svijesti osoblja o sajber bezbjednosti. Kroz komparativnu analizu s drugim regionima, kandidat će predložiti smjernice za uspješno sprovođenje ove strategije u MPS.

U svom istraživanju, naglasit ćemo ulogu CERT-a u zaštiti od sajber prijetnji, identifikujući njihovu ključnu ulogu u otkrivanju i rješavanju sajber incidenata. CERT institucije nisu još formirane na državnom i entitetskom nivou (Republika Srpska trenutno radi na osnivanju), tako da ne postoje ni zakoni o sajber nasilju. Rad bi trebao biti preteča i pravac u kojem bi CERT sistemi u BiH trebali da krenu ali i osnova njihovog razvoja i kreiranja. Saradnja preduzeća sa lokalnim CERT-om trebala bi da predstavlja značajan faktor u uspješnoj implementaciji Defense in Depth strategije, omogućavajući što sigurnije informacione sisteme sa što manje sajber propusta.

Defense in Depth strategija informacione sigurnosti uključuje primjenu slojevite i sveobuhvatne zaštite podataka i informacionih sistema kako bi se smanjili rizici od sajber prijetnji i incidenata. Ovaj pristup ima za cilj da obezbijedi višestruke odbrambene mehanizme i spriječi neovlašteni pristup, otkrije i reaguje na potencijalne prijetnje, kao i da umanji štetu u slučaju napada.

Ključni elementi

Defense in Depth strategije obuhvataju:

• Perimetarska zaštita;

• Unutrašnja zaštita;

• Korisnička autentifikacija i autorizacija;

• Korisnička edukacija i svijest;

• Redundantnost i oporavak od katastrofe;

• Nadzor i nadgledanje;

• Bezbjednost aplikacija;

• Upravljanje identitetom.

Svaki sloj Defense in Depth strategije predstavlja dodatni nivo zaštite koji doprinosi cjelokupnoj sigurnosti informacionih sistema preduzeća. Implementacija ovog pristupa omogućava preduzećima da stvore snažan i integrisan okvir zaštite, minimizirajući rizike od sajber prijetnji i obezbjeđujući kontinuiranu zaštitu.

Kroz istraživanje koje će biti provedeno putem upitnika - ankete na IT osoblje preduzeća, dobit ćemo rezultate u kakvom stanju se trenutno nalazi svijest o sigurnosti sistema informacijsko-komunikacijske tehnologije (u daljem tekstu: ICT) i njihova podložnost prijetnjama.

1.2. Cilj istraživanja

Postavljanje jasnih ciljeva istraživanja u oblasti informacione sigurnosti MSP zahtijeva polaznu tačku koja uzima u obzir trenutni institucionalni i regulatorni okvir Bosne i Hercegovine. Izostanak zvaničnih CERT institucija na državnom ili entitetskom nivou, kao i nepostojanje zakonodavne regulative o sajber nasilju, usmjerava fokus ka analizi postojećih neformalnih inicijativa i mogućnosti njihove integracije u širu strategiju zaštite poslovnog sektora. Ovakav kontekst podrazumijeva da jedno od osnovnih istraživačkih težišta mora biti procjena kako poslovni subjekti mogu samostalno razviti mehanizme detekcije, reakcije i prevencije incidenata oslanjajući se na interne kapacitete ili saradnju sa lokalnim CSIRT timovima (Krulík, 2018). Uz institucionalne nedostatke, cilj je identifikovati trenutno stanje svijesti o sajber rizicima unutar MSP-a, ali ne samo u smislu tehničke opremljenosti, nego i spremnosti zaposlenih da postupaju u skladu sa politikama bezbjednosti. To obuhvata mapiranje postojećih obrazovnih programa i formalnih procedura za reagovanje na incidente radi ocjene njihove primjenjivosti i efikasnosti u praksi. Posebna pažnja posvetiće se situacijama u kojima je edukacija ograničena ili prepuštena individualnim inicijativama menadžmenta kompanije, što često dovodi do fragmentiranog pristupa bez jasne koordinacije (Safitri & Darjat, 2024). Ovaj rad teži da oblikuje metodologiju za evaluaciju nivoa usklađenosti MSP-a sa međunarodnim normama informaciono-bezbjednosnih politika. Takva procjena podrazumijeva upotrebu međunarodno priznatih standarda kao orijentira za domaće kompanije kako bi se vizualizirala razlika između željenog stanja sigurnosti sistema i realnog

nivoa otpornosti na sajber prijetnje (Judijanto, Rahardian, i ostali, 2023). Analiza će uključiti poređenje dobre prakse iz zemalja koje su razvile institucionalnu podršku kroz nacionalne CERT strukture sa modelom koji bi mogao biti implementiran u BiH uslijed postojećeg nedostatka formalne infrastrukture. Važan segment ciljeva jeste ispitivanje spremnosti MSP-a za incident menadžment. To podrazumijeva detaljno sagledavanje procesa prijavljivanja napada, koordinacije unutar organizacije tokom kriznih situacija, kao i sposobnost čuvanja digitalnih dokaza u skladu sa relevantnim zakonskim okvirom (el-Khameesy & Mohamed, 2013). U ovakvom okviru potrebno je vidjeti kako kompanije integrišu procedure odgovora na incidente sa redovnim operativnim aktivnostima, a da pritom ne naruše kontinuitet poslovanja. Istraživanje također treba da sistematski prikupi podatke o percepciji rizika kod MSP kroz prilagođene upitnike ili intervjue. Metodološki pristup zasniva se na formiranju pitanja koja pokrivaju tehničke aspekte zaštite mreža, upravljanje korisničkim nalozima, procese verifikacije identiteta korisnika, kao i postojeće politike restrikcije pristupa informacijama (Riebe i ostali, 2023). Na temelju odgovora moguće je izdvojiti najčešće slabosti u postojećem stanju bezbjednosti mreža MSP-a koje bi bile predmet daljeg rada i preporuka. Jedan od planskih ciljeva obuhvata razvoj okvira za formalizaciju saradnje između MSP-a i obrazovnih institucija ili stručnih centara koji se bave sajber bezbjednošću. Takva saradnja može uključivati obuku kadra za specifične tipove prijetnji kao što su phishing kampanje ili malver koji koristi legitimne komunikacione kanale unutar mreže kompanije (Kuipers & Fabro, 2006). Time bi se stvorila prilika za podizanje znanja u zajednicama gdje trenutno nema centralnog tijela zaduženog za koordinaciju zaštite informacionih sistema. Predviđa se da dio ciljeva bude usmjeren na provjeru kako se ljudski faktor tretira unutar organizacija, posebno kroz procese selekcije kadra i internog praćenja pristupa povjerljivim informacijama. Ovaj dio analize povezuje bezbjednosne protokole sa praksama kadrovskih službi kako bi se umanjila vjerovatnoća zloupotreba pozicija od strane zaposlenih (el-Khameesy & Mohamed, 2013). Pitanje pozadinskih provjera zaposlenih dobija dodatnu težinu kada nema centralnog nadzornog organa na nivou države koji može usmjeravati takve procedure. Na kraju, ali jednako važno, istraživanje ima cilj da uključi komparativni pregled strukture informaciono-bezbjednosnih mjera koje MSP-a primjenjuju u BiH sa onima primjenjenim u sektorima od javnog značaja poput energetike ili finansijskih institucija koje već imaju jasno definisane interne protokole zaštite (Krulík, 2018). Ovakvo poređenje omogućava realističnu projekciju

razvojnih koraka koje privatni sektor može implementirati uprkos manjku institucionalne podrške na nacionalnom nivou.

1.3. Metodološki okvir

Istraživanje Defense in Depth strategije informacione sigurnosti za MSP, razmotrit će različite metode kako bi dobio sveobuhvatne i pouzdane rezultate. Evo nekoliko metoda koje će se koristiti:

- Anketiranje: Možemo kreirati anketu i distribuirati je među relevantnim kompanijama kako bismo prikupili kvantitativne podatke o njihovim praksama informacione sigurnosti, implementaciji Defense in Depth strategije, produktivnosti i drugim varijablama. Anketiranje omogućava efikasno prikupljanje podataka od većeg broja učesnika;
- Intervjui: Sprovođenje strukturiranih intervjua sa predstavnicima kompanija ili ekspertima u oblasti informacione sigurnosti može pružiti dublje razumijevanje njihovih iskustava i perspektiva. Intervjui omogućavaju kvalitativno istraživanje i dubinsku analizu;
- Analiza dokumenata: Pravilno analiziranje relevantnih dokumenata, kao što su interni izvještaji o sigurnosti, planovi implementacije, izvještaji o sigurnosnim incidentima i slično dat će uvid u stvarne prakse i promjene tokom vremena;
- Studija slučaja: Istraživanje nekoliko odabranih kompanija ili organizacija može omogućiti dubinsku analizu primjene Defense in Depth strategije i njenih efekata na različite aspekte informacione sigurnosti;
- Statistička analiza: Za prikupljanje kvantitativnih podataka, koristit će se statističke metode kako bismo analizirali podatke i testirali hipoteze. To može uključivati T-testove, analizu varijanse, regresijsku analizu i slično, u zavisnosti od prirode podataka;
- Analiza slučajeva: Analizirat će se konkretne situacije i incidenti povezani sa informacionom sigurnošću u određenim kompanijama kako bi se razumjeli i načini na koje su primijenjene sigurnosne strategije uticale na te situacije;
- Anonimni upitnici i feedback od zaposlenih: mogu pružiti perspektivu „iznutra“ o primjeni sigurnosnih strategija i njihovim efektima.

Metodološki pristup ovom istraživanju osmišljen je da omogući kombinovanje kvantitativnih i kvalitativnih tehnika, sa ciljem postizanja što potpunijeg uvida u stanje informacione

sigurnosti kod MSP. Kvantitativna komponenta usmjerena je na prikupljanje struktuiranih podataka o informacionoj sigurnosti, dok kvalitativni dio obuhvata analizu iskustava ispitanika i interpretaciju značenja koje oni pridaju sopstvenim sigurnosnim praksama. Ovakva kombinacija metoda omogućava da se numerički indikator ranjivosti dopuni narativnim objašnjenjima koja otkrivaju logiku ponašanja i stavove unutar organizacija. Kvantitativni dio istraživanja temelji se na anketama sprovedenim među MSP-ovima, pri čemu su pitanja strukturirana tako da pokrivaju tehničke aspekte poput konfiguracije mrežnih sistema, primjene procedura autentifikacije korisnika, učestalosti ažuriranja softverskih komponenti i održavanja sigurnosnih kopija podataka. Ovdje se koristi skala koja omogućava rangiranje nivoa implementacije određenih bezbjednosnih kontrola, čime se mjeri stepen usklađenosti sa standardima informaciono-bezbjednosne politike (Shekh, 2024). Podaci iz ovog segmenta analize obrađuju se statističkim tehnikama koje omogućavaju identifikaciju korelacija između veličine preduzeća, sektora poslovanja i nivoa primijenjenih mjera zaštite. Kvalitativna komponenta uvodi perspektivu ispitanika kroz intervjue. Korišten je pristup koji dopušta fleksibilno mijenjanje toka intervjua u zavisnosti od odgovora sagovornika, kako bi se istražila njihova percepcija ranjivosti sistema, iskustva sa incidentima i stepen povjerenja u interne procedure reagovanja na napade. Takva strategija prikupljanja podataka posebno je korisna kada kvantitativni rezultati ukazuju na neobične obrasce koji zahtijevaju dublje razumijevanje. Za validaciju metodološkog okvira odabran je pristup ekspertne procjene, gdje su stručnjaci iz oblasti sajber bezbjednosti ocjenjivali upotrebljivost instrumenta istraživanja u kontekstu MSP-a. Evaluacija je uključivala provjeru jasnoće pitanja, relevantnosti tema koje pokriva anketa kao i sposobnosti instrumenata da generišu podatke pogodne za dalju komparativnu analizu. Ovakav korak uveden je kako bi se izbjeglo prikupljanje podataka koji ne bi mogli biti dosljedno interpretirani ili primijenjeni na plansko oblikovanje preporuka. Tok prikupljanja podataka oslanjao se na namjerno odabrane uzorke preduzeća različitih djelatnosti radi postizanja šireg spektra iskustava o sajber incidentima. U kvantitativnoj fazi koristili su se elektronski upitnici za efikasniju distribuciju i olakšano arhiviranje odgovora, dok su za kvalitativni segment intervjui vođeni uživo ili putem videopoziva zavisno od raspoloživosti sagovornika. Posebno su dokumentovani slučajevi gdje su incidenti doveli do prekida poslovnog procesa ili gubitka povjerljivih podataka, jer ovakvi primjeri pružaju materijal za procjenu efikasnosti postojećih mjera zaštite. Obrada kvantitativnih podataka uključuje deskriptivnu statistiku radi pregleda osnovnih trendova, kao i inferencijalne metode za

testiranje hipoteza o povezanosti određenih faktora sa učestalošću incidenata. Npr., ispitivana je hipoteza da li preduzeća koja imaju formalno definisane politike reagovanja bilježe manji broj uspješnih napada. U kvalitativnom dijelu analiza prati metod tematskog grupisanja sadržaja odgovora ispitanika kako bi se kategorizovali glavni izazovi koje oni navode, od nedostatka tehničke opreme do problema koordinacije između zaposlenih tokom incidenta. Integracija oba seta rezultata odvija se kroz proces triangulacije podataka. Ako kvantitativna analiza pokaže visoku učestalost određenog tipa napada, kvalitativni dio može objasniti razloge zašto taj napad prolazi neprimijećeno ili ostaje neriješen duže vrijeme. Na ovaj način dobija se složeniji model stanja bezbjednosti MSP-a koji kombinuje mjerenje objektivnih parametara sa subjektivnim opisima iskustava. Pored samog prikupljanja primarnih podataka, metodološki okvir predviđa korištenje sekundarnih izvora kako bi se uzorci iz domaćeg konteksta smjestili u širi međunarodni okvir poređenja. Upoređivanje sa sličnim istraživanjima koja obuhvataju male firme u drugim zemljama doprinosi boljem tumačenju rezultata jer pokazuje da li određena praksa predstavlja lokalnu specifičnost ili dio univerzalnog problema malih organizacionih struktura. Konačno, predviđena je iterativna priroda cjelokupnog metodološkog procesa, preliminarna analiza prvog talasa prikupljenih podataka koristi se za eventualno prilagođavanje instrumenata istraživanja prije nego što se nastavi na širu populaciju ispitanika. Time se postiže veća preciznost mjerenja i obezbjeđuje mogućnost detektovanja novih fenomena koji nisu bili planirani prvim dizajnom studije. Ovaj pristup omogućava dinamično upravljanje istraživačkim procesom tokom samog njegovog trajanja uz očuvanje kvaliteta i konzistentnosti dobijenih informacija.

1.4. Hipoteze

Polazeći od postavljenih ciljeva disertacije, kao i na osnovu sveobuhvatnih analiza postojećih istraživačkih pristupa i relevantnih naučnih literatura, formulisane su sljedeće hipoteze:

Opšta hipoteza:

H_0: Moguće je implementirati Defense in Depth strategiju informacione sigurnosti i u zavisnosti od veličine kompanije izabrati potrebni hardver i softver koji će unaprijediti i zaštititi informacioni sistem. Implementacijom strategije smanjuje se rizik informacione bezbjednosti. Strategija je i dodatna polazna tačka za uvođenje dodatnih kvaliteta kompaniji kroz certifikaciju za ISO standarde (npr. ISO 9000, 9001, 22301 i 27001).

Indikatori: Ovo su neki od indikatora za opštu hipotezu:

- Broj i vrsta implementiranih sigurnosnih slojeva (layer-a): Mjeri koliko različitih sigurnosnih slojeva ili slojeva sigurnosti (npr. firewall, antivirus, sistemi za detekciju/preveniciju upada (Intrusion Detection System, u daljem tekstu: IDS/Intrusion Prevention System, u daljem tekstu: IPS) je implementirano u informacionom sistemu u skladu sa Defense in Depth strategijom;
- Veličina budžeta za sigurnost informacionog sistema: Može se analizirati koliki dio budžeta kompanije se troši na sigurnosne aspekte, uključujući hardver i softver za informacionu sigurnost;
- Vrijeme za odgovor na sigurnosni incident: Ovaj indikator može mjeriti efikasnost i brzinu reagovanja na sigurnosne incidente. Brži odgovor može ukazivati na efikasniju implementaciju sigurnosnih strategija;
- Nivo obuke i certifikacija osoblja: Mjeri se nivo obuke i certifikacija osoblja koje radi na sigurnosti informacionog sistema, što može biti direktno povezano sa strategijom Defense in Depth i pripremom za ISO standarde;
- Broj i vrsta certifikata za ISO standarde: Mjeri se koliko i koje ISO standarde je kompanija certifikovala nakon implementacije Defense in Depth strategije;
- Broj i vrsta incidenata vezanih za sigurnost: Ovaj indikator može mjeriti broj i vrstu incidenata prije i nakon primjene strategije Defense in Depth. Manji broj sigurnosnih incidenata nakon primjene strategije može ukazivati na poboljšanu sigurnost.

Pomoćne hipoteze:

H1: Implementacijom strategije informacione tehnologije se povećava produktivnost kompanije.

Indikatori: Produktivnost se može mjeriti na različite načine, kao što su povećanje prihoda, smanjenje troškova, smanjenje vremena potrebnog za izvršavanje određenih poslovnih procesa.

H_2: Strategija Defense in Depth povećava sigurnost informacionog sistema, a samim tim i cjelokupne kompanije.

Indikatori: Sigurnost informacionog sistema možemo mjeriti kroz različite metrike, kao što su broj incidenata sa sigurnošću podataka, broj napadačkih pokušaja koji su odbijeni, procijenjeni troškovi povezani sa sigurnosnim incidentima.

H_3: Kroz implementaciju novih platformi uvodi se sklad i harmonizacija procesa kompanije koja na kraju dovodi do zadovoljavanja svjetskih standarda.

Indikatori: Sklad i harmonizacija procesa se mogu mjeriti putem internih procesnih metrika, kao što su vrijeme izvršavanja poslovnih procesa, stopa grešaka u procesima, itd. Isto tako, zadovoljavanje svjetskih standarda, kao što su ISO 9000, 9001, 22301 i 27001, može se mjeriti putem procjene da li su ovi standardi ispunjeni.

H_4: Implementacija Defense in Depth strategije smanjuje rizik od zloupotrebe podataka.

Indikatori: Za ovu hipotezu mogli bismo napraviti procjenu broja incidenata sa zloupotrebom podataka prije i poslije primjene strategije, kao i broja otkrivenih i riješenih zloupotreba.

H_5: Defense in Depth strategija pomaže u smanjenju finansijskih gubitaka uslijed sigurnosnih incidenata.

Indikatori: Prethodna hipoteza prezentuje iznos finansijskih gubitaka uslijed sigurnosnih incidenata prije i poslije primjene strategije, kao i procjenu troškova implementacije strategije.

H_6: Defense in Depth strategija poboljšava percepciju i povjerenje klijenata i partnera u kompaniji.

Indikatori: Uključivanje anketiranja klijenata i partnera kako bismo procijenili njihovu percepciju sigurnosti i povjerenja u kompaniju.

H_7: Implementacija Defense in Depth strategije zahtijeva veći broj tehničkih resursa (baziranih na novoj AI, ML i Docker infrastrukturi) u većim kompanijama.

Indikatori: Hipoteza bi trebala uključivati analizu resursa, kao što su broj zaposlenih zaduženih za sigurnost informacionog sistema i tehnički hardver koji se koristi.

Varijable su mjerljive karakteristike koje koristimo za analizu i testiranje navedenih hipoteza.

2. Teorijsko razmatranje o informacionoj sigurnosti

2.1. Pojam i značaj informacione sigurnosti

Informaciona sigurnost predstavlja jedan od najvećih faktora rizika u svakoj kompaniji. Kao takav izložen je svakodnevnim pokušajima napada i upada u informacioni sistem. Kroz ovo poglavlje rada ćemo se upoznati sa pojmovima u informacionoj sigurnosti koji su nam neophodni kako bismo shvatili tematiku ovog rada.

2.1.1. Definicija informacione sigurnosti

Informaciona sigurnost se u savremenoj literaturi tumači kao skup formalizovanih pravila, tehničkih mjera i organizacionih procedura čija je svrha zaštita podataka od neovlaštenog pristupa, izmjene, uništavanja ili ometanja tokom cijelog životnog ciklusa njihove obrade (Kamis et al., 2025) Definicije se razlikuju u naglasku koji autori stavljaju na pojedine aspekte, ali preovladava shvatanje da ona obuhvata integrisani pristup tehničkim i ljudskim faktorima radi očuvanja atributa povjerljivosti, integriteta i dostupnosti informacija (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Ovi atributi predstavljaju temelj bez kojeg sistemi ne mogu garantovati validnost svojih procesa niti pouzdanost rezultata koje generišu. Standardi poput ISO/IEC 27001 i 27003 formulišu minimalni set ovih atributa, dok prošireni metodološki modeli uključuju i dodatne dimenzije kao što su vjerodostojnost, odgovornost i pouzdanost resursa (Ionescu i ostali, 2018). Peña-Montes De Oca i Mondragón-Gutiérrez (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023) navode da je po definiciji Međunarodne telekomunikacione unije informaciona sigurnost zapravo funkcionalna kombinacija politika, smjernica, alata za upravljanje rizikom, akcija zaposlenih i tehničkih sistema koja štiti digitalne resurse organizacije i korisnike u sajber okruženju. Information Systems Audit and Control Association (u daljem tekstu: ISACA) proširuje ovu definiciju insistirajući da se radi o zaštiti digitalnih informacionih resursa kroz tretiranje prijetnji koje ugrožavaju podatke obrađene, skladištene ili prenesene putem međusobno povezanih informacionih sistema. Takvo tumačenje uvodi element aktivnog odgovora na dinamične oblike ugrožavanja, uključujući napade koji potiču iz spoljnog i unutrašnjeg okruženja organizacije. Primjenom ovakvog koncepta u praksi zahtijeva se jasno dokumentovanje sistema bezbjednosnih politika (Ionescu i ostali, 2018), jer tek kada su norme zapisane postaje moguće mjerenje stepena usklađenosti sa njima. Neformalna primjena mjera može pružiti privid zaštite, ali bez formalnog oslonca gubi se mogućnost sistemske kontrole nad procesima. Time definicija informacione sigurnosti

postaje operativni instrument: ona ne opisuje samo cilj, već implicitno usmjerava aktivnosti neophodne da bi se taj cilj ostvario. Safitri i Darjat (Safitri & Darjat, 2024) ističu vezu između kvaliteta ovih mjera i ukupnog nivoa zrelosti sajber bezbjednosti organizacije. Njihova analiza pokazuje da ulaganje u tehnologije poput kontrole pristupa, enkripcije i sistema detekcije upada direktno korelira sa višim nivoima otpornosti prema prijetnjama. Ovdje se definicija informacione sigurnosti nadovezuje na mjerljive performanse sistema, ona nije samo deklarativna već vodi ka konkretnim indikatorima efikasnosti odbrambenih kapaciteta. Uloga ljudskog faktora u definiciji informacione sigurnosti ne smije biti marginalizovana. Modeli poput HAIS-Q (Human Aspects of Information Security Questionnaire) naglašavaju da zaštita podataka zavisi od znanja, stavova i ponašanja korisnika sistema (Jevtić & Alhudaidi, 2023). To znači da se koncept ne može svesti isključivo na tehničku infrastrukturu; potrebno je uključiti obrazovne procese koji oblikuju kako zaposleni percipiraju rizik i kako postupaju u skladu sa propisanim procedurama. Organizacije koje definišu informacionu sigurnost samo kroz tehničke parametre propuštaju kritičan segment zaštite koji leži u pravilnoj upotrebi tih tehnologija. Postoji još jedan sloj u razumijevanju definicije, povezan sa fizičkom zaštitom digitalnih resursa. Možemo također reći da fizičko obezbjeđenje prostorija i opreme predstavlja prvu liniju odbrane koja kontroliše pristup servisnim provajderima, ograničava mogućnost neovlaštenog ulaska u server sobe ili manipulacije uređajima koji sadrže osjetljive informacije. Na taj način definicija se širi izvan granica virtuelnog prostora ka materijalnim uslovima bez kojih virtuelna zaštita ne može biti potpuna. El-Khameesy i Mohamed (el-Khameesy & Mohamed, 2013) dodaju da efektivna informacija sigurnosti uključuje raspodjelu odgovornosti unutar organizacije, jasno uspostavljene procese nabavke tehnologija potrebnih za detekciju upada i praćenje performansi sistema. U tom kontekstu važan je aspekt lične odgovornosti svakog učesnika procesa, od sistem administratora do krajnjeg korisnika, što proširuje definiciju sa institucionalnog nivoa na individualni. Sagledavanje ovih različitih perspektiva pokazuje da jedna univerzalna definicija pokušava obuhvatiti širok spektar komplementarnih oblasti: tehničku konfiguraciju sistema (npr. primjenu enkripcije), proceduralni okvir (politike pristupa informacijama), edukativnu komponentu (osposobljavanje kadra) i fizičke aspekte infrastrukturne zaštite (kontrola ulaza u data centre). Bez sinhronizovanog djelovanja ovih elemenata teško je govoriti o stvarnom ispunjenju ciljeva informacione sigurnosti. Na kraju treba istaći da savremeni normativni pristupi sve češće tretiraju informacionu sigurnost kao kontinuirani proces unapređenja zasnovan na ciklusu

Plan–Do–Check–Act (Ionescu i ostali, 2018). Primjena ovog modela implicira redefinisanje bezbjednosnih politika kad god evaluacija pokaže odstupanje od željenih standarda ili pojavu novih tipova prijetnji. Na taj način sama definicija dobija adaptivni karakter: ona više nije statični opis nego dinamičan okvir spreman na promjene koje nameće realno okruženje sajber prijetnji. Tako koncipirana informaciona sigurnost djeluje istovremeno kao teorijski konstrukt i praktični vodič rada unutar organizacija koje žele održati pouzdanost svojih podataka i procesa. Ona predstavlja složenu kombinaciju standardizovanih zahtjeva, prilagođenih strategija implementacije i stalne evaluacije učinka svih uključenih mehanizama zaštite, bilo digitalnih ili fizičkih.

2.1.1.1. Povjerljivost

Povjerljivost predstavlja osnovni stub informacione bezbjednosti, čiji je cilj da se zaštiti pristup podacima tako da im pristupaju isključivo ovlašteni subjekti. U okviru strategije Defense in Depth ovaj princip se implementira kroz kombinaciju tehničkih, proceduralnih i organizacionih kontrola koje zajedno čine višeslojnu odbranu od neautorizovanog pristupa. Osnovna premisa povjerljivosti jeste obezbjeđenje da se osjetljive informacije ne otkrivaju neovlaštenim korisnicima ni u jednom obliku – bilo tokom prijenosa, skladištenja ili obrade. Jedan od temeljnih slojeva zaštite povjerljivosti u Defense in Depth sistemima uključuje perimetarske mehanizme filtriranja saobraćaja, poput firewall i IDS/IPS, koji sprečavaju ulazak nelegitimnih konekcija. Međutim, oslanjanje samo na perimetar nije dovoljno, jer sofisticirani napadi često prolaze van glavne mrežne granice preko kompromitovanih uređaja ili aplikacija. Zbog toga se implementiraju dodatni slojevi unutar mreže, kao na primjer segmentacija zasnovana na principu najmanjih privilegija koja ograničava kretanje potencijalnog napadača i štiti interne resurse čak i ako jedan segment bude narušen (Kuipers & Fabro, 2006). Autentifikacija i autorizacija korisnika igraju ključnu ulogu u očuvanju povjerljivosti. Višefaktorska autentifikacija (u daljem tekstu: MFA) smanjuje vjerovatnoću kompromitovanja naloga putem krađe akreditiva, dok precizno definisane dozvole osiguravaju da pristup podacima ima samo osoblje kojem su ti podaci nužni za izvršavanje poslovnih funkcija (Neri, et al., 2022). Time se utiče na kontrolisanje unutrašnjih prijetnji – bilo slučajnih grešaka zaposlenih ili namjernog pokušaja zloupotrebe. Pored autentifikacije, enkripcija je osnovni alat zaštite povjerljivosti materijala. Enkripcija u tranzitu (npr. Transport Layer Security protokol, u daljem tekstu: TLS) sprečava „presretanje" komunikacije između entiteta, dok

enkripcija u mirovanju štiti podatke pohranjene na serverima ili lokalnim uređajima od pristupa bez odgovarajućih ključeva. Posebno mjesto zauzimaju tehnologije povjerljivog računarstva (confidential computing), gdje se podaci obrađuju unutar zatvorenih procesorskih okruženja poznatih kao trusted execution environments (u daljem tekstu: TEE). Ove arhitekture omogućavaju obradu šifrovanih podataka bez njihovog izlaganja host sistemu, čime se značajno smanjuje rizik od curenja informacija (Bartock, et al., 2021). Ljudski faktor ostaje važan segment slojevite odbrane povjerljivosti. Edukacija korisnika o osnovama zaštite informacija, rizicima phishing kampanja i socijalnog inženjeringa stvara dodatnu barijeru protiv napada koji direktno targetiraju povjerljive podatke. Okruženja MSP naročito zavise od ovog sloja, jer finansijska ograničenja mogu onemogućiti primjenu najnovijih tehničkih sistema detekcije – svijest zaposlenih o pravilnom rukovanju povjerljivim informacijama time dobija strateški značaj. Za očuvanje povjerljivosti važni su i procesi upravljanja identitetom (Identity Management), koji centralizuju kontrolu nad kreiranjem korisničkih naloga, dodjelom privilegija te opozivom pristupa kada to pravila nalažu. Kombinovanje ovakvog upravljanja sa redovnim auditom dozvola omogućava brzo otkrivanje odstupanja koja mogu ugroziti zaštitu podataka. Redundantan sistem provjera minimizira šansu da osjetljivi sadržaji budu dostupni preko zaboravljenih ili pogrešno konfigurisanih naloga. Kao dio sveobuhvatne strategije, održavanje povjerljivosti zahtijeva stalnu procjenu ranjivosti svih komponenti sistema koje rukuju podacima. Identifikovanje i dokumentovanje tih ranjivosti omogućava ciljano unapređenje određenih slojeva zaštite. Redovno ažuriranje softvera uklanja poznate sigurnosne nedostatke koje bi napadači mogli iskoristiti za dolazak do povjerljivih informacija. Backup sistemi, posebno oni sa vanmrežnim kopijama ili pohranom u sigurnim oblacima, predstavljaju dodatnu sigurnosnu odbranu. Iako njihova primarna svrha može biti kontinuitet poslovanja, oni doprinose i povjerljivosti ukoliko su kopije adekvatno zaštićene enkripcijom, a kontrole pristupa su striktne (Neri, et al., 2022). Napad koji uništi primarne sisteme bez uspjeha u kompromitovanju sigurnosnih kopija neće rezultirati trajnim gubitkom povjerljivih podataka. Primjena strategije Defense in Depth na području povjerljivosti mora uzeti u obzir razlike između spoljnjih prijetnji (npr. hakera koji pokušavaju presresti komunikaciju) i unutrašnjih izazova (npr. zaposlenog sa legitimnim pristupom koji neovlašteno otkriva podatke). Svaki sloj treba imati jasno definisanu namjenu sa aspekta ovog principa: perimetar blokira neželjeni spoljni saobraćaj, a unutrašnja segmentacija izoluje potencijalno kompromitovanje, tako onda i autentifikacija garantuje

validnost identiteta, a aplikativna kontrola prati ponašanje nad osjetljivim sadržajem radi otkrivanja anomalija. Ovakav višeslojni pristup nije statičan – svaki sloj povremeno prolazi testiranje otpornosti putem simuliranih incidenata. Penetracioni testovi usmjereni ka provjeri privilegovanih naloga ili enkripcionih kanala daju uvide u realnu sposobnost sistema da očuva privatnost informacija čak i tokom pokušaja kompromitovanja više segmenata odjednom. Rezultati takvih testova zatim informišu prilagođavanje kontrola kako bi se zatvorile eventualne praznine. Na teorijskom nivou može se reći da povjerljivost unutar informacione sigurnosti predstavlja koordinisano djelovanje niza nezavisnih, ali međusobno komplementarnih mehanizama sa ciljem stvaranja situacije gdje jedini način za kompromitaciju jeste simultano probijanje svih relevantnih slojeva – što statistički smanjuje vjerovatnoću uspješnog napada i ostavlja veći manevarski prostor timu zaduženom za incident odgovor (response) da reaguje prije nego što dođe do katastrofalnog gubitka podataka (Ejjami, 2024).

2.1.1.2. Integritet

Integritet unutar informacione sigurnosti odnosi se na očuvanje tačnosti, potpunosti i vjerodostojnosti podataka i sistema, tako da oni ostaju neizmjenjeni bez odgovarajuće autorizacije tokom cijelog životnog ciklusa obrade. Ovaj princip ima dva komplementarna aspekta, sprečavanje neovlaštenih ili nenamjernih izmjena informacija i struktura sistema, te pravovremeno otkrivanje i ispravljanje eventualnih odstupanja od originalnog stanja. U slojevitoj arhitekturi zaštite integritet se štiti kombinacijom tehničkih kontrola, administrativnih politika i organizacionih procedura koje zajedno stvaraju redundantne mehanizme provjere i korekcije. Tehnička implementacija ovog principa u Defense in Depth modelu počinje već na perimetarskom nivou. Filteri mrežnog saobraćaja, IDS/IPS i segmentacija mreže ne samo da ograničavaju pristup već prate i potencijalno maliciozne aktivnosti koje mogu ukazivati na pokušaj izmjene aplikativnog koda ili kritičnih konfiguracionih fajlova (Amro & Gkioulos, 2023). Uvedene liste dozvoljenih komandi ili protokola (whitelisting) daju dodatnu garanciju da komunikacioni kanali nose isključivo legitimne podatke u očekivanom formatu. Tako IDS/IPS platforme sa podrškom za dubinsku inspekciju paketa (Deep Packet Inspection, u daljem tekstu: DPI) mogu automatski identifikovati neusklađene obrasce prijenosa koji bi potencijalno mogli ugroziti integritet poslovnih informacija. Na aplikativnom sloju, integritet se održava primjenom metoda

validacije unosa i kontrole pristupa prema logici najmanjih privilegija (Neri, et al., 2022). Kontrole kao što su hash funkcije i digitalni potpisi omogućavaju provjeru da li su datoteke ili poruke izmijenjene nakon što su generisane. Tehnologije kriptografske zaštite platformskog firmware-a, definisane kroz okvire poput NIST SP 800-193 (Nacionalni Institut za Standardizaciju i Tehnologiju, u daljem tekstu: NIST), pružaju formalni model koji uključuje faze zaštite od korupcije koda (protection), detekcije promjena (detection) i oporavka na stanje integriteta (recovery), čime se obezbjeđuje povratak sistema u poznatu ispravnu verziju čak i nakon uspješnog eksploatisanja ranjivosti (Bartock, et al., 2021). Unutrašnja segmentacija mreže igra važnu ulogu u izolaciji potencijalnih incidenata koji mogu ugroziti integritet podataka (n.a., 2009). Na primjer, baza podataka koja se nalazi u zasebnoj sigurnosnoj zoni može biti dostupna samo posredstvom aplikacionog servera s precizno definisanim paketnim pravilima. Time se rizik od direktne manipulacije zapisima umanjuje čak i ako dođe do kompromitovanja jednog dijela infrastrukture. Ovakva granularna kontrola pristupa povezana je sa centralizovanim identitetskim servisima koji upravljaju autentifikacijom i autorizacijom korisnika uz vođenje evidencije svih pokušaja pristupa. Sistemi za nadzor događaja i njihovu korelaciju (Security Information and Event Management, u daljem tekstu: SIEM) koriste prikupljene log-ove kako bi detektovali anomalije koje mogu narušiti integritet (Amro & Gkioulos, 2023). To uključuje neočekivane izmjene konfiguracionih fajlova, modifikacije korisničkih privilegija izvan standardnih procedura ili neuobičajene obrasce upita prema bazi podataka. Automatizovana upozorenja omogućavaju bezbjednosnom timu brzu reakciju prije nego što male izmjene eskaliraju u ozbiljan incident. Uloga ljudskog faktora je također prisutna, obučeni administratori imaju sposobnost interpretacije ovih signala u širem kontekstu poslovanja kako bi razlikovali realne prijetnje od benignih anomalija (Ejjami, 2024). Redundantnost predstavlja još jedan stub očuvanja integriteta unutar Defense in Depth strategije. Kreiranje više nezavisnih kopija kritičnih informacija na različitim lokacijama ili medijima osigurava dostupnost autentične verzije podataka čak i ako primarna instanca bude kompromitovana (n.a., 2009). Važno je naglasiti da ove kopije moraju biti zaštićene jednakim ili višim nivoima kontrole pristupa kako same po sebi ne bi postale mete napadača koji žele mijenjati istorijske zapise i time ugroziti pouzdanost sistema. Protokole verifikacije integriteta potrebno je sprovesti kroz cijeli lanac obrade informacija, od inicijalnog unosa od strane korisnika, preko internih transformacija do skladištenja rezultata u bazama podataka. Primjena detekcionih mehanizama kao što su

checksums tokom prijenosa fajlova između servisa minimizira mogućnost pojave tihih korupcija sadržaja izazvanih hardverskim kvarovima ili softverskim greškama. Osim toga, politike dvojnog odobravanja izmjena kod ključnih konfiguracionih parametara uvode proceduralni sloj provjere gdje dvije nezavisne osobe moraju potvrditi ispravnost promjene prije njenog stupanja na snagu (Neri, et al., 2022). Obuka korisnika ima indirektnu, ali važnu ulogu za očuvanje integriteta jer smanjuje vjerovatnoću namjernog ili slučajnog unošenja štetnih modifikacija. Na primjer, razumijevanje rizika povezano sa preuzimanjem datoteka iz nepoznatih izvora može spriječiti instalaciju malvera koji ciljano mijenja podatke radi izazivanja grešaka ili manipulacije evidencijom. Programi edukacije pomažu zaposlenima da prepoznaju sumnjive aktivnosti koje bi mogle dovesti do kompromitovanja sistema, a jasno definisana odgovornost osoblja jača disciplinu pridržavanja pravila. Integritet mora biti razmatran zajedno sa incident response procedurama koje preciziraju kako vraćati sistemsko stanje nakon narušavanja pouzdanosti informacija.

Planovi oporavka uključuju ne samo obnavljanje iz sigurnosnih kopija već i identifikaciju uzroka promjene, zatvaranje vektora napada te sprovođenje forenzičkih analiza radi procjene štete. Takav holistički pristup minimizira rizik ponovnog narušavanja te daje određenu otpornost sistema protiv ponavljanih scenarija ugrožavanja integriteta. Sve navedeno pokazuje da očuvanje integriteta unutar slojevite strategije nije izolovan zadatak jednog tehničkog sredstva već rezultat koordinisanog rada niza komponenti, od perimetarske filtracije mrežnog saobraćaja preko aplikativne validacije do kontinuiranog monitoringa događaja (Bartock, et al., 2021). Svaki sloj može uhvatiti određeni tip pokušaja kompromitovanja i njihova zajednička funkcija je stvoriti stanje u kojem je statistički veoma teško sprovesti trajne, nedetektovane izmjene kritičnih informacija ili sistemskih komponenti.

2.1.1.3. Dostupnost

Dostupnost kao jedan od osnovnih principa informacione sigurnosti obuhvata osiguravanje da ovlašteni korisnici i sistemi mogu pristupiti potrebnim podacima i uslugama u vremenu kada im je to potrebno, bez neplaniranih prekida ili degradacije performansi. Unutar strategije slojevite zaštite, ovaj princip se implementira kroz kombinaciju tehničkih i organizacionih mjera koje zajedno sprečavaju ili ublažavaju efekte incidenata koji bi mogli dovesti do zastoja (n.a., 2009). Na osnovnom nivou, dostupnost podrazumijeva da svaki sloj sistema – od fizičke infrastrukture, preko mrežnih komponenti i serverskih servisa, do aplikacija – bude

projektovan sa tolerancijom na greške i kapacitetom za oporavak u slučaju narušavanja standardnog rada. Perimetarska zaštita ima indirektnu ulogu u očuvanju dostupnosti. Filtriranje saobraćaja putem firewall-a ili IDS/IPS smanjuje rizik od napada vrste Denial of Service (u daljem tekstu: DoS) koji ciljaju na iscrpljivanje resursa (Kuipers & Fabro, 2006). Ako se ovakvi napadi probiju, unutrašnja segmentacija mreže može ih ograničiti samo na jedan dio infrastrukture, omogućavajući nastavak rada drugih segmenata bez potpunog prekida. Segmentacija zajedno sa pravilima kontrole pristupa (Access Control Lists, u daljem tekstu: ACL) obezbjeđuje da, čak i pri kompromitaciji jednog podsistema, kritične funkcije ostanu operativne. Redundantnost je ključan sloj za dostupnost. Projektovanje sistema sa redundancijom kapaciteta – bilo kroz duplikate serverskih instanci, mrežnih uređaja ili skladišta podataka – omogućava automatsko preusmjeravanje prometa na funkcionalne komponente u slučaju otkaza primarnog dijela. Ovi mehanizmi „failover“ konfiguracije moraju biti sinhronizovani sa centralizovanim nadzornim sistemima radi momentalnog prepoznavanja problema i pokretanja procedura oporavka (Amro i Gkioulos, 2023). Redundantne veze između centara podataka smanjuju vrijeme nedostupnosti tokom havarije povezane s mrežnom infrastrukturom. Planovi oporavka od katastrofe su dodatni sloj unutar Defense in Depth koji direktno utiče na dostupnost. Definisane procedure za backup i recovery omogućavaju vraćanje usluga nakon incidenta unutar predviđenog vremenskog okvira (Recovery Time Objective, u daljem tekstu: RTO). Efikasna politika izrade sigurnosnih kopija uključuje geografski razdvojene lokacije ili upotrebu cloud servisa sa snažnim sigurnosnim kontrolama. Važno je da svi backup sistemi podržavaju ne samo enkripciju radi povjerljivosti već i verifikaciju verzija kako bi se obezbjedio integritet obnovljenih podataka (immutable backup). Autentifikacija i autorizacija korisnika imaju ulogu za održavanje dostupnosti jer sprečavaju neovlaštene aktivnosti koje mogu prouzrokovati prekid rada. Ograničavanje privilegija umanjuje mogućnost da korisnik slučajno ili namjerno izvrši operacije koje blokiraju usluge ili modifikuju kritične komponente aplikacija (Neri, et al., 2022). MFA dodaje sigurnosni sloj protiv preuzimanja naloga koji bi mogao inicirati akcije ugrožavanja dostupnosti. Nadzor sistema i stalno praćenje performansi predstavljaju proaktivan sloj zaštite dostupnosti. Instrumenti poput SIEM platformi analiziraju log-ove događaja tražeći indikatore potencijalnog pada performansi ili pokušaja sabotaže (Amro i Gkioulos, 2023). Uočene anomalije aktiviraju automatizovane alarme kako bi timovi reagovali prije nego što problem eskalira do potpunog prekida rada. Nadzorni mehanizmi mogu

uključivati specifične threshold parametre, kao što su procenat korištenja CPU-a (Central Processing Unit) ili kašnjenje u mreži, koji signaliziraju potrebu za intervencijom. Bezbjednost aplikacija doprinosi dostupnosti tako što sprečava exploit ranjivosti koje bi napadači mogli iskoristiti za upade sa većim posljedicama (Rahman, et al., 2019). Implementacijom testiranja koda tokom cijelog životnog ciklusa razvoja softvera smanjuje se vjerovatnoća postojanja grešaka koje mogu uzrokovati pad usluga. Ažuriranje aplikacija uklanja poznate ranjivosti koje inače mogu biti iskorištene za uskraćivanje pristupa legitimnim korisnicima. Ljudski faktor ovdje ima dvojak uticaj, s jedne strane obučeni operatori mogu brzo reagovati na incidente čime se minimizira vrijeme nedostupnosti; s druge strane, needukovani korisnici mogu nesvjesno izazvati prekid usluga svojim postupcima (Bada i Nurse, 2019). Edukacija o rizicima povezanima s resursnom potrošnjom (npr. generisanje velikih količina nepotrebnih zahtjeva ka serveru) doprinosi samokontroli korisnika, a time i očuvanju funkcionalnog statusa sistema. Upravljanje identitetom dodatno pomaže održavanju stabilnog rada tako što jasno definiše ko može upravljati kojim resursima unutar infrastrukture. Centralizovana kontrola naloga (Active Directory, Open LDAP, Entra ID, Oauth2) omogućava brzo opozivanje pristupa u slučaju detektovanih zloupotreba koje ugrožavaju kontinuitet rada. Tehnička infrastruktura mora biti otporna na tzv. cliff edge efekat, situaciju gdje mali poremećaji naglo prelaze prag tolerancije sistema i izazivaju potpuni kolaps rada. Stabilan dizajn sa širokim operativnim marginama sprečava da kratkotrajna odstupanja prouzrokuju dugotrajne posljedice po dostupnost usluga. Sve navedene komponente ukazuju da očuvanje dostupnosti unutar slojevite strategije nije rezultat samo jednog izolovanog sredstva, već sklop više međuzavisnih mehanizama tehničke i organizacione prirode. Svaki sloj adresira specifičan aspekt rizika po kontinuitet rada, jer njihova istovremena primjena stvara otpornost koja značajno smanjuje vjerovatnoću dugotrajne nedostupnosti sistema čak i u uslovima koordiniranih sajber napada ili neočekivanih tehničkih kvarova.

2.1.2. Razlika između informacione i sajber sigurnosti

Razlika između informacione i sajber sigurnosti zahtijeva pažljivo razmatranje oba pojma u njihovim tehničkim, organizacionim i konceptualnim dimenzijama. Informaciona sigurnost predstavlja širi okvir koji obuhvata zaštitu svih oblika informacija, bez obzira na medijum u kojem se nalaze – bilo da je riječ o elektronskim bazama podataka, papirnoj dokumentaciji ili usmenoj komunikaciji unutar organizacije (Shekh, 2024). Njena osnovna svrha je očuvanje

ključnih svojstava informacija: povjerljivosti, integriteta i dostupnosti, kroz kontinuirano upravljanje rizikom i primjenu politika koje jasno definišu kako se informacije prikupljaju, obrađuju, skladište i dijele. Sajber sigurnost je uži pojam, usmjeren isključivo na zaštitu digitalnih resursa i infrastrukture povezanih kroz računarske mreže (Tetteh, 2024). Ona se odnosi na očuvanje bezbjednosti sistema koji funkcionišu u sajber prostoru, uključujući serversku opremu, mrežne servise, aplikativni softver i korisničke uređaje. U ovom kontekstu fokus je prvenstveno na prevenciji, detekciji i odgovoru na prijetnje koje koriste digitalne kanale pristupa – od malicioznog softvera do sofisticiranih napada usmjerenih na ranjivosti protokola komunikacije (Kuipers & Fabro, 2006). Iako oba termina dijele zajednički cilj – zaštitu vrijednih podataka i resursa – njihov obim primjene pokazuje jasne razlike. Praktičan primjer ove distinkcije mogao bi biti incident krađe povjerljive informacije iz poslovne arhive kompanije. Ako je kopija dokumenta odštampana i fizički uklonjena iz zatvorenog ormara, radi se o narušavanju informacione sigurnosti koje nema nužno digitalnu dimenziju. Suprotno tome, ako je isti dokument kompromitovan upotrebom zlonamjernog softvera instaliranog putem phishing poruke poslane zaposlenom, tada govorimo o incidentu sajber sigurnosti. Shodno tome, informaciona sigurnost obuhvata šire okruženje gdje podaci mogu biti ugroženi čak i bez elektronskog posrednika (Shekh, 2024), dok sajber sigurnost tretira isključivo prijetnje koje nastaju ili se realizuju u digitalnim sistemima. Pitanje granica između ovih oblasti postaje važno kada se razvijaju politike zaštite unutar organizacije. Organizacije koje se fokusiraju isključivo na sajber sigurnost mogu zanemariti rizike povezane sa fizičkim pristupom informacijama. Na primjer, sistem autentifikacije korisnika može biti tehnički napredan i efikasan, ali ako ne postoji kontrola fizičkog pristupa server sobi ili ako zaposlenima nije zabranjeno iznošenje hard diskova iz objekta, cjelokupna digitalna zaštita gubi značajan dio svoje funkcionalnosti. S druge strane, organizacije koje imaju razvijen sistem informacione sigurnosti sa strogim pravilima rukovanja dokumentima moraju imati svijest da savremeni napadi često kombinuju fizičke i digitalne metode zaobilaženja ovih pravila. U praktičnoj implementaciji razlike se ogledaju i u alatima koji se koriste za ostvarenje ciljeva obje discipline. Informaciona sigurnost može podrazumijevati procedure klasifikacije dokumenata prema nivou povjerljivosti, pravne instrumente kao što su ugovori o povjerljivosti sa zaposlenima ili partnerima, te treninge o zaštiti podataka namijenjene različitim kategorijama osoblja (el-Khameesy & Mohamed, 2013). Sajber sigurnost će koristiti tehnologije poput firewalla, IDS/IPS, enkripciju prijenosa podataka preko mreže i višefaktorsku autentifikaciju

korisnika (Tetteh, 2024). Iako ti pristupi djeluju komplementarno, svaki ima svoje specifične proceduralne korake koji ne moraju biti primjenjivi van okvira kome pripada. Povjerljivost (confidentiality) kao zajednički atribut pokazuje zanimljive razlike između ova dva koncepta kada se posmatra u praksi. U informacionoj sigurnosti ona uključuje ograničavanje pristupa kako elektronskim tako i fizičkim zapisima podataka. U sajber sigurnosti povjerljivost stoji kao zaštita elektronskog prenosa i skladišta podataka od digitalnog kompromitovanja kroz mehanizme poput SSL /TLS protokola ili end-to-end enkripcije aplikacija za komunikaciju. Kod integriteta (integrity) situacija je slična – kod informacione sigurnosti integritet znači sprečavanje neovlaštenih promjena nad bilo kojim oblikom informacije; kod sajber sigurnosti fokus je na validaciji sadržaja digitalnih zapisa kroz checksum postupke ili blockchain zasnovane verifikacione metode. Još jedan indikativan aspekt razlike leži u ljudskom faktoru. Dok su edukativni programi unutar informacione sigurnosti usmjereni ka opštem razumijevanju rizika rukovanja informacijama bilo kojeg tipa (el-Khameesy & Mohamed, 2013), programi sajber bezbjednosti često naglašavaju specifične vrste digitalnih prijetnji poput phishing kampanja ili ransomware napada. Time dolazi do divergencije metoda evaluacije uspješnosti ovih programa – kod informacione sigurnosti mjeri se cjelokupna usklađenost organizacije sa politikama zaštite svih oblika podataka; kod sajber sigurnosti mjeri se otpornost infrastrukture na definisane scenarije digitalnog napada. U nekim teorijskim modelima sajber sigurnost navodi se kao potkategorija informacione sigurnosti, što jasno odražava logiku odnosa: svaki incident u sajber domenu predstavlja slučaj narušavanja informacione sigurnosti digitalnog segmenta poslovanja. Međutim, praktična implikacija ovog odnosa jeste da menadžeri zaduženi za informacionu bezbjednost moraju imati kompetencije koje prelaze granice jednog domena – njihova nadležnost obuhvata kako virtuelnu infrastrukturu tako i kontrolu fizičkih procedura čuvanja podataka. Analiza iz perspektive MSP-a pokazuje da pogrešno poistovjećivanje ova dva pojma može dovesti do ozbiljnih propusta u sistemu zaštite. Na primjer, kompanija može investirati značajne resurse u softversku odbranu od mrežnih napada ali bez osnovnih politika za arhiviranje papirnog materijala koji sadrži osjetljive podatke o klijentima. Takva praksa ostavlja nenamjerno otvoren vektor napada koji bi mogao biti iskorišten mimo ikakvih digitalnih interakcija. Kada se konceptualno raščlane oba pojma postaje jasnije da odnos između njih ima karakter hijerarhije: informaciona sigurnost kao okvirni pojam daje ciljnu strukturu strategijama bezbjednosti organizacije; sajber sigurnost predstavlja tehničku specijalizaciju unutar tog

okvira fokusiranu isključivo na digitalni segment poslovanja. Ova struktura pomaže ne samo teorijskoj preciznosti nego omogućava praktično profilisanje odgovornosti unutar organizacije – time se sprečava preklapanje zadataka između timova zaduženih za različite aspekte zaštite podataka i gradi sinergija između fizičke i virtuelne odbrane resursa.

2.2. Globalni okvir i trendovi

U savremenom digitalnom okruženju, informaciona sigurnost postala je globalno pitanje koje prevazilazi nacionalne granice, industrijske sektore i pojedinačne organizacije. Sve veća međuzavisnost informacionih sistema, rast obima podataka i ubrzana digitalna transformacija doveli su do potrebe za uspostavljanjem jedinstvenih, međunarodno priznatih okvira koji omogućavaju sistematsko upravljanje rizicima informacione sigurnosti. U tom kontekstu, međunarodni standardi predstavljaju temelj za harmonizaciju sigurnosnih praksi, osiguravanje interoperabilnosti sistema i izgradnju povjerenja između organizacija, korisnika i regulatornih tijela na globalnom nivou.

Globalni okvir informacione sigurnosti oblikovan je kroz djelovanje međunarodnih organizacija za standardizaciju, kao što su ISO/IEC, NIST i ITU (International Telecommunication Union, u daljem tekstu: ITU), koje razvijaju smjernice i normative s ciljem uspostavljanja minimalnih sigurnosnih zahtjeva i najboljih praksi. Ovi standardi omogućavaju organizacijama da na strukturiran način identifikuju prijetnje, procijene rizike i implementiraju odgovarajuće tehničke, organizacione i proceduralne mjere zaštite, nezavisno od njihove veličine ili djelatnosti. Poseban značaj imaju standardi koji se fokusiraju na upravljanje informacionom sigurnošću, zaštitu privatnosti i kontinuitet poslovanja, čime se osigurava otpornost informacionih sistema u uslovima sve kompleksnijih i sofisticiranih napada.

Savremeni trendovi u oblasti informacione sigurnosti ukazuju na pomjeranje fokusa sa isključivo tehničkih kontrola ka holističkom pristupu koji integriše upravljanje rizicima, usklađenost sa regulatornim zahtjevima i kontinuirano poboljšanje sigurnosnih procesa. Dodatno, rast primjene cloud tehnologija, mobilnih platformi i vještačke inteligencije nameće potrebu za stalnom evolucijom međunarodnih standarda, kako bi oni ostali relevantni i primjenjivi u dinamičnom globalnom okruženju. U tom smislu, međunarodni standardi informacione sigurnosti ne predstavljaju statičan skup pravila, već adaptivni okvir koji prati tehnološke i organizacione promjene u savremenim informacionim sistemima.

2.2.1. Međunarodni standardi i norme

Međunarodni standardi i norme u oblasti informacione sigurnosti predstavljaju struktuiran skup pravila, procedura i preporuka osmišljenih da harmonizuju prakse zaštite podataka u različitim zemljama i industrijama. Oni pružaju okvir u kojem organizacije mogu mjerenjem usklađenosti procijeniti svoje kapacitete za upravljanje rizicima, dok istovremeno olakšavaju međusobno povjerenje u razmjeni informacija. Važnost ovih standarda u kontekstu MSP potiče iz činjenice da MSP često nemaju interne resurse za razvoj kompleksnih politika, pa oslanjanje na međunarodne norme postaje temeljni korak ka podizanju nivoa bezbjednosti. ISO/IEC 27001:2022, kao najpoznatiji standard za sisteme upravljanja informacionom bezbjednošću, predviđa formalizovan proces definisanja politika zaštite podataka, sprovođenja analize rizika i implementacije kontrola koje obuhvataju tehničke, proceduralne i organizacione aspekte. Ovaj standard je posebno relevantan za MSP-ove budući da daje jasnu strukturu koraka koja se može skalirati prema veličini organizacije. Kada se opisuju kontrole pristupa – od ograničavanja privilegija korisnika do verificiranja identiteta – standard naglašava minimalizaciju pravila pristupa radi smanjenja mogućnosti zloupotrebe (Neri i ostali, 2022). Time se povezuje sa praksama koje su primjenjive u širem okviru informacione sigurnosti, a ne samo na digitalne sisteme. ISO/IEC 27032 je fokusiran na sigurnost u sajber prostoru, posebno adresirajući zaštitu tokom razmjene informacija preko mreže i koordinaciju između subjekata kako bi se suzbio sajber kriminal (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Ovaj dokument dopunjuje klasične modele zaštite dodavanjem okvira za međusobnu saradnju između organizacija i nadležnih tijela. To ima poseban značaj u sredinama gdje nedostaju centralizovane institucije poput nacionalnog CERT-a – standard tu nudi osnovu za formiranje neformalnih partnerstava radi brže reakcije na napade. Komplementarni dokumenti, poput smjernica koje redovno objavljuje European Union Agency for Cybersecurity (u daljem tekstu: ENISA), obezbjeđuju ažurne preporuke usklađene sa trenutnim trendovima prijetnji (Neri i ostali, 2022). Te smjernice obuhvataju procjene rizika zasnovane na sektorskim prioritetima i nude praktična rješenja koja ne zahtijevaju kompleksnu infrastrukturu, što ih čini pogodnima za MSP. Korištenje ENISA publikacija može biti način da mala preduzeća nadomjeste manjak domaćih regulatornih dokumenata. Standardi poput ISO/IEC 13335 serije (kasnije prevedene u ISO/IEC 27005) usmjereni su na upravljanje bezbjednosnim rizicima kroz globalno priznate modele. Ova serija obuhvata pojmovne modele ICT bezbjednosti (27005-1), metodologiju procjene rizika (27005-2) i

tehnike upravljanja IT bezbjednošću (27005-3). MSP koja primjenjuju ovakve dokumente mogu sistematično graditi procedure koje nisu vezane samo za trenutne tehnologije već integrisano gledaju cjelokupni životni ciklus informacija. NIST Cybersecurity Framework (u daljem tekstu: CSF) dodaje dimenziju kroz definisanje pet osnovnih funkcija: identifikovati, zaštititi, detektovati, reagovati i oporaviti se (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Ove funkcije daju holistički koncept pristupa informacijama prilagodljiv infrastrukturnim karakteristikama MSP-a. Struktura NIST CSF-a pogoduje organizacijama koje žele jednostavniji start – moguće je početi sa osnovnim mjerama identifikacije kritičnih resursa prije nego što se uvedu složeniji mehanizmi zaštite. Critical Security Controls predstavljaju još jedan referentni okvir praktičnih koraka za podizanje nivoa sajber sigurnosti. Iako su često viđeni kao tehnički orijentisani dokumenti sa prioritetnim kontrolama kao što su inventar hardvera/softvera ili implementacija sigurnosnih konfiguracija sistema, oni imaju potpunu kompatibilnost sa ciljevima šire informacione sigurnosti. MSP koja ih primjenjuju postižu vidljive pomake ka standardizaciji stavova o ključnim tehničkim mjerama. Control Objectives for Information and Related Technologies (u daljem tekstu: COBIT) framework dodaje poslovnu perspektivu integracije IT ciljeva sa korporativnom strategijom (Neri i ostali, 2022). Za MSP koja moraju bilježiti vezu između investicija u zaštitu i poslovnog učinka COBIT nudi jasno mapiranje procesa upravljanja tehnologijama sa očekivanim ishodima – bilo finansijskim bilo operativnim. U praksi, integracija različitih međunarodnih normi često zahtijeva selektivnu adaptaciju. Na primjer, kombinovanje ISO/IEC 27001 procedura sa NIST CSF funkcijama može rezultirati balansom između formalnog sistema upravljanja bezbjednošću i operativnog odgovora na incidente. MSP pritom treba da uzmu u obzir sopstvenu veličinu i sektor djelatnosti kako bi odredili realan obim primjene pojedinih zahtjeva. Važno je pomenuti da međunarodni standardi ne garantuju automatsku otpornost sistema – njihova vrijednost leži u pružanju provjerenih okvira koji olakšavaju konzistentnu provjeru stanja bezbjednosti. Implementacija mora biti podržana internom kulturom koja cijeni poštovanje procedura i transparentno rukovanje incidentima (Ejjami, 2024). Bez ovog segmenta čak i potpuna usklađenost sa standardima može proizvesti samo formalni efekat, dok stvarna zaštita ostaje ograničena. Ovaj komparativni pregled pokazuje da međunarodne norme funkcionišu kao univerzalni jezik među organizacijama različitih profila – od velikih globalnih korporacija do lokalnih MSP. Korištenjem takvih okvira stvara se osnova za saradnju preko granica industrija ili država jer postoji zajedničko razumijevanje očekivanog nivoa

zaštite podataka (Judijanto, Hindarto, i ostali, 2023). Za kompanije iz regiona koje nemaju razvijen institucionalni sistem sajber odbrane primjena ovih normi predstavlja mogućnost sinhronizacije svojih procesa sa onima kod partnera iz zemalja sa višim regulatornim kapacitetima. Na kraju treba istaći da pravilna interpretacija međunarodnih normi zahtijeva stručan kadar sposoban da ih prilagodi lokalnim okolnostima bez gubitka osnovnih principa dokumenta. Time se gradi most između svjetskih preporuka i konkretne operativne realnosti MSP-a koji posluju unutar specifičnih pravnih i ekonomskih okvira.

2.2.2. Regulatorni zahtjevi i zakonski okvir

Regulatorni zahtjevi i zakonski okvir za informacionu bezbjednost predstavljaju formalizovan skup normi, pravila i procedura kojima se uređuje način zaštite podataka, reagovanja na incidente i usklađivanja sa međunarodnim obavezama u oblasti sajber bezbjednosti. U širem kontekstu globalnog okvira, kreatori politika teže da harmonizuju zakonske odredbe kako bi se obezbijedilo međusobno povjerenje između različitih ekonomskih i institucionalnih subjekata, dok se na lokalnom nivou posebna pažnja poklanja transponovanju ovih normi u nacionalno zakonodavstvo (Kashyap & Chaudhary, 2023). Analiza regulatornog okvira unutar MSP pokazuje da zahtjevi nisu samo tehničke prirode – oni uključuju pravnu definiciju odgovornosti, obavezu prijavljivanja incidenata i poštovanje propisanih standarda rukovanja osjetljivim informacijama. Zakonska regulativa u oblasti sajber bezbjednosti mora uzeti u obzir da MSP raspolažu ograničenim finansijskim i kadrovskim resursima za implementaciju kompleksnih mjera zaštite. Iako zakoni mogu postaviti visok prag zahtjeva, njihova primjena često zavisi od interpretacije regulatornih tijela i spremnosti organizacija da prilagode sopstvene procedure tim normama. Vlade pojedinih zemalja nastoje postići ravnotežu između promovisanja inovacija kroz digitalnu transformaciju i nametanja strogih sigurnosnih mjera koja treba smanjiti rizik od kompromitovanja podataka. Međutim, pretjerano komplikovan regulatorni okvir može otuđiti manja preduzeća ili ih primorati na minimalnu usklađenost bez stvarnog unapređenja bezbjednosnih kapaciteta. Jedan od izazova u ovakvim sistemima jeste neujednačena distribucija resursa za podršku MSP-ovima. Dok pojedine kompanije dobijaju državne podsticaje ili subvencije za unapređenje sajber bezbjednosti, druge ostaju van tokova pomoći zbog nedostatka informisanosti ili nepristupačnih procedura prijave. Posljedica toga je produbljivanje digitalnog jaza – manja preduzeća koja nemaju pristup adekvatnoj obuci ili tehnologijama teže ispunjavaju regulatorne kriterije, a time ostaju

ranjivija na sofisticirane napade. Primjeri iz prakse pokazuju i da sektorski specifični zakonski okviri mogu olakšati integraciju propisa sa realnim poslovnim potrebama. Kreiranje sektorskog regulatornog modela omogućava interpretaciju nacionalne politike kroz prizmu konkretnih operativnih izazova određenih industrija (Ejjami, 2024). Takav pristup uključuje organizaciju radionica, edukativnih sesija i konsultacija kako bi se poslovna zajednica upoznala sa pravnim zahtjevima i dobila jasne smjernice za usklađivanje interne dokumentacije sa zakonom. U nekim jurisdikcijama postoji dobro razvijen okvir zaštite podataka koji kombinuje tehničke preporuke sa pravno obavezujućim mjerama. Na primjer, kombinovanje zakona o zaštiti ličnih podataka sa propisima o elektronskoj trgovini stvara sinergiju koja istovremeno tretira privatnost korisnika i sigurnost transakcija (Kashyap & Chaudhary, 2023). Međutim, sprovođenje takvih propisa često nailazi na prepreke u dijelu nadzora – ukoliko institucije zadužene za kontrolu nemaju dovoljno tehničkih kapaciteta ili pravnih alata za brzu intervenciju u slučaju povrede podataka, efekat samog zakona ostaje ograničen. Regulatorni zahtjevi moraju također biti povezani s međunarodnim standardima kako bi domaće kompanije mogle nesmetano poslovati na globalnom tržištu. Standardi poput ISO/IEC 27001 integrišu se kroz nacionalne strategije sajber bezbjednosti kako bi se domaći subjekti uskladili s praksama svojih inostranih partnera. Neusklađenost može dovesti do gubitka poslovnih prilika; partner iz EU može odbiti saradnju ako domaće preduzeće ne posjeduje certifikate koji potvrđuju primjenu minimalnih kontrola zaštite podataka. Izostanak centralizovanih institucija poput CERT-a na nivou države ili entiteta otežava implementaciju zakona koji predviđaju koordinisano reagovanje na široko rasprostranjene prijetnje. U situaciji kada formalna struktura ne postoji, MSP su prisiljena da se oslanjaju na ad hoc mreže saradnje sa privatnim sektorom ili akademskim institucijama radi razmjene informacija o prijetnjama. Ovo rješenje je funkcionalno samo do određene granice – bez formalne podrške zakonodavca takva saradnja nema standardizovane protokole ni garanciju obaveznosti postupanja svih uključenih strana. Postoje i problemi egzekucije regulative: čak kada su zakoni donijeti, njihovo sprovođenje može oslabiti zbog slabog institucionalnog kapaciteta inspekcijskih organa ili sudova nadležnih za sankcionisanje povreda. Primjer jedne napredne azijske države pokazuje da izazovi u provođenju regulative dovode do situacije gdje pravni okvir postoji samo nominalno; digitalna infrastruktura ostaje ranjiva jer mehanizmi nadzora nisu dovoljno efikasni (Judijanto, Rahardian, et al., 2023). Razmatranje regulatornog okvira za informacionu bezbjednost mora uključiti i međunarodne ugovore te direktive koje dopunjuju nacionalne

propise. Regionalne koalicije često propisuju minimalne standarde koje sve članice treba da inkorporiraju u sopstveni zakonodavni sistem. Za MSP to znači da pored državnog zakonodavstva moraju pratiti obaveze koje proizilaze iz članstva zemlje u takvim inicijativama. Poseban segment čini oblast e-trgovine gdje zakoni o sajber bezbjednosti moraju pratiti dinamiku tržišta koje funkcioniše gotovo isključivo preko digitalne infrastrukture (Kashyap & Chaudhary, 2023). Tu je važno definisati odgovornost učesnika transakcije – od provajdera platforme do krajnjeg korisnika – kako bi se umanjio rizik od zloupotreba i povećalo povjerenje kupaca. Sinhronizacija zakonskih okvira sa tehničkim smjernicama kao što su one definisane u NIST CSF-u doprinosi praktičnoj provedbi kontrole koje dokumenti poput ISO standarda opisuju na konceptualnom nivou (Thach et al., 2020). Time se osigurava da propisi nisu samo deklarativni već implementirani kroz definisane procedure koje MSP mogu slijediti prema svojim kapacitetima. U konačnici, kvalitet regulatornog okvira mjeri se njegovom sposobnošću da poveže pravne norme sa operativnim praksama organizacija različitih profila. Zakoni koji ostaju izolovani od realnog poslovnog konteksta završavaju kao birokratsko opterećenje bez suštinskog doprinosa sigurnosti sistema. Zato analiza zahtjeva mora uzeti u obzir ne samo formalnu usklađenost sa tekstom propisa nego i nivo podrške koju institucije pružaju subjektima pri njihovoj primjeni.

2.2.3. Uticaj globalizacije i digitalizacije

Procesi globalizacije i digitalizacije izuzetno su transformisali okruženje u kojem se razvija i sprovodi informaciona sigurnost, stvarajući istovremeno nove mogućnosti i izazove za male i srednje preduzetnike. Globalizacija podrazumijeva međusobnu povezanost tržišta, protok informacija i kapitala, dok digitalizacija unosi široku primjenu informaciono-komunikacionih tehnologija u gotovo sve aspekte poslovanja. Ovi trendovi zajedno ubrzavaju razmjenu podataka preko nacionalnih granica, ali i povećavaju broj vektora napada koji potiču iz različitih geografskih i pravnih okvira, što zahtijeva kompleksniji pristup zaštiti resursa. Digitalna transformacija direktno utiče na diversifikaciju prijetnji koje pogađaju preduzeća. Prelazak na cloud infrastrukturu, integracija IoT uređaja u proizvodne i administrativne procese te razvoj e-poslovanja proširuju digitalni pejzaž organizacije(Kamis et al., 2026). Svaki novi segment digitalnog poslovanja donosi specifične bezbjednosne zahtjeve – od šifrovanja komunikacionih kanala do usklađivanja sa međunarodnim propisima o zaštiti podataka. Povećana zavisnost MSP-ova od mrežnih servisa povlači potrebu da se standardi poput

ISO/IEC 27001 ili NIST CSF-a promatraju ne samo kroz prizmu tehničke implementacije, već kao temelj za održavanje interoperabilnosti sa partnerima iz drugih zemalja (Peña-Montes De Oca i Mondragón-Gutiérrez, 2023). Jedan od najizraženijih efekata globalizacije na informacionu bezbjednost jeste pritisak da se lokalni sistemi usklade sa regulativama koje važe u jurisdikcijama ključnih poslovnih partnera. Na primjer, kompanije koje posluju sa državama članicama EU suočavaju se sa potrebom poštovanja General Data Protection Regulation (u daljem tekstu: GDPR), čak i kada domaći zakoni ne predviđaju identične obaveze. Ovaj pritisak može dovesti do adaptacije internih procedura koje prevazilaze minimalne lokalne zahtjeve, čime se stvara složenija struktura bezbjednosne politike. Globalizacija je povećala učestalost transnacionalnih sajber napada. Napadi više nisu ograničeni na lokalno ili regionalno tržište; sofisticirani akteri koriste distribuirane mreže kako bi targetirali sisteme širom planete, često iskorištavajući ranjivosti koje proizlaze iz razlika u regulatornim sistemima. U takvom kontekstu MSP moraju razvijati nove moderne modele procjene rizika koji uzimaju u obzir geografski raspon mogućih prijetnji. Standardi upravljanja rizikom predloženi u dokumentima poput ISO/IEC 27005 omogućavaju strukturnu analizu koja uključuje međunarodne incidente kao parametar procjene vjerovatnoće i uticaja napada (Shekh, 2024). Sa druge strane, digitalizacija uvodi tehnologije koje redefinišu operativni tok MSP-a – od automatizovanih procesa nabavke do elektronskog obračuna finansija. Implementacija složenih informaciono-komunikacionih sistema donosi korist kroz optimizaciju, ali istovremeno generiše nove tačke potencijalnog kompromitovanja podataka. IoT senzori za praćenje produktivnosti mogu biti zloupotrebljeni zbog slabog sistema autentifikacije; cloud platforme mogu biti meta napada metodama prilagođenim specifičnostima tog okruženja, poput „cross-tenant" eksploatacija (Isaac, et al., 2024). Tehnološka konvergencija u okviru digitalizacije stvara situaciju gdje tradicionalna granica između internog sistema preduzeća i spoljnog partnera postaje fluidna. Korištenje zajedničkih Software as a Service (u daljem tekstu: SaaS) aplikacija ili dijeljenih aplikacijskih programskih interfejsa (u daljem tekstu: API) znači da sigurnosni incident kod jednog partnera može imati kaskadni efekat na cjelokupnu mrežu uključenih entiteta. To pojačava značaj implementacije sigurnosnih standarda koji predviđaju koordinisane reakcije na incidente (Judijanto, et al., 2023). Nacionalni pristupi bezbjednosti često se susreću s izazovima interpretacije međunarodnih normi u lokalnom kontekstu. Na primjer, mala kompanija može posjedovati tehničke kapacitete da primjeni enkripciju podataka prema AES-256 standardu, ali nedostaje

joj pravna struktura koja bi definisala pravila za razmjenu tih podataka sa inostranim partnerima niti ima institucionalnu podršku preko nacionalnog CERT-a. Nedostatak formalne koordinacije otežava pravovremeno reagovanje na prijetnje koje prelaze granice IT infrastrukture jedne zemlje. Digitalizacija također donosi veću dostupnost alata za sajber zaštitu – od besplatnih antivirus programa do sofisticiranih AI sistema za detekciju anomalija u mrežnom saobraćaju (Islam, et al., 2024). Međutim, mala preduzeća često nailaze na barijere prilikom integracije ovih tehnologija; visoka cijena licenci ili složena konfiguracija može rezultirati time da instalirani sistem ostane neaktiviran ili podešen s „default“ parametrima koji su ranjivi na napade. Upravo ova dihotomija između povećane povezanosti (zahvaljujući globalnoj ekonomiji) i fragmentiranosti regulative zahtijeva poseban pristup MSP planiranju svojih bezbjednosnih strategija. Potrebno je uzeti u obzir ne samo lokalne tehničke mogućnosti već i sposobnost integracije resursa kroz međunarodnu saradnju – bilo formalnu putem ugovora o bezbjednosnom partnerstvu ili neformalnu kroz razmjenu informacija o prijetnjama putem industrijskih asocijacija (Sharkov, 2020). Uticaj globalizacije vidljiv je čak i u svakodnevnim operacijama MSP-a kroz zahtjev da njihovi sistemi budu kompatibilni sa raznovrsnim tehnološkim okruženjima partnera iz različitih zemalja. Sa aspekta digitalizacije ovo znači prilagođavanje softverskih rješenja višestrukim jezicima aplikacija, valutama transakcija i tehničkim zahtjevima interoperabilnosti različitih baza podataka – što dodatno komplikuje sigurnosnu konfiguraciju čitavog sistema. Na kraju treba istaći kako oba procesa – globalizacija i digitalizacija – generišu stalnu potrebu za ažuriranjem bezbjednosnih politika unutar MSP-a kako bi one zadržale funkcionalnost uprkos dinamičnim promjenama poslovnog okruženja i tehnološkog spektra dostupnih rješenja za zaštitu podataka. Integrisanje ovih politika s tehnološkim alatima mora biti praćeno edukacijom korisnika o scenarijima prijetnji koji prate internacionalno poslovanje i upotrebu digitalne infrastrukture, čime se stvara otporniji sistem sposoban da odgovori izazovima jedinstvenim za spoj globalnog tržišta i sveprožimajuće digitalne tehnologije.

2.2.4. ISO 27001

Standard ISO/IEC 27001:2013 definiše međunarodno prihvaćen okvir za uspostavljanje, implementaciju, održavanje i kontinuirano unapređenje Sistema upravljanja bezbjednošću informacija (u daljem tekstu: ISMS) (Hlaponin, et al., 2022). On pruža strukturiran skup zahtjeva koje organizacije mogu koristiti kao osnovu za izgradnju slojevite zaštite svojih

podataka i informacionih sistema u skladu sa principima koje promoviše strategija „Defense in Depth“. Dok sama strategija podrazumijeva višestruke međusobno komplementarne nivoe kontrole – od perimetarske zaštite do aplikativnog nadzora – ISO 27001 daje operativnu metodologiju kako sve te slojeve integrisati unutar jedinstvenog upravljačkog sistema. Jezgro ISO 27001 temelji se na pristupu zasnovanom na procjeni rizika, pri čemu se identifikuju potencijalne prijetnje, ranjivosti i uticaj na poslovne procese, nakon čega se definišu odgovarajuće kontrolne mjere (Neri et al., 2022). Takav pristup direktno korespondira sa filozofijom „Defense in Depth“ jer omogućava dizajniranje više slojeva odbrane prema prioritetima proisteklim iz analize rizika. Na primjer, ako procjena pokaže visoku vjerovatnoću DoS napada na mrežnu infrastrukturu, perimetarski sloj se nadograđuje specifičnim mehanizmima filtriranja saobraćaja i sistemima za prevenciju upada. Istovremeno, unutrašnja segmentacija mreže minimizuje lateralno kretanje napadača čak i ako prvi sloj bude probijen. ISO 27001 uključuje Anex A koji sadrži referentni skup kontrola preuzetih iz ISO/IEC 27002; one obuhvataju različite aspekte bezbjednosti – upravljanje identitetom i pristupom, kriptografske mjere, fizičku bezbjednost, bezbjednost operacija – koje su svi prepoznatljivi elementi u višeslojnoj arhitekturi (Hlaponin, et al., 2022). Upravljanje identitetom u okviru standarda podrazumijeva definisanje pravila za kreiranje, izmjenu i brisanje korisničkih naloga te kontrolu privilegija prema principu najmanjih ovlaštenja. Ove procedure su ključan unutrašnji sloj odbrane koji sprečava zloupotrebu ili eskalaciju pristupa. Kada se povežu sa višefaktorskom autentifikacijom omogućenom kroz tehničke mehanizme, dobija se snažna barijera protiv neovlaštenog pristupa. Perimetarska zaštita unutar ISO 27001 okvira tretirana je kao dio kontrolnih mjera koje obezbjeđuju bezbjednost komunikacionih mreža. To podrazumijeva instalaciju firewall-a, IDS/IPS sistema te enkripciju komunikacije radi osiguranja povjerljivosti i integriteta podataka u tranzitu (Neri, et al., 2022). Enkripcija nije samo tehnička mjera već i dio proceduralne politike koja se sprovodi kroz dokumentovana pravila ISMS-a. Time se povezuje tehnička implementacija sa širim organizacionim kontekstom. Edukacija korisnika prema ISO 27001 spada u domen podizanja svijesti o bezbjednosti informacija i kontinuiranog treninga zaposlenih (Hlaponin, et al., 2022). Taj element ima jednaku važnost u „Defense in Depth“ strategiji jer ljudski faktor često predstavlja najranjiviji sloj odbrane. Obučeni korisnici bolje prepoznaju phishing pokušaje ili anomalije u radu sistema, čime doprinose ukupnoj otpornosti organizacije. Standard propisuje redovne programe edukacije i evaluacije efikasnosti tih programa. Redundantnost i

oporavak od katastrofe također pronalaze mjesto unutar ISO 27001 preko kontrola koje se odnose na kontinuitet poslovanja. Procedure poput odziva na incidente (Incident Response), kreiranja rezervnih kopija i testiranja procedura oporavka definisane su kao obavezni elementi ISMS-a za osiguranje dostupnosti resursa. Ove mjere su direktan odgovor na potencijalne prekide usluga – bilo izazvane sajber napadima ili fizičkim kvarovima – te predstavljaju slojeve zaštite koji stupaju na snagu kad preventivne kontrole ne uspiju da spriječe incident. Standard ističe važnost stalnog praćenja performansi bezbjednosnih kontrola putem internih audita i pregleda rukovodstva (Hlaponin, et al., 2022). Kontinuirani nadzor uklapa se u koncept „Defense in Depth“ kao zaseban sloj detekcije anomalija unutar sistema. SIEM sistemi ili drugi alati za centralizovano prikupljanje i analizu log-ova mogu biti tehnička podrška ovom zahtjevu; njihova svrha je brza identifikacija događaja koji odstupaju od normalnog stanja rada. ISO 27001 eksplicitno zahtijeva dokumentovanje svih politika, procedura i zapisa vezanih uz bezbjednost informacija. Ovaj formalni okvir dokumentacije olakšava koordinaciju među različitim slojevima odbrane – od tehničke infrastrukture do ljudskih procesa – jer svaki segment ima jasno definisanu svrhu, odgovornost i način verifikacije ispravnosti rada. Dokumentovanjem kontrola smanjuje se rizik preklapanja funkcionalnosti ili stvaranja praznina između slojeva. Primjena ISO 27001 standarda donosi dodatnu vrijednost MSP-ovima kojima su finansijski resursi ograničeni jer omogućava fokusiranje na prioritetne rizike proistekle iz analize poslovnog konteksta (Wang, 2023). Integrisanjem ovog okvira u strategiju „Defense in Depth“ MSP mogu birati kontrole koje daju najveći doprinos otpornosti uz minimalan trošak održavanja. Povezanost između standarda i višeslojnog modela osiguranja pokazuje se kroz ciklus Plan-Do-Check-Act koji je temelj ISO 27001 metodologije. U planiranju se definišu slojevi prema identifikovanim prijetnjama i to faza implementacije uključuje postavljanje tehničkih i organizacionih mjera; faza provjere prati njihovu efikasnost kroz nadzor, a faza djelovanja podrazumijeva korekciju nedostataka ili nadogradnju postojećih slojeva. Ovakav ciklus osigurava da „Defense in Depth“ strategija ostane dinamična i usklađena sa realnim potrebama organizacije tokom vremena. Ono što posebno vrijedi naglasiti jeste da ISO 27001 ne propisuje konkretne tehnologije nego ciljeve koje treba postići svakom kategorijom kontrole. To pruža fleksibilnost adaptacije različitim industrijama dok zadržava konzistentnost načela višeslojne zaštite: bez obzira koristi li organizacija komercijalne firewall-e ili open-source rješenja za IDS/IPS, bitno je da ti mehanizmi ispunjavaju svoj definisani zadatak u mrežnom sloju odbrane. Na isti način planovi

oporavka mogu koristiti cloud ili on-premise infrastrukturu, sve dok zadovoljavaju zahtjeve standarda o dostupnosti. Treba primjetiti da integracija ISO 27001 okvira sa strategijom „Defense in Depth“ omogućava MSP-ima postavljanje mjerljivih ciljeva bezbjednosti te njihovo dokazivo ispunjavanje prema internim ili eksternim auditima. Time se stvara stanje gdje višeslojna zaštita nije samo konceptualna već provjerljiva praksa podložna stalnom unapređenju na temelju empirijskih podataka o efikasnosti pojedinih slojeva.

2.2.5. NIST okvir

NIST je razvio okvir sajber bezbjednosti sa ciljem da pomogne organizacijama, uključujući MSP, u upravljanju rizicima i implementaciji sveobuhvatnog sistema zaštite digitalnih resursa. Okvir se zasniva na pet osnovnih funkcija: identifikacija, zaštita, detekcija, reagovanje i oporavak. Ove funkcije se mogu posmatrati kao međusobno povezani slojevi unutar koncepta Defense in Depth, gdje svaki nivo ima sopstvenu ulogu u sprečavanju ili umanjenju efekata sajber prijetnji. Funkcija identifikacije uključuje procese inventarizacije opreme, softverskih komponenti i podataka koji su kritični za poslovanje. Ona postavlja osnovu za pravilnu konfiguraciju perimetarske zaštite kroz definisanje granica mrežnog okruženja u skladu sa mapom resursa. Uz to, kreiranje politike sajber bezbjednosti koja jasno određuje odgovornosti i postupke zaštite omogućava da organizacija definiše prioritete kod dodavanja novih slojeva odbrane. Taj sloj mapiranja resursa značajno olakšava kasniju segmentaciju mreže jer se jasno zna koje komponente zahtijevaju dodatnu izolaciju. Funkcija zaštite unosi u proces mehanizme kontrolisanog pristupa mreži i aplikacijama, primjenu sigurnosnog softvera, enkripciju podataka kako bi se očuvala povjerljivost i integritet informacija, kao i sprovođenje redovnih rezervnih kopija bitnih podataka. MFA ovdje ima presudnu vrijednost – ona stvara dodatnu prepreku napadaču čak i ako uspije da pribavi kredencijale korisnika (Neri, et al., 2022). Automatizovana ažuriranja softvera osiguravaju brzo zatvaranje poznatih ranjivosti koje bi eventualno mogle biti iskorištene za kompromitovanje jednog sloja odbrane. Treća funkcija, detekcija, odnosi se na praćenje u realnom vremenu radi otkrivanja neovlaštenih aktivnosti ili anomalija u radu sistema. Nadzorni sistem može uključivati IDS/IPS rješenja i SIEM platforme koje prikupljaju log-ove iz različitih slojeva infrastrukture kako bi generisale alarm pri uočenom odstupanju od normalnog obrasca rada (Amro & Gkioulos, 2023). U kontekstu Defense in Depth modela, ova funkcija obezbjeđuje da čak i ako perimetarska zaštita bude probijena, unutrašnji slojevi poput segmentacije mreže ili

aplikativnog nadzora otkriju napad prije nego što dođe do potpune eskalacije. Prednost ovakvog pristupa jeste mogućnost povezivanja događaja iz fizičke infrastrukture, mrežnih komponenti i aplikacija radi dobijanja holističkog pogleda na stanje sistema. Funkcija reagovanja bavi se operativnim procedurama koje stupaju na snagu kada se detektuje incident. Plan reagovanja mora sadržavati protokol za izolovanje pogođenih segmenata mreže, obavještavanje relevantnih strana i privremeno održavanje kontinuiteta ključnih poslovnih operacija. Integrisana struktura kontrole omogućava brzu aktivaciju svih potrebnih slojeva odbrane, od blokiranja kompromitovanih naloga preko primjene rezervnih resursa do uspostavljanja komunikacije sa regulatornim tijelima. Ovakva koordinacija direktno smanjuje vrijeme potrebno da incident bude stavljen pod kontrolu. Posljednja funkcija, oporavak, povezuje redundantne mehanizme sistema sa formalnim procedurama obnove podataka i vraćanja pune operativne funkcionalnosti nakon incidenata. U višeslojnom okviru ovo znači vraćanje rada kako tehničkih komponenti tako i proceduralnih pravila koja su eventualno bila privremeno modifikovana tokom incidenta. Redundantna infrastruktura mora biti testirana unaprijed kroz simulaciju katastrofalnih scenarija kako bi se provjerila pouzdanost failover mehanizama (n.a., 2009). Primjena NIST okvira u MSP-ima donosi posebne izazove zbog ograničenih budžetskih kapaciteta. Međutim, njegova modularna struktura dozvoljava prilagođavanje tako da najkritičniji resursi budu pokriveni odgovarajućim slojevima odbrane (Ejjami, 2024). Na primjer, ako MSP raspolažu manjim brojem servera koji čuvaju osjetljive podatke klijenata, NIST okvir pomaže pri odluci koje kontrole moraju biti postavljene oko tih serverskih instanci, prvenstveno perimetarski firewall sa pravilima pristupa baziranim na Internet protocol (u daljem tekstu: IP) filtriranju, pa segmentacija koja izdvaja bazu podataka u zasebnu sigurnosnu zonu, i enkripcija podataka korištenjem Advanced Encryption Standard (u daljem tekstu: AES) algoritma tokom skladištenja, zatim monitoring u realnom vremenu za praćenje upita ka bazi i na kraju redovan backup sa verifikacijom integriteta kopija. Kombinovanjem NIST strukture sa filozofijom Defense in Depth dobija se metodološki okvir koji istovremeno zadovoljava tehničke standarde i pruža prostor za edukaciju ljudskih resursa kao dijela sistema zaštite (Neri, et al., 2022). Edukacija spada u funkciju zaštite prema NIST-u jer sprečava proboj socijalno-inženjerskim metodama kojima tehnički sistemi često nisu dorasli. Treninzi rada unutar propisanih granica privilegija korisnika smanjuju rizik namjernog ili nenamjernog narušavanja povjerljivosti ili integriteta informacijskih resursa. Implementacija ovog okvira zahtijeva stalnu evaluaciju efikasnosti svakog sloja kako bi se

identifikovala područja za poboljšanje. Upotreba metrike poput Mean Time to Detect (u daljem tekstu: MTTD) i Mean Time to Respond (u daljem tekstu: MTTR) pomaže pri „kvantifikovanju“ performansi postojećih kontrola, tako ako su ta vremena predugačka, NIST preporučuje dodavanje ili unapređenje specifičnih mehanizama unutar funkcija detekcije ili reagovanja. Na strateškom nivou, prednost NIST okvira ogleda se u njegovoj fleksibilnosti da obuhvati kombinaciju preventivnih mjera (perimetarska kontrola pristupa, enkripcija), detekcionih alata (monitoring performansi sistema), reaktivnih protokola (incident response) te kontinuiranih aktivnosti obnove poslovanja (disaster recovery). Sve ove komponente su kompatibilne sa višeslojnom arhitekturom jer svaka predstavlja zaseban ali komplementaran sloj bezbjednosnog ekosistema organizacije. Takva kompatibilnost olakšava integraciju okvira čak i kod MSP-a koja nemaju opsežne timove sajber bezbjednosti; modularnost NIST-a daje mogućnost gradnje od osnovnog ka naprednom nivou po mjerilima poslovnog konteksta. Nacionalni okvir time postaje alat ne samo za ispunjenje regulatornih zahtjeva već i za praktičnu operacionalizaciju koncepta Defense in Depth kroz jasno definisane faze rada koje prate životni ciklus napada; prvi korak je priprema kroz identifikaciju resursa, zatim stvaranje barijera putem zaštitnih mjera, nakon čega nastupa praćenje dešavanja radi detekcije pokušaja kompromitacije, u procesu je potrebno uraditi upravljanje incidentom dok traje, a oporavak uz vraćanje punog potencijala odbrambenog sistema radi se nakon završetka krizne situacije. Ova sinteza procesa pruža MSP-ima realne smjernice kako da optimalno rasporede svoje tehničke kapacitete i ljudske resurse radi očuvanja sigurnosti informacionih sistema na nivou uporedivom sa znatno većim organizacijama.

2.3. Uloga nacionalnih institucija

Uspostavljanje efikasnog sistema informacione sigurnosti na nacionalnom nivou predstavlja jedan od ključnih izazova savremenih država, naročito u kontekstu rastućih sajber prijetnji i povećane zavisnosti društva od digitalne infrastrukture. Nacionalne institucije imaju centralnu ulogu u definisanju strateških ciljeva, normativnog okvira i koordinacije aktivnosti u oblasti informacione sigurnosti. Međutim, u državama sa složenom administrativnom strukturom kao što Bosna i Hercegovina i nedovoljno razvijenim institucionalnim kapacitetima, izostanak jedinstvenog nacionalnog CERT-a značajno otežava koordinisan odgovor na sajber incidente.

U takvom okruženju, odgovornosti vezane za prevenciju, detekciju i odgovor na sigurnosne incidente često su fragmentirane između više institucija, sektorskih tijela ili entitetskih i organizacijskih CERT timova. Ovakva decentralizacija dovodi do neujednačenih sigurnosnih praksi, ograničene razmjene informacija i usporene reakcije na incidente koji imaju međusektorski ili transnacionalni karakter. Nedostatak centralnog koordinacionog tijela dodatno otežava saradnju sa međunarodnim organizacijama i mrežama CERT/CSIRT timova, što je od posebnog značaja u kontekstu globalne prirode sajber prijetnji.

Uloga nacionalnih institucija u ovakvim okolnostima ogleda se prvenstveno u stvaranju regulatornih i strateških pretpostavki za budući razvoj nacionalnog sistema sajber sigurnosti. To uključuje izradu nacionalnih strategija informacione sigurnosti, usklađivanje zakonodavstva sa međunarodnim standardima i direktivama, kao i podsticanje formiranja sektorskih CERT-ova u kritičnim oblastima poput energetike, telekomunikacija i finansijskog sektora. Istovremeno, nacionalne institucije imaju odgovornost da iniciraju mehanizme saradnje, razmjene informacija i zajedničkih procedura za upravljanje incidentima, čak i u odsustvu formalno uspostavljenog državnog CERT-a.

U tom smislu, izostanak nacionalnog CERT-a ne treba posmatrati isključivo kao institucionalni nedostatak, već i kao razvojnu fazu u izgradnji cjelovitog sistema informacione sigurnosti. Aktivna uloga nacionalnih institucija u jačanju kapaciteta, edukaciji kadrova i međunarodnoj saradnji može predstavljati osnovu za postepeno uspostavljanje centralizovanog mehanizma za odgovor na sajber incidente, u skladu sa specifičnim političko-administrativnim i pravnim okvirom države.

2.3.1. Funkcija CERT-a u sajber zaštiti

Funkcija CERT-a u sistemu sajber zaštite obuhvata specifičan skup zadataka koji imaju cilj da identifikuju, analiziraju i koordinišu odgovore na incidente u informacionim sistemima, pružajući stručno vođstvo organizacijama pogođenim napadima. CERT timovi djeluju kao centralna tačka za prikupljanje i distribuciju informacija o prijetnjama, ranjivostima i preporukama za mitigaciju, čime se ostvaruje koordinisan pristup rješavanju problema sajber bezbjednosti (Kashyap & Chaudhary, 2023). Njihova uloga je posebno vidljiva u kontekstu nacionalnih okvira gdje predstavljaju vezu između javnog sektora, privatnih kompanija i međunarodnih sigurnosnih mreža. U državama sa razvijenim institucionalnim modelom, poput onih koje su integrisane u Forum of Incident Response and Security Teams (u daljem

tekstu: FIRST) ili evropski TF-CSIRT okvir, nacionalni CERT funkcioniše kao registrovana institucija unutar globalne mreže od oko 300 timova širom svijeta (Krulík, 2018). Ova integracija omogućava brzu razmjenu tehničkih podataka o novootkrivenim napadima i ranjivostima te nadogradnju sopstvenih kapaciteta kroz međunarodnu saradnju. U takvim sistemima CERT ima direktan pristup informacijama koje mogu imati kritičan značaj za sprečavanje domino efekta sajber incidenata koji prelaze granice pojedinačnih infrastruktura. Specifičnost funkcije CERT-a ogleda se i u njegovom mandatu da postupa proaktivno – publikovanjem upozorenja o potencijalnim kampanjama napada i distribucijom tehničkih smjernica za jačanje odbrane. Na primjer, državni CERT-ovi pojedinih država objavljuju preporuke, tehničke biltene, konsultativne dokumente o ranjivostima softverskih paketa koji se masovno koriste u e-trgovini ili javnim službama, zajedno sa smjernicama za implementaciju zakrpa. Takva praksa smanjuje vrijeme potrebno da organizacije reaguju na novoidentifikovane prijetnje. Osnova operativne efikasnosti CERT-a je jasno definisana struktura ovlaštenja. Dok neke jurisdikcije daju nacionalnom CERT-u izvršna prava da naloži primjenu određenih mjera zaštite na nivou kritične infrastrukture ili sektorskih sistema (Kashyap & Chaudhary, 2023), drugi modeli ga pozicioniraju isključivo kao savjetodavno tijelo bez direktnog mandata za sprovođenje akcija.

Nedostatak legislativne podrške znači da i najstručniji tim ostaje ograničen u primjeni svojih preporuka kada organizacije nisu voljne ili spremne da ih usvoje. CERT timovi imaju zadatak da prate tokove prijave incidenata od trenutka kada organizacija identifikuje problem do njegove finalne analize. Tokom ovog procesa oni definišu prioritete reakcije prema težini incidenta – što može uključivati izolaciju kompromitovanog sistema iz mreže, zaštitu forenzičkih dokaza radi eventualne pravne procedure i obnavljanje funkcionalnosti servisa na siguran način. Spremnost na brzu intervenciju zahtijeva stalnu dostupnost ekspertskog kadra koji poznaje specifičnosti nacionalnog digitalnog okruženja. Saradnja sa sektorom kritične infrastrukture zahtijeva od CERT-a poseban protokol rada zbog potencijalno katastrofalnih posljedica nepravilno kontrolisanog napada. U mnogim industrijskim sektorima kompromitovanje kontrolnog domena sistema može dovesti do direktnih fizičkih šteta (Kuipers & Fabro, 2006). Iz tog razloga CERT često razvija sektorski prilagođene planove djelovanja koji uključuju izolaciju ključnih kontrolnih resursa, redundansu komunikacionih kanala i testiranje otpornosti implementiranih bezbjednosnih mjera. Veza između

nacionalnog CERT-a i lokalnih organizacionih CSIRT timova predstavlja važan segment koordinacije sajber zaštite. Lokalni CSIRT-i unutar akademskih institucija, industrijskih konzorcija ili velikih korporacija primjenjuju specifične politike zasnovane na tehničkoj prirodi svoje infrastrukture. Nacionalni CERT prikuplja izvode iz iskustava tih timova kako bi formirao agregirane preporuke relevantne za širu zajednicu (Krulík, 2018). Interakcija između dva nivoa omogućava preciznije adresiranje prijetnji koje su već viđene unutar pojedinačnih sektora. U situacijama gdje formalni državni CERT ne postoji ili nema adekvatan pravni okvir djelovanja – kao što je slučaj u Bosni i Hercegovini – preduzeća se mogu osloniti na partnerstva s regionalnim sigurnosnim tijelima ili industrijskim udruženjima radi razmjene informacija o prijetnjama. Iako takva rješenja donekle popunjavaju prazninu, ona rijetko uključuju standardizovane protokole prijave i koordinisanog odgovora zasnovane na međunarodno priznatoj metodologiji. Time dolazi do varijabilnosti kvaliteta reakcije koja zavisi od kapaciteta pojedinačnog aktera. Funkcija CERT-a se ne iscrpljuje samo u tehnološkim intervencijama već obuhvata kontinuiranu edukaciju subjekata o promjenjivom karakteru sajber prijetnji. Organizovanje radionica, simulacija incidenata i javno dostupnih obrazovnih materijala omogućava povećanje svijesti kod krajnjih korisnika o njihovoj ulozi u sprečavanju napada. Edukativni programi često naglašavaju odgovornost svakog učesnika digitalnog ekosistema – od tehničkog osoblja koje upravlja mrežom do običnih korisnika koji svakodnevno pristupaju sistemu. Na međunarodnom planu članstvo nacionalnog CERT-a u globalnim mrežama incident odgovora predstavlja ključnu prednost za pravovremeno dobavljanje informacija o novim tipovima prijetnji. Pristup bazi znanja FIRST-a ili TF-CSIRT platforme omogućava brz transfer tehničkih detalja potrebnih za razvoj zakrpa ili blokiranje malicioznih kampanja prije nego što postanu raširene. Za MSP ovaj kanal komunikacije može biti jedini način da blagovremeno implementiraju efikasnu zaštitu protiv prijetnji koje potiču izvan lokalnog konteksta. Na kraju, vrijednost funkcije CERT-a mjeri se sposobnošću transformacije prikupljenih informacija o prijetnjama u praktične vodiče djelovanja prilagođene različitim vrstama organizacija. Kombinovanjem tehničke ekspertize sa vještinama koordinacije među više subjekata istovremeno se postiže operativna otpornost sistema na incidente i osigurava kontinuitet poslovanja čak u uslovima visokog intenziteta sajber ugrožavanja. Bez ovakve centralizovane funkcije razmjena informacija ostaje fragmentna, a zatvaranje ranjivosti sporije, što povećava mogućnost ponavljanja istih tipova napada kroz duži vremenski period (Kosseff, 2019).

2.3.2. Preporuke za razvoj nacionalnog CERT-a

Razvoj nacionalnog CERT-a zahtijeva sveobuhvatan pristup koji kombinuje institucionalno planiranje, zakonsku podršku i tehničke kapacitete u skladu sa međunarodnim standardima. Posmatrano iz perspektive trenutnog nedostatka formalne strukture, neophodno je definisati korake koji će omogućiti stabilno funkcionisanje ovog tijela od samog početka njegovog postojanja. Institucionalni dizajn mora obuhvatiti jasnu podjelu nadležnosti između različitih sektora – javnog, privatnog i akademskog, – kako bi se osigurala potpuna pokrivenost svih relevantnih segmenata digitalne infrastrukture (Baker & Robinson, 2022). U tom pogledu, formiranje koordinacionog odbora unutar kojeg bi predstavnici ključnih sektora imali jasno definisane zadatke može doprinijeti smanjenju fragmentacije informacija o prijetnjama. Zakonski okvir treba da pruži CERT-u ovlaštenja neophodna za efikasno djelovanje. Njegova uloga neće biti potpuna ukoliko se ograniči na savjetodavne funkcije bez mogućnosti nametanja obaveznih bezbjednosnih mjera kada se utvrdi ozbiljna ugroženost kritične infrastrukture. Modeli iz zemalja koje već posjeduju nacionalni CERT pokazali su da prisustvo izvršnih ovlaštenja, posebno u sektorima energetike, telekomunikacija i javne administracije, značajno ubrzava implementaciju zaštitnih procedura. Da bi zakonska podrška bila operativna, dokumenti moraju definisati protokole prijave incidenata, vremenske okvire reakcije i sankcije za nepostupanje u skladu sa preporukama ili nalozima nacionalnog CERT-a. Potrebno je predvidjeti opremljenost stručnjaka alatima za analizu zlonamjernog koda, forenzičku obradu događaja i pregled mrežnog saobraćaja u realnom vremenu (Rébé, 2022). Ove tehnologije se moraju uskladiti sa standardima interoperabilnosti kako bi tim mogao komunicirati sa drugim nacionalnim i međunarodnim CERT strukturama bez tehničkih prepreka. Integracija u mreže poput FIRST ili TF-CSIRT treba biti prioritet, jer ona širom otvara pristup bazama znanja o novim tipovima prijetnji i omogućenim vektorima napada (Krulík, 2018). Edukativna komponenta razvoja nacionalnog CERT-a jednako je važna kao tehnička. Pored obuke internog osoblja, potrebno je planirati kontinuirane programe informisanja javnosti i poslovne zajednice o prijetnjama koje se pojavljuju i mjerama zaštite koje su dostupne (Kashyap & Chaudhary, 2023). Radionice, simulacije incidenta i javne kampanje stvaraju osnovu za širenje svijesti da sajber rizik nije statičan fenomen, već dinamičan proces kojim upravljaju mnogi faktori – od ljudske greške do sofisticiranih napada koji koriste ranjivosti kontrolnih sistema. Poseban naglasak treba staviti na sektor-specifične protokole reagovanja. Na primjer, industrijski sistemi kontrole (Industrial Control System, u daljem

tekstu: ICS) imaju jedinstvene sigurnosne izazove jer njihova kompromitacija može dovesti do fizičkih šteta velikih razmjera. Nacionalni CERT mora razviti priručnike prilagođene ovakvim okruženjima koji definišu procedure izolacije kritičnih resursa, održavanja komunikacione redundanse i testiranja otpornosti uvedenih mjera na potencijalne napade. Veza između nacionalnog CERT-a i lokalnih CSIRT timova treba biti institucionalizovana kroz formalne kanale razmjene informacija o incidentima. Lokalni timovi često prvi dolaze do saznanja o pojavi nove prijetnje unutar svoje organizacije ili sektora; pravovremeno prosljeđivanje tih podataka centralnom tijelu omogućava izgradnju zajedničke baze znanja koja povećava brzinu reakcije (Krulík, 2018). Formalizovana saradnja smanjuje varijabilnost kvaliteta odgovora, jer uvodi standardizovane protokole prijave i obrade incidenata zasnovane na međunarodno priznatoj metodologiji. Implementacija interoperabilnih sistema za detekciju i praćenje prijetnji mora biti dio početnog plana formiranja nacionalnog CERT-a. Korištenjem globalno priznatih modela kao što je Cybersecurity Capacity Maturity Model for Nations (u daljem tekstu: CMM), moguće je procijeniti zrelost domaćih kapaciteta kroz dimenzije politike, strategije, tehnoloških kontrola i obrazovanja (Sharkov, 2020). Rezultati takvih analiza usmjeravaju gdje treba ulagati najviše napora – bilo da se radi o pravnoj infrastrukturi, tehničkoj opremi ili edukaciji kadra. U okviru međunarodne saradnje važno je zajamčiti mogućnost brze razmjene tehničkih detalja novootkrivenih ranjivosti. Nacionalni CERT treba da potpiše memorandume o razumijevanju (u daljem tekstu: MoU) sa relevantnim međunarodnim institucijama kako bi ubrzao mehanizme upućivanja upozorenja poslovnom sektoru unutar zemlje. Time se minimizira vrijeme između detekcije egzogene prijetnje (nastale van domaće infrastrukture) i momenta kada domaće kompanije mogu sprovesti preventivne ili korektivne mjere. Na kraju, razvoj nacionalnog CERT-a mora uključivati sistem evaluacije sopstvenih performansi kroz testne incidente ili simulirane sajber krize. Takva praksa omogućava identifikaciju slabosti reakcionih protokola u kontrolisanom okruženju prije nego što stvarne situacije dovedu do velikih posljedica. Evaluacija rezultata simulacija pruža osnovu za stalnu adaptaciju procedura rada, čime se gradi dinamična otpornost sistema koja prati promjene u pejzažu sajber prijetnji. Bez implementacije ovakvog ciklusa unapređenja teško je očekivati dugoročnu efikasnost nacionalnog CERT-a čak i uz optimalnu početnu konfiguraciju njegovih kapaciteta.

2.4. Informacione prijetnje

Savremeni informacioni sistemi suočeni su sa rastućim brojem prijetnji koje ugrožavaju povjerljivost, integritet i dostupnost informacija. Digitalna transformacija, povećana povezanost sistema i široka upotreba interneta doprinijeli su proširenju površine napada, čineći informacione prijetnje jednim od ključnih rizika za organizacije i društvo u cjelini. Za razliku od tradicionalnih sigurnosnih izazova, savremene informacione prijetnje karakterišu dinamičnost, prilagodljivost i globalni domet.

Izvori informacionih prijetnji obuhvataju zlonamjerne aktere, unutrašnje prijetnje, kao i nenamjerne greške i tehničke propuste. Njihov uticaj prevazilazi tehničke aspekte i često rezultira značajnim poslovnim, pravnim i reputacijskim posljedicama. Zbog toga se informacione prijetnje ne mogu posmatrati isključivo kao tehnički problem, već kao strateški izazov koji zahtijeva sistematski i proaktivan pristup upravljanju sigurnošću.

2.4.1. Rani oblici sajber kriminala

Rani oblici sajber kriminala razvijali su se u periodu kada su računarske mreže bile u procesu komercijalne ekspanzije, a sigurnosni mehanizmi nisu bili dovoljno sofisticirani da prepoznaju neovlaštene aktivnosti u realnom vremenu. Ovi incidenti najčešće su uključivali jednostavne metode iskorištavanja ranjivosti, poput zloupotrebe otvorenih portova na mrežnim servisima ili upotrebe osnovnog socijalnog inženjeringa radi pribavljanja povjerljivih informacija. Tipični primjer predstavlja tzv. „phreaking”, praksa manipulacije telefonskih sistema kako bi se dobio besplatan pristup međunarodnim linijama. Phreakeri su koristili tonalne sekvence koje su imitirale signalne šifre telekom operatera, čime su zaobilazili sistem naplate poziva. Kako su se brzo uvodile mrežne komunikacione tehnologije, posebno TCP/IP protokol (Transmission Control Protocol / Internet Protocol), pojavili su se prvi poznati slučajevi zloupotrebe mrežnih ranjivosti kroz otvorene portove ili nezaštićene usluge. Napadi skeniranjem portova omogućavali su identifikovanje aktivnih servisa i slanje specijalno kreiranih paketa podataka koji bi izazvali neželjeno ponašanje aplikacija. U kontekstu ranih oblika kriminala, SQL (Structured Query Language) injekcije i „buffer overflow” tehnike bile su dominantne kod kompromitovanja serverskih aplikacija. Takvi napadi koristili su nedovoljno filtrirane korisničke ulaze u aplikacijama kako bi ubacili maliciozne instrukcije koje sistem interpretira kao validne komande. Prve varijante zlonamjernog softvera, virusi i crvi, imale su relativno jednostavnu strukturu, ali visoku sposobnost širenja. „Morris Worm”, pušten 1988. godine,

pokazao je koliko brzo jedan automatizovani program može paralizovati značajan dio tadašnje internetske infrastrukture (Goldsmith, 2022). Mehanizam širenja oslanjao se na iskorištavanje sigurnosnih propusta u Telnet i Sendmail servisima, kao i slabosti r-protokola koji je dozvoljavao neautentifikovan pristup između međusobno povezanih sistema. Socijalni inženjering bio je ključna komponenta mnogih ranih incidenata, naročito kod phishing kampanja koje su targetirale elektronsku poštu korisnika sa ciljem prikupljanja autentifikacionih podataka. Napadači bi kreirali poruke koje vizuelno oponašaju legitimne komunikacije banaka ili drugih institucija, vodeći žrtvu na lažne web stranice na kojima unosi svoje podatke. Ove metode ostaju relevantne i danas zbog njihovog oslanjanja na psihološke faktore umjesto složenog tehničkog znanja. DoS napadi javljaju se već sredinom devedesetih godina kao metoda preopterećenja serverskih resursa putem velikog broja zahtjeva generisanih u kratkom vremenskom intervalu. Ovakvi napadi bili su mogući zahvaljujući tome što administratorski alati za monitoring nisu imali mogućnost filtriranja neprirodnog saobraćaja ili automatskog ograničavanja pristupa iz sumnjivih izvora. Distribuirani oblici DoS (u daljem tekstu: DDoS) razvijeni krajem iste decenije koristili su tzv. „botnet" mreže hakovanih uređaja da orkestriraju napad iz više geografski udaljenih tačaka. Napadi zasnovani na krađi kolačića (cookie theft) postali su poznati sa ekspanzijom web aplikacija koje nisu primjenjivale sigurne metode skladištenja sesija. Nezaštićeni HTTP protokol (HyperText Transfer Protocol) dopuštao je presretanje kolačića kroz packet sniffing alate, pružajući napadaču mogućnost da se autentifikuje kao legitimni korisnik bez posjedovanja lozinke. Otvaranje bežičnih mreža bez enkripcije stvorilo je dodatni vektor ugrožavanja; tzv. „wardriving" podrazumijevao je fizičko pretraživanje područja u potrazi za nezaštićenim Wi-Fi mrežama koje napadač potom koristi za anonimno izvođenje ilegalnih radnji. Slabe konfiguracije WEP (Wired Equivalent Privacy) enkripcije mogle su biti probijene za nekoliko minuta uz tada dostupne alate. Manipulacija web zahtjevima kroz Cross-Site Request Forgery (u daljem tekstu: CSRF) bila je među sofisticiranijim tehnikama krajem devedesetih. Iskorištavanjem činjenice da web preglednik automatski šalje autentifikacione informacije serveru, napadač bi navodio korisnika da klikne na skriveni link koji izvršava neželjenu akciju pod njegovim identitetom. Rani primjeri hakovanja putem socijalnog inženjeringa često uključuju direktnu komunikaciju sa osobljem ciljane organizacije radi dobijanja pristupnih kodova ili informacija o internim procedurama. Ovakve metode pokazale su da tehnička zaštita može biti beskorisna ukoliko ljudski faktor nije obučen da prepozna pokušaje

manipulacije. Razvoj ovih tehnika bio je ograničen nizom faktora: manjkavost standardizovanih bezbjednosnih politika u korporativnim mrežama, nedostatak edukacije korisnika o digitalnoj higijeni i spor odgovor tehničkih timova na indikatore kompromitovanja sistema. Veza između ranih oblika sajber kriminala i savremenog pejzaža prijetnji leži u kontinuitetu konceptualnih modela, većina današnjih sofisticiranijih metoda ima svoje korijene upravo u osnovnim tehnikama iz ovog perioda (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Evolucija od phreakinga ka modernim napadima na VoIP (Voice over Internet Protocol) sisteme pokazuje adaptaciju istog principa zloupotrebe telekomunikacionog protokola; prelazak od jednostavnih virusa ka ransomwaru predstavlja produžetak ideje kontrole nad tuđim digitalnim resursom radi lične koristi.

2.4.2. Evolucija malicioznih softvera

Razvoj malicioznih softvera pratio je putanju sve veće sofisticiranosti, od relativno jednostavnih programa koji su se oslanjali na predvidljive vektore napada, do kompleksnih modularnih sistema sposobnih za višeslojno kompromitovanje digitalne infrastrukture. Rane varijante virusa i crva bile su ograničene u funkcionalnosti, ali su imale visoku sposobnost širenja zahvaljujući slaboj implementaciji osnovnih bezbjednosnih mjera i odsustvu alata za pravovremeno detektovanje anomalija. Kako se globalna mrežna povezanost širila, maliciozni kod počeo je da koristi ranjivosti u protokolima komunikacije i servisima koji nisu imali adekvatnu kontrolu pristupa. Ovakvi programi inicijalno su imali prvenstveno destruktivnu svrhu, brisanje datoteka ili ometanje rada sistema, dok je kasniji razvoj bio vođen motivima finansijske dobiti. Pomak ka profitno orijentisanom modelu malicioznog softvera može se posmatrati kroz pojavu trojanaca koji maskirani kao legitimne aplikacije otvaraju skriveni kanal pristupa napadaču. Trojanci su omogućavali daljinsko upravljanje kompromitovanim sistemom, prenos podataka i instaliranje dodatnog koda. Evolucija je dalje išla u smjeru integracije funkcionalnosti keylogger-a koji zapisuju svaki unos sa tastature i šalju zapise na udaljeni server. Kombinacija ovih tehnika značila je da jedan maliciozni paket može istovremeno pratiti aktivnost korisnika, eksfiltrirati povjerljive informacije i pripremiti infrastrukturu za sljedeće faze napada. Crvi nove generacije počeli su koristiti složenije algoritme replikacije kako bi izbjegli osnovne filtere mrežnog saobraćaja. Umjesto prostog širenja kroz e-mail priloge, usvajali su strategiju iskorištavanja „zero-day“ ranjivosti u popularnim aplikacijama. Napadi na ranjive verzije web servera dovodili su do

automatizovanog preuzimanja kontrole nad stotinama ili hiljadama sistema bez direktnog kontakta između napadača i žrtve. Kasniji modeli crva uključivali su mehanizme za automatska ažuriranja koda iz komandnog centra (Command & Control servera), čime se maliciozni softver dinamično prilagođavao novim okolnostima odbrane (Isaac, et al., 2024). Spyware kao zasebna kategorija usmjeren je na diskretno praćenje aktivnosti korisnika bez njihovog znanja. Početne verzije fokusirale su se na prikupljanje podataka o pretrazi interneta radi plasiranja ciljanih reklama, dok moderni spyware obuhvata sofisticirane funkcije poput snimanja ekrana, krađe lozinki i čitanja sadržaja zaštićenih komunikacija. Ovakav softver često koristi legitiman pristup sistemskim resursima da bi izbjegao detekciju, oslanjajući se na potpisivanje koda ili zloupotrebu certifikata radi stvaranja privida legitimnosti. Razvoj ransomware-a označio je jedan od najdramatičnijih pomaka u evoluciji malicioznih programa. Prve verzije bile su rudimentarne, enkripcija fajlova uz zahtjeve za uplatu otkupnine, dok današnji modeli koriste hibridne algoritme enkripcije kombinovanjem simetričnih i asimetričnih metoda kako bi otežali proces dešifrovanja bez ključa napadača (Tetteh, 2024). Istovremeno, ransomware kampanje povezuju se sa taktikama javnog sramoćenja žrtava (tzv. double extortion), gdje kompromitovane informacije nisu samo zaključane već se prijeti njihovim objavljivanjem ukoliko uplata ne bude izvršena. Malware namijenjen napadima na industrijske kontrolne sisteme predstavlja posebnu kategoriju koja ilustruje prelazak malicioznog koda iz domena informacionih tehnologija u okruženje operativne tehnologije. Napadački vektori uključuju manipulaciju firmware-a kontrolera ili iskorištavanje slabosti u sistemu za nadzor i prikupljanje podataka (Supervisory Control and Data Acquisition, u daljem tekstu: SCADA) (Kuipers & Fabro, 2006). U takvim scenarijima cilj nije nužno krađa podataka već izazivanje fizičke štete kroz promjenu parametara upravljačkih procesa. Botnet mreže kao agregat više zaraženih uređaja omogućile su realizaciju masovnih distribuiranih napada i pružile infrastrukturnu podršku drugim oblicima malware-a. Savremeni botnet-i mogu biti modularni: osnovna funkcija vrši DDoS napade dok dodatni moduli omogućavaju rudarenje kriptovaluta ili distribuciju phishing poruka prema unaprijed definisanim listama meta. Kombinacija malicioznog softvera sa tehnikama socijalnog inženjeringa dala je posebno potentne forme prijetnji jer spaja tehničku eksploataciju sa psihološkom manipulacijom korisnika (Shekh, 2024). Advanced Threat Protection (u daljem tekstu: ATP) sistemi slijede ovu logiku uvodeći dugačke kampanje infiltracije unutar ciljane organizacije uz minimalni otisak koji bi mogao izazvati alarm većine odbrambenih sistema. Današnji trend jasno

pokazuje da evolucija malicioznih softvera ide ka heterogenim arhitekturama koje obuhvataju više tipova funkcionalnosti unutar jednog paketa, automatizovan proces adaptacije koda te korištenje „mitigacionih“ tehnika protiv forenzičke analize. Integrisani malware sistemi mogu mijenjati svoj digitalni potpis, koristiti polimorfizam da otežaju statičku detekciju ili primjenjivati „sandbox evasion“ metode koje sprečavaju njihovo izvršavanje u kontrolisanom okruženju namjenjenom analizi. Ovaj proces transformacije malicioznog softvera nije linearan, povratak starijih tehnika javlja se kada one postanu opet efikasne zbog promjena u konfiguraciji sistemskih odbrana ili ljudskog faktora kod korisnika. Primjera radi, makro virusi za kancelarijske pakete ponovo bilježe rast nakon što je porasla upotreba dijeljenih cloud dokumenata bez adekvatnog skeniranja sadržaja prije učitavanja. Analiza pokazuje jasnu vezu između tehničkog razvoja infrastrukture i sposobnosti autora malicioznog softvera da iskoriste nove mogućnosti kompromitovanja resursa. Evolucija je vođena dvostrukim pritiskom: s jedne strane motivima ekonomskog profita kroz ilegalne aktivnosti poput krađe finansijskih podataka ili iznude putem enkripcije, s druge strane strateškim interesima određenih aktera spremnih da koriste digitalne metode za destabilizaciju protivničkih sistema. Kombinacija oba motivaciona faktora rezultira time što savremeni maliciozni softver posjeduje karakteristike koje prevazilaze granice tradicionalnog računarskog kriminala i prelaze u domenu sajber ratovanja.

2.4.3. Savremeni tipovi prijetnji

Savremeni napadi na informacione sisteme predstavljaju jednu od najznačajnijih globalnih sigurnosnih prijetnji. Organizacije širom svijeta sve su češće izložene različitim oblicima sajber napada, zbog čega ulažu značajne resurse i kontinuirane napore u zaštitu podataka, kao i u očuvanje integriteta i dostupnosti cjelokupne IT infrastrukture.

2.4.3.1. Phishing i socijalni inženjering

Phishing i socijalni inženjering predstavljaju dva međusobno povezana koncepta sajber prijetnji, zasnovana na manipulaciji ljudskog faktora kako bi se ostvario neovlašteni pristup informacijama, finansijskim sredstvima ili kritičnim resursima organizacije. Za razliku od većine tehničkih napada koji ciljaju ranjivosti softvera ili mrežne infrastrukture, ove metode eksploatišu slabosti u znanju, pažnji i heuristikama zaposlenih, oslanjajući se na psihološke mehanizme povjerenja i autoriteta (Kamis, 2020). Phishing kao tehnika kompromitovanja digitalnog identiteta tipično uključuje slanje poruka koje imitiraju komunikaciju legitimnih

entiteta, najčešće banaka, dobavljača ili internih službi organizacije. Poruke su konstruisane tako da izazovu osjećaj hitnosti – npr., upozorenje o isteku šifre ili sumnjivoj transakciji – čime se podstiče brz odgovor bez promišljanja. Krajnji korisnik preusmjerava se ka lažnoj web stranici koja vizuelno replicira originalnu, gdje unosi povjerljive podatke poput korisničkog imena, lozinke ili PIN koda. Napadač koristi dobijene informacije za direktan pristup sistemu ili izvođenje daljih koraka u kompromitovanju cilja. Metodologija phishing napada može biti prilagođena specifičnoj infrastrukturi MSP-a. Ciljana varijanta, tzv. spear phishing, usmjerena je na pojedince sa visokim ovlaštenjima unutar kompanije – najčešće članove uprave ili administratore IT sistema – čime se obezbjeđuje maksimalni efekat kompromitovanja u kraćem vremenskom okviru. Ove poruke često koriste informacije dobijene iz otvorenih izvora ili prethodnih incidenata curenja podataka kako bi povećale vjerodostojnost poruke i smanjile vjerovatnoću otkrivanja prevare. Socijalni inženjering obuhvata širu paletu tehnika koje mogu biti integrisane sa phishingom ili primjenjivane samostalno. Podrazumijeva manipulativne taktike poput pretvaranja da se radi o tehničkoj podršci kompanije (tech support scam), traženja privatnih informacija pod izgovorom verifikacije identiteta, fizičkog pristupa zaštićenim prostorijama kroz impersonaciju zaposlenog ili poslovnog partnera, pa sve do kompleksnih višefaznih scenarija poznatih kao „pretexting”. Pretexting se oslanja na kreiranje uvjerljivog narativa: napadač glumi relevantnu osobu koja ima opravdan razlog da traži određene informacije (npr., revizor koji navodno provjerava finansijske izvještaje). Mnogi ukazuju da socijalni inženjering prolazi kroz ciklus koji počinje fazom istraživanja mete, nastavlja se kreiranjem priče kojom se stiče povjerenje žrtve, zatim dolazi manipulacija koja omogućava izvršenje napada, da bi na kraju napadač nestao iz komunikacije nakon dostizanja cilja. Svaka od ovih faza ima svoje mikro-taktike, istraživanje uključuje prikupljanje javno dostupnih informacija sa društvenih mreža, dok faza kreiranja priče zavisi od sposobnosti imitacije komunikacionog stila prave osobe ili institucije. Društvene mreže predstavljaju kritičan kanal putem kojeg napadači mogu prikupljati podatke za pripremu personalizovanih phishing poruka. Javne objave zaposlenih o projektima na kojima rade, poslovnim sastancima ili lokacijama mogu nenamjerno otkriti unutrašnje procese kompanije. Ukazuje se na značaj pravilnog korištenja podešavanja privatnosti kao preventivne mjere protiv takvih formi eksploatacije informacija. Uticaj ovih prijetnji na MSP često je dublji nego kod velikih organizacija jer mali biznisi nerijetko nemaju formalizovane protokole provjere autentičnosti upita niti specijalizovane timove za detekciju anomalija.

2.4.3.2 Ransomware napadi

Ransomware napadi spadaju među najdestruktivnije i ekonomski najštetnije oblike savremenih sajber prijetnji, jer kombinuju blokiranje pristupa digitalnim resursima metodama enkripcije sa iznudom novčane otkupnine kao uslova za dešifrovanje podataka. Struktura ovakvih kampanja često uključuje višeslojnu strategiju kompromitovanja sistema. Inicijalna infekcija odvija se preko vektora pristupa kao što su phishing poruke, kompromitovani dodaci elektronske pošte ili iskorištavanje ranjivosti u ne update-anim serverima i VPN servisima. Statistički podaci pokazuju da phishing predstavlja najčešći ulazni kanal za ransomware napade, sa udjelom od 53% među analiziranim incidentima, nakon čega slijede ne update-ani serveri/ Virtual Private Network (u daljem tekstu: VPN) okruženja i krađa korisničkih lozinki. Ova distribucija jasno ukazuje na kombinaciju tehničkih propusta i slabosti ljudskog faktora u fazi inicijalnog pristupa. Primljeni payload često je dizajniran da izvrši enkripciju datoteka koristeći jake algoritme poput AES-a za simetričnu enkripciju sadržaja i RSA-a (Rivest–Shamir–Adleman) za enkripciju ključeva, čime se praktično onemogućava dešifrovanje bez pristupa privatnom ključu napadača. Novije varijante ransomware-a uvode dodatne mehanizme pritiska kroz taktiku tzv. „double extortion" – prije nego što se fajlovi zaključaju, njihovi sadržaji bivaju eksfiltrirani ka infrastrukturama napadača, a potom se žrtvama prijeti javnim objavljivanjem ukoliko odbiju plaćanje. Takva praksa stvara dvostruki rizik: gubitak dostupnosti podataka i narušavanje reputacije zbog potencijalnog odavanja povjerljivih informacija. Finansijski aspekt ovih napada ogleda se u prosječnim iznosima otkupnina koje MSP plaćaju; procjene govore o prosjeku od oko $16 000 u Sjedinjenim Državama tokom jednogodišnjeg perioda. Međutim, uprkos plaćanju, samo 50% organizacija uspije da povrati sve svoje podatke. Polovina preduzeća koja plati ucjenu, mora naknadno rekreirati sisteme od nule, dok se 27% suoči sa ponovnim napadima ili dodatnim zahtjevima za uplatu od istih aktera (Tetteh, 2024). Ovi podaci pokazuju da sama finansijska transakcija ne donosi garanciju oporavka niti prekida ugrožavanja. Metodologija širenja ransomware-a postala je sofisticirana kako bi minimizirala mogućnost otkrivanja. Nakon infekcije, maliciozni kod često onemogućava sigurnosne procese na sistemu – deaktivira antivirusne alate, briše shadow kopije datoteka kako bi spriječio interno vraćanje sistema i modifikuje konfiguracije firewall-a radi komunikacije sa komandnim centrima (Command & Control) bez ograničenja. Mnoge moderne kampanje oslanjaju se na „living off the land" tehnike korištenjem legitimnih administrativnih alata (npr. PowerShell) kako bi se izbjegla detekcija zasnovana na

heurističkim analizama. Za MSP problem je često vezan uz nedostatak segmentacije mreže i centralizovane kontrole pristupa. Kada ransomware kompromituje jedan uređaj, lateralno kretanje kroz internu mrežnu infrastrukturu omogućava brzo širenje do ključnih servera ili mrežnih lokacija gdje su pohranjeni kritični poslovni dokumenti. Napadi koji ciljaju ICS posebno su opasni jer mogu istovremeno izazvati digitalnu blokadu i fizičke posljedice – manipulacijom industrijskih procesa dovesti do prekida proizvodnje ili štete na opremi. Razlozi visoke stope ponovljenih napada leže u tome što mnoge organizacije, nakon inicijalnog incidenta, vraćaju operativnu funkcionalnost bez dublje analize vektora ugrožavanja. Ako inicijalni ulaz nije neutralisan – bilo kroz tehničku zakrpu ranjivosti ili promjenu kompromitovanih akreditiva – infrastruktura ostaje otvorena za sljedeće cikluse penetracije istog ili povezanog aktera. Nedostatak prijave incidenata dodatno otežava situaciju; oko 44% sajber krivičnih djela ostaje neprijavljeno nadležnim organima ili servis provajderima, čime se smanjuje mogućnost koordinisanog odgovora i razmjene obavještajnih informacija o aktivnim kampanjama. Mjere zaštite protiv ransomware-a zahtijevaju višesložni pristup koji obuhvata tehničke kontrole (redovna ažuriranja sistema i aplikacija, MFA), organizacione protokole (politike kontrole pristupa podacima prema načelu minimalnih privilegija) i edukaciju korisnika radi smanjenja uspješnosti phishing pokušaja. Simulacije phishing scenarija pokazale su da čak 85% korisnika u testiranom okruženju klikne na maliciozni link tokom prve faze evaluacije, pa veći dio firmi nakon takvih rezultata planira značajne promjene – uključujući nove tehnologije zaštite interne infrastrukture i povećanje obuka osoblja (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Napadi sve češće uključuju elemente tzv. Ransomware-as-a-Service (u daljem tekstu: RaaS) modela gdje grupe koje razvijaju maliciozni kod daju ga u zakup drugim kriminalnim akterima uz podjelu profita od otkupnina. Time se barijera tehničkog znanja potrebna za izvođenje kampanje znatno spušta – praktično bilo ko sa osnovnim poznavanjem digitalne komunikacije može sprovoditi ovakve napade koristeći unaprijed pripremljene pakete alata i infrastrukture Command & Control servera koje mu pruža RaaS dobavljač (Tetteh, 2024). Za MSP ovo znači da broj potencijalnih protivnika postaje mnogo veći nego što to sugeriše analiza samo visoko sofisticiranih grupa. Strategije oporavka moraju biti zasnovane na pouzdanim offline backup sistemima koji nisu trajno povezani na mrežu ili cloud immutable backup rješenjima, koja moraju imati verzionisanje kako bi omogućila vraćanje stanja prije kompromitovanja čak ako ransomware uspije doći do online kopija. Forenzička analiza poslije incidenta treba dokumentovati sve korake infekcije kako bi

plan mitigacije bio precizan, periodična testiranja procedura vraćanja sistema imaju ključnu ulogu u provjeri njihove operativne vrijednosti u realnom okruženju. Sumarno posmatrano, ransomware predstavlja prijetnju čiji efekti prelaze granice običnog gubitka podataka – oni uključuju dugotrajne prekide poslovanja, narušavanje odnosa sa klijentima zbog percepcije nedostatka bezbjednosti te potencijalno pravne posljedice zbog curenja povjerljivih informacija. MSP koja žele umanjiti rizik moraju razvijati strategiju koja povezuje prevenciju tehničkih ranjivosti sa stalnom edukacijom zaposlenih i jasno definisanim protokolima reakcije na incidente kako bi eventualni napad imao minimalan operativni uticaj na poslovanje.

2.4.3.3. Napadi na kritičnu infrastrukturu

Napadi na kritičnu infrastrukturu predstavljaju sve kompleksniji sigurnosni izazov u savremenom digitalnom okruženju, reflektujući duboku integraciju informacionih i operativnih tehnologija u kritične sektore društva. Kritična infrastruktura se u literaturi definiše kao skup fizičkih i sajber sistema čiji prekid može uzrokovati ozbiljne posljedice za javno zdravlje, sigurnost i ekonomske funkcije (Rinaldi, et al., 2001). U kontekstu napada, posebno je značajno razumijevanje dinamičnih prijetnji koje ne ciljaju samo velike državne ili korporativne sisteme, već sve učestalije i manje i srednje organizacije koje učestvuju u funkcionalnim lancima vrijednosti. Takvi napadi često koriste sofisticirane tehnike koje kombinuju napredne persistentne prijetnje (Advanced Persistent Threat - APT) i automatizovane hakerske alate. Ransomware, napadi na lanac snabdijevanja i kompromitacija industrijskih kontrolnih sistema ilustruju sveobuhvatnu prirodu prijetnji koje mogu paralizovati kritične funkcije. Posljedice ovih napada prevazilaze tehničke domene jer se ogleda i u narušenom povjerenju korisnika, prekidu usluga ključnih za funkcionisanje društvenih sistema i povećanom ekonomskom riziku.

3. Defense in Depth strategija informacione sigurnosti

Strategija Defense in Depth predstavlja koncept slojevite zaštite informacionih sistema i podataka kroz niz međusobno povezanih mehanizama koji zajedno pružaju viši nivo bezbjednosti od bilo kojeg pojedinačnog kontrolnog elementa (Rahman, et al., 2019). Ovaj pristup podrazumijeva postavljanje više linija odbrane, koje se mogu razlikovati po funkciji, opsegu i tehnološkoj osnovi. Klasični elementi uključuju perimetarsku zaštitu poput firewall-a i detekcije - prevencije upada, unutrašnje sisteme kontrole pristupa i segmentaciju mreže, autentifikaciju zasnovanu na višefaktorskim metodama, kao i stalnu edukaciju korisnika radi smanjenja vjerovatnoće uspješnih socijalno-inženjerskih napada (Bada i Nurse, 2019). Iz perspektive savremenih sajber prijetnji, perimetarska zaštita nije dovoljna jer sofisticirani napadi često zaobilaze spoljne barijere preko kompromitovanih uređaja ili cloud aplikacija. Zbog toga se u Defense in Depth okviru kombinuju mehanizmi poput kontinuiranog nadzora sistema (monitoringa), analize događaja u stvarnom vremenu, kao i politike upravljanja identitetima, gdje svaki entitet u sistemu prolazi verifikaciju bez obzira na prethodni nivo povjerenja (Tetteh, 2024). Model nultog povjerenja (Zero Trust) uklapa se prirodno u ovaj koncept, jer insistira na stalnoj validaciji korisnika i uređaja pri svakoj interakciji sa resursima organizacije. Ovakav slojevit pristup teško je efikasno primijeniti bez jasne strategije koja povezuje tehničke procese s organizacionim političkim odlukama. Pitanje liderstva i izgradnje kulture bezbjednosti unutar zaposlenih postaje centralno, posebno kod MSP, gdje raspoloživi resursi za sajber sigurnost mogu biti ograničeni (Ejjami, 2024). Edukacija zaposlenih ne može biti jednokratan proces; ona zahtijeva kontinuiranu nadogradnju znanja kroz simulacije napada, osvrt na aktuelne prijetnje i ažuriranje standarda ponašanja u digitalnom okruženju. Različiti slojevi odbrane treba da adresiraju različite potencijalne vektore prijetnji. Na primjer:

- Perimetarska zaštita sprečava neautorizovano pristupanje izvan mreže;
- Unutrašnja segmentacija mreže umanjuje širenje napada unutar sistema;
- MFA povećava otpornost na ugrožavanje naloga putem krađe akreditiva;
- Edukacija korisnika smanjuje uspješnost phishing kampanja;
- Redundantnost i planovi oporavka od katastrofe obezbjeđuju kontinuitet rada čak i tokom incidenata;
- Bezbjednost aplikacija uvodi kontrole tokom cijelog životnog ciklusa softvera.

Kod MSP-a navedeni pristupi zahtijevaju balans između troškova uvođenja dodatnih slojeva odbrane i njihove operativne održivosti (Enitan, 2025). Statističke analize efekata investiranja u IT infrastrukturu pokazuju da kombinacija tehničkih mjera sa redovnim treninzima zaposlenih pozitivno korelira sa povećanjem spremnosti organizacije da odgovori na sajber incidente. To implicira da izolovane tehničke investicije bez ulaganja u ljudske kapacitete ne postižu željeni efekat otpornosti na prijetnje. Sajber bezbjednost se posmatra kao dio ukupnog sistema upravljanja informacijama gdje je cilj sprečavanje štete ili eksploatacije digitalnih resursa (Wallang, et al., 2022). Prema globalnim indeksima, zemlje koje postižu najviše rezultate implementiraju višeslojne strategije koje kombinuju nacionalne propise, industrijske standarde i tehničke provjere kompatibilnosti sa novim tehnologijama. Iako MSP nemaju iste resurse kao velike korporacije ili nacionalni centri sajber bezbjednosti, ona mogu adaptirati principe Defense in Depth koristeći skalabilna rješenja prilagođena njihovom obimu poslovanja (Wang, 2023). Također treba istaći da spoljne prijetnje poput phishinga ili ransomware-a često imaju polaznu tačku preko ranjivosti koje su nastale zbog nepatch-ovanog softvera ili slabih politika upravljanja identitetima. U tom kontekstu slojevito osiguranje znači da čak i ako jedan sloj bude probijen – recimo kroz uspješan phishing – sljedeći sloj (npr. segmentirana mreža sa ograničenjem privilegija) može spriječiti širenje kompromitacije. Time se minimizira potencijalna šteta dok se incident istražuje i otklanja. Kritički posmatrano, obrambeni koncepti ponekad trpe zbog rigidne implementacije koja ne prati dinamiku stvarnih operativnih potreba MSP-a. Preagresivne kontrole mogu omesti tok posla ili demotivisati korisnike da ih dosljedno primjenjuju. Iz tog razloga važno je da integrisani okvir zaštite bude fleksibilan – odnosno da se pojedini slojevi mogu prilagoditi promjenama rizika, regulative ili poslovnih procesa bez gubitka koherentnosti čitavog sistema odbrane (Levi & Williams, 2013). Određena nesigurnost postoji oko optimalnog broja slojeva odbrane, jer previše kontrola može stvoriti kompleksnost koju napadači potom iskorištavaju kroz slabo održavane komponente sistema. Sa druge strane, premali broj slojeva ostavlja otvorene puteve preko kojih napadi lako zaobilaze postojeće barijere. Zbog toga praksa preporučuje fokusiranje na međusobno komplementarne mehanizme koji adresiraju različite faze životnog ciklusa napada – od prevencije do detekcije i odgovora – uz što bolju koordinaciju između tehničkog osoblja sigurnosti i ostalih zaposlenih koji koriste informacione sisteme kompanije (Bada i Nurse, 2019).

3.1. Definicija i značaj Defense in Depth strategije

Strategija Defense in Depth se konceptualno definiše kao sveobuhvatni pristup zaštiti informacionih sistema i podataka, koji koristi višestruke slojeve odbrane raspoređene kroz različite tehničke, proceduralne i organizacione komponente (Amro & Gkioulos, 2023). Ideja je da se, umjesto oslanjanja na jedan jedini mehanizam zaštite, implementira niz međusobno povezanih kontrola koje se nadopunjuju. (Kamis & Stamenković, 2023) Na taj način čak i ako jedan sloj bude kompromitovan, preostali slojevi nastavljaju da pružaju zaštitu. Premisa ovog pristupa leži u smanjenju vjerovatnoće uspješne eksploatacije ranjivosti i ograničavanju obima štete ukoliko do incidenta ipak dođe (Rahman, et al., 2019). Ovaj koncept se ne odnosi isključivo na tehničke mjere poput firewall-a ili sistema za detekciju upada, već kombinuje i elemente upravljanja korisnicima, edukacije zaposlenih i procesa oporavka nakon incidenata. Perimetarska zaštita je obično osnovni sloj koji kontroliše saobraćaj između internog sistema i spoljne mreže, dok unutrašnja segmentacija mreže usporava ili sprečava širenje napada unutar organizacije (Prasad & Rohokale, 2019). Autentifikacija korisnika može uključivati više faktora potvrde identiteta (lozinka, token, biometrijski podaci) kako bi se minimizirala mogućnost neovlaštenog pristupa čak i u slučaju kompromitovanih akreditiva. Edukacija zaposlenih ima poseban značaj, jer ljudski faktor često predstavlja najslabiju kariku – mnogi napadi počinju preko phishing poruka ili socijalnog inženjeringa. Značaj Defense in Depth strategije posebno dolazi do izražaja kod organizacija koje obrađuju osjetljive podatke kao što su finansijski zapisi ili medicinski dosijei. Krađa takvih informacija ima direktne implikacije po reputaciju, pravnu odgovornost i kontinuitet poslovanja (Wallan, et al., 2022). U praksi se slojevita odbrana pokazuje kao efikasnija od monolitnih rješenja iz razloga što omogućava diferencijaciju funkcija – spoljne barijere, kao recimo firewall fokusiraju se na filtriranje nelegitimnog saobraćaja, unutrašnje kontrole osiguravaju validaciju korisničkih zahtjeva, a dodatne procedure verifikacije pružaju sekundarnu provjeru legitimnosti aktivnosti. Razvoj Defense in Depth arhitekture polazi od analize prijetnji koje mogu ugroziti ključne resurse organizacije – softver, hardverske komponente, povjerljive informacije. Tokom dizajniranja određuju se slojevi prema ranjivostima identifikovanim u sistemu i budžetskim ograničenjima (Rahman, et al., 2019). Pravilan raspored odbrambenih komponenti smanjuje mogućnost postojanja „skrivenih ulaza“ u sistem koji često nastanu iz zaboravljenih ili neadekvatno konfigurisanih elementa infrastrukture. Važan aspekt definicije ove strategije jeste njena

sposobnost da integriše tehničke kapacitete sa procesima rada i operativnim politikama – time stvara dinamičan okvir za odbranu koji je prilagođen realnim potrebama organizacije. Upravljački dio uključuje jasnu podjelu odgovornosti za održavanje svakog sloja odbrane i periodičnu provjeru njegove efikasnosti kroz simulirane incidente. Ovakav integrisani pristup omogućava sinergiju između preventivnih mjera, detekcije incidenata i odgovora na njih. Značaj primjene ovog modela potvrđuju različiti sektori, na primjer energetski pogoni koriste Defense in Depth kako bi spriječili i mitigovali posljedice nesreća putem kombinacije fizičkih barijera, sigurnosnih protokola rada i redovnog testiranja opreme (n.a., 2009); dok IT sektor implementira višeslojne zaštitne sisteme nad serverima, mrežama i korisničkim aplikacijama radi prevencije prodora malicioznih kodova ili krađe akreditiva (Boggs et al., 2014). Sama definicija pojma dopušta određenu fleksibilnost: prema NIST-u ona obuhvata koordinisano djelovanje ljudi, tehnologije i operativnih sredstava kako bi se stvorile varijabilne prepreke kroz različite dimenzije organizacije (Amro & Gkioulos, 2023). Takva definicija vraća fokus na potrebu balansiranja među slojevima – ni jedan sloj ne smije biti toliko slab da postane očigledna tačka ulaza za napadača. Pri posmatranju značaja ove strategije valja uzeti u obzir da ona podržava filozofiju „odbrane kroz dubinu" poznatu iz nuklearne regulative gdje višestruke barijere štite javnost od potencijalnih posljedica nesreća. Iako kontekst informacione sigurnosti ima drugačiji skup prijetnji u odnosu na fizičku infrastrukturu elektrana, načelo ostaje isto, redundantne kontrole sprečavaju lančano otkazivanje cijelog sistema. Povezanost sa programskom komponentom također nije zanemarljiva – sigurnost aplikacija traži testiranje koda tokom čitavog životnog ciklusa i integrisanje automatizovanih alata za otkrivanje ranjivosti. Postoji argument da višeslojna arhitektura može biti kompleksnija za administriranje nego jednostavna rješenja; međutim dobro struktuirana Defense in Depth strategija zapravo pojednostavljuje reakciju tokom incidenta, jer unaprijed definisani slojevi nude jasna mjesta kontrole događaja. Time se smanjuje prostor za improvizaciju u kriznim situacijama što povećava ukupni nivo pouzdanosti sistema. Iz perspektive menadžmenta rizika ova strategija nudi ravnotežu između probabilističkog pristupa (modeli vjerovatnoće nastanka incidenata) i determinističkog pristupa (konkretne tehničke mjere prevencije) (n.a., 2009), dajući menadžerima jasniji okvir unutar kojeg mogu racionalno distribuirati resurse bez narušavanja operativnog toka poslovanja.

3.1.1. Istorijski razvoj slojevite odbrane

Koncept slojevite odbrane, koji se danas prepoznaje kao strategija Defense in Depth, ima dugu istoriju koja prevazilazi granice isključivo digitalnog konteksta. Njegovi korijeni potiču iz vojnih doktrina gdje je ideja bila da se neprijatelj iscrpi prolaskom kroz više sukcesivnih linija odbrane, sve kako bi se povećala vjerovatnoća zaustavljanja napada kroz kombinaciju fizičkih barijera i taktičkih rasporeda (n.a., 2009). Sa razvojem informacionih sistema ovaj pristup dobija prenesen značaj u sajber domenu – logika višestrukih prepreka integriše se u arhitekture zaštite podataka i mrežnih resursa. Rani oblici digitalne slojevite odbrane pojavili su se u periodu kada su organizacije započele sa primjenom firewall-a i osnovnih kontrola pristupa na mrežnim gateway uređajima. Kako su mreže postajale kompleksnije tokom 80-ih i 90-ih godina, pojava internet okruženja i većeg nivoa međusobne povezanosti sistema otvorila je vrata sofisticiranijim napadima koji su mogli zaobići osnovne perimetarske kontrole. Upravo ovo iskustvo dovelo je do potrebe implementacije unutrašnjih slojeva zaštite – segmentacija mreže unutar organizacije postala je standardna praksa kako bi se spriječio lateralni pokret napadača (Kuipers & Fabro, 2006). U isto vrijeme, razvoj antivirusnih rješenja pokazuje ograničenja jednolinijske zaštite, pa istraživanja demonstriraju poboljšanja kada se kombinuje rad više različitih antivirus „engine“, što predstavlja analogiju višeslojnom pristupu u segmentu anti-malware zaštite (Boggs, et al., 2014). Sa širenjem interneta i prelaskom poslovanja na web-pristup, slojevita odbrana dobija dodatne dimenzije kroz autentifikaciju korisnika i upravljanje identitetima. MFA javlja se kao direktan odgovor na krađu lozinki, dok centralizovano upravljanje privilegijama minimizira šanse da kompromitovani nalog omogući potpuni pristup sistemu (Rahman, et al., 2019). Tehnologije poput PKI infrastrukture (Public Key Infrastructure - infrastruktura javnog ključa) također ulaze u arsenal kao dodatni sloj verifikacije autentičnosti entiteta u komunikaciji. Razvoj ovog koncepta nije vođen isključivo tehničkim imperativima već i regulatornim zahtjevima. Na primjer, sektori sa visokim rizikom poput energetike preuzeli su filozofiju višestrukih barijera iz nuklearne regulative za implementaciju u IT bezbjednosne politike (n.a., 2009). To znači da model Defense in Depth nije samo ad-hoc reakcija na prijetnje, već postaje ugrađen u standarde ponašanja industrije kroz gotovo obaveznu upotrebu redundantnih kontrola. Početkom XXI vijeka značajan uticaj dolazi iz nacionalnih i međunarodnih normativnih tijela poput NIST-a koji promovišu „inherentno” sigurnu platformsku arhitekturu zasnovanu na više slojeva tehničkih i

administrativnih mjera (Bartock, et al., 2021). Ova institucionalizacija koncepta skreće fokus sa pukog dodavanja novih tehnologija ka integraciji različitih komponenata – ljudi, procesa i tehničkih resursa – u koherentan sistem odbrane. Time je uveden standardizovan pristup gdje evaluacija performansi svakog sloja prati stalna testiranja (proof-of-concept), simulacije i formalnu procjenu rizika. U posljednjim decenijama posebno je vidljiv pomak ka uključivanju ljudskog faktora kao ključnog sloja odbrane. Edukacija zaposlenih prelazi iz inicijalnog treninga ka kontinuiranim programima za podizanje svijesti o sajber prijetnjama (Ejjami, 2024). Studije su pokazale da socijalno-inženjerski napadi mogu proći kroz najjače tehničke barijere ukoliko korisnik pogrešno reaguje tokom interakcije s phishing sadržajem ili malicioznim linkovima (Tetteh, 2024). Paralelno sa tim raste značaj monitoringa sistema u realnom vremenu. Uvođenje IDS/IPS rješenja dopunjuje tradicionalne slojeve zaštite automatskim detekcijama anomalija koje mogu signalizirati početak incidenta. Ovi sistemi se kasnije nadograđuju SIEM platformama koje omogućavaju korelaciju događaja preko više izvora kako bi se brže prepoznale koordinisane aktivnosti protiv infrastrukture (Kuipers & Fabro, 2006). Posmatrano iz perspektive MSP-a, istorijski razvoj pokazuje pomjeranje od minimalne zaštitne konfiguracije – često samo antivirus + osnovni firewall – ka mnogo kompleksnijim sistemima koji uključuju segmentaciju interne mreže, striktnu kontrolu privilegija, periodična ažuriranja softvera te planove oporavka nakon incidenta (Rahman, et al., 2019). Taj razvoj ipak nailazi na balanse između troškova implementacije dodatnih slojeva i njihove operativne održivosti. Može se reći da aktuelni model stoji na nasljeđu fizičkih strategija višestruke odbrane, ranih digitalnih eksperimenata s perimetarskim alatima te formalizacije kroz međunarodne standarde. Evolucija ovog pristupa pokazuje da stagnacija vodi ka zastarjelim metodama izloženim novim oblicima napada, zbog toga moderni okvir slojevite zaštite ne ostaje fiksiran već se adaptira prema detektovanim scenarijima rizika koristeći probabilističku analizu potencijalnih neočekivanih situacija udruženu s determinističkim mjerama prevencije (n.a., 2009).

3.1.2. Razlike između Defense in Depth i drugih pristupa

Strategija Defense in Depth se suštinski razlikuje od tradicionalnih pristupa sigurnosti koji se oslanjaju na pojedinačne tačke zaštite, jer uvodi višeslojnu arhitekturu gdje svaki sloj ima sopstveni skup kontrola i mehanizama reagovanja. U monolitnim modelima bezbjednosti fokus je najčešće na perimetarskoj barijeri – npr. mrežnom firewall ili IDS/IPS uređaju – koji

filtrira ulazno-izlazni saobraćaj i pokušava da prepozna upade. Problem takvih pristupa je očigledan čim napadač uspije da probije spoljnu liniju odbrane: svi unutrašnji resursi postaju ranjivi zbog odsustva dodatnih kontrolnih tačaka (Jander, et al., 2019). U kontrastu, Defense in Depth ne tretira bezbjednost kao binarnu funkciju „dozvoljeno-zabranjeno“ već kao kaskadni sistem barijera koje produžavaju vrijeme i povećavaju složenost napada, dajući operativnim timovima veće šanse za detekciju i odgovor. Druga ključna razlika odnosi se na integrisanost i komplementarnost mjera. Klasični pristupi često funkcionišu fragmentisano, sa malo međusobne komunikacije između mrežnog tima, tima za aplikacionu sigurnost i osoblja zaduženog za korisničke privilegije. Nasuprot tome, u Defense in Depth strategiji tehničke komponente (firewall-i, segmentacija mreže, enkripcija komunikacija) usko su povezane sa proceduralnim i administrativnim mjerama (upravljanje identitetom, dozvolama i politikama pristupa) (Chapple & Seidl, 2021). Na primjer, čak i ako koristimo snažnu enkripciju podataka u tranzitu uz TLS, dodatni slojevi poput kontrole lozinki ili MFA sprečavaju zloupotrebu legitimnog kanala od strane neovlaštenog subjekta. U poređenju sa Zero Trust modelom, koji također insistira na provjeri svakog zahtjeva nezavisno od lokacije korisnika ili uređaja, Defense in Depth podržava sličnu filozofiju stalne provjere ali ostavlja prostor za kombinovanje kontekstualnih odluka. Zero Trust se često zasniva na ideji eliminacije implicitnog povjerenja kroz centralizovane politike verifikacije svih konekcija; Defense in Depth može uključiti te principe ali zadržati elemente tradicionalne segmentacije mreže ili fizičkih barijera tamo gdje to ima smisla iz perspektive performansi ili zakonskih obaveza (Amro & Gkioulos, 2023). Dakle, dok Zero Trust vidi granice kao logičke cjeline koje se neprekidno provjeravaju, slojevita odbrana ih može implementirati i fizički i logički. Bitno je primjetiti da tradicionalna perimetarska sigurnost obično ne predviđa slojeve edukacije korisnika ili simulirane testove napada kao dio standardne prakse. U Defense in Depth oni predstavljaju ravnopravne komponente sistema jer se priznaje da socijalno-inženjerske metode mogu probiti tehničke zaštitne mehanizme (Almoaigel & Abuabid, 2023). Redovno sprovođenje phishing simulacija i treninga pomaže zaposlenima da razviju refleks prepoznavanja malicioznih pokušaja kontaktiranja što je u klasičnim arhitekturama izolovani zadatak službi bezbjednosti bez šire institucionalne integracije. Još jedna distinktivna odlika je primjena višestrukih linija kontrole unutar samih aplikacija. Dok jednostavniji modeli mogu osloniti sigurnost aplikacija isključivo na mrežnu segmentaciju ili validaciju ulaznih parametara u kodu, slojevita arhitektura dodaje interne sisteme nadgledanja performansi aplikacija i

otkrivanja anomalija ponašanja. U tom smislu koristan je princip agregacije pokrivenosti iz različitih proizvoda bezbjednosti kako bi se kvantifikovalo povećanje ukupne stope detekcije (Boggs. et al., 2014). Ovakva metoda evaluacije nije tipična za linearne modele zaštite gdje svaka komponenta radi nezavisno, a uspjeh cjelokupnog sistema teško se mjeri objektivno. Defense in Depth također podrazumijeva sofisticiraniji pristup menadžmentu rizika nego tradicionalni modeli. Naime, koriste se referentni okviri poput MITRE ATT&CK (MITRE Adversarial Tactics, Techniques, and Common Knowledge) za mapiranje prepoznatih vektora napada direktno na odgovarajuće kontrolne mjere. Time se dobija mogućnost preciznog praćenja implementiranih zaštita od trenutka procjene rizika do evaluacije stvarnog učinka što omogućava dinamičko prilagođavanje slojeva relevantnim prijetnjama. S druge strane tradicionalna arhitektura često reaguje reaktivno – tek nakon incidenata – umjesto da koristi predvidljive modele zasnovane na naprednoj analitici. Vrijedno je pomenuti i razlike u odnosu na standarde certifikacije i audita. Monolitni sistemi sigurnosti uglavnom prolaze periodične statičke provjere koje potvrđuju da konfiguracija odgovara unaprijed definisanom modelu. Slojevita strategija preferira kontinuiranu verifikaciju kroz penetration testing, fuzz testove ili pasivna mjerenja čime proaktivno otkriva ranjivosti prije nego što budu iskorištene od napadača (Amro i Gkioulos, 2023). Ovakav ciklus unapređenja kroz stalnu povratnu informaciju nije prioritet u jednostavnim modelima kojih cilj može biti samo formalna usklađenost sa minimumom propisa. Poseban aspekt koji razlikuje Defense in Depth odnosi se na skalabilnost zaštitnih mehanizama prema vrijednosti resursa koji se štite. Kod skupljih tehničkih rješenja koja imaju mali marginalni doprinos ukupnoj stopi detekcije preporučuje se njihovo usmjeravanje samo ka najvrjednijim segmentima infrastrukture kako bi investicija imala opravdan efekat (Boggs et al, 2014). Takva granularnost raspodjele resursa gotovo da ne postoji u klasičnim jednolinijskim arhitekturama gdje ista vrsta zaštite obuhvata sve sisteme podjednako. Na praktičnom nivou ovo znači da organizacija koja primjenjuje Defense in Depth gradi sigurnosni ekosistem koji uključuje perimetarsku kontrolu (npr. firewall), unutrašnje mikrosegmentirane zone sa strogim ACL pravilima (Amro i Gkioulos, 2023), dosljednu autentifikaciju i autorizaciju na aplikativnom nivou, kontinuirani nadzor događaja pomoću SIEM-a, redovno testiranje spremnosti osoblja te planove oporavka (backup i DR planovi) uz redundantne resurse za kritične funkcije. Takva širina komponenti nudi slojevitu otpornost koju drugi pristupi rijetko dostižu zbog inherentne redukcije fokusa na pojedinačne oblasti sigurnosti. Može se zaključiti da razlike nisu samo kvantitativne već prije svega

kvalitativne: umreženost mjera, fleksibilnost adaptacije novim prijetnjama i povezanost tehničkog segmenta sa ljudskim faktorom čine suštinu razdvajanja između ovog koncepta i drugih okvira bezbjednosne zaštite informacionih sistema. Upravo zbog ovih karakteristika Defense in Depth se sve češće vidi kao standard prakse tamo gdje su posljedice potencijalnog proboja visoke kako sa finansijske tako i sa regulatorne strane.

3.1.3. Prednosti i ograničenja Defense in Depth strategije

Prednosti strategije Defense in Depth proizilaze iz njene osnovne filozofije višestrukih barijera koje, pravilno integrisane, stvaraju otporniji sigurnosni okvir od bilo kojeg pojedinačnog kontrolnog mehanizma. Jedna od najvažnijih prednosti leži u činjenici da proboj jednog sloja ne mora automatski značiti potpuni gubitak zaštite, dok drugi slojevi preuzimaju funkciju ograničavanja štete i vremena potrebnog napadaču da ostvari cilj. Time se povećava vjerovatnoća otkrivanja incidenta prije nego što prouzrokuje trajne posljedice. Na operativnom nivou, ovakav pristup omogućava balansiranje tehničkih mjera (firewall, IDS/IPS sistemi, enkripcija podataka u tranzitu i mirovanju) sa proceduralnim i organizacionim politikama (upravljanje identitetima, kontrola pristupa, edukacija zaposlenih), čime se postiže komplementarnost mjera unutar cjelokupne arhitekture zaštite (Ejjami, 2024). Integracija različitih tipova zaštitnih mehanizama ima još jednu funkcionalnu korist: ona umanjuje zavisnost od performansi pojedinačne tehnologije i smanjuje rizik od tzv. „single point of failure". Ako firewall zakaže zbog greške konfiguracije ili exploita ranjivosti, unutrašnja segmentacija mreže i MFA mogu zaustaviti dalji prodor. Perimetarska zaštita filtrira spoljni saobraćaj dok nadzor aktivnosti korisnika i aplikacija u realnom vremenu pruža detekciju anomalija koje mogu signalizovati napad iznutra. Slojevitost ovog modela daje mogućnost granularne reakcije – incident može biti izolovan i tretiran unutar jednog segmenta sistema bez potrebe za gašenjem cjelokupnog poslovanja. Posebnu vrijednost strategiji daje uključivanje ljudskog faktora kao sloja odbrane. Kontinuirana edukacija zaposlenih o phishing-u, socijalnom inženjeringu i novim oblicima sajber prijetnji može drastično smanjiti uspješnost napada koji propuštaju tehničke kontrole. Studije pokazuju da poznavanje taktika napada smanjuje vjerovatnoću da će zaposleni nesvjesno kliknuti na maliciozni link ili unijeti podatke na kompromitovanu stranicu. Ova komponenta je posebno korisna za MSP koja nemaju resurse za sofisticirane sisteme detekcije, jer ljudska svijest postaje dodatna barijera. Još jedna prednost ogleda se u fleksibilnosti implementacije. Defense in Depth ne nameće

univerzalno rješenje već omogućava prilagođavanje broja i vrste slojeva zavisno od industrije, veličine organizacije i skupova podataka koji se štite. Organizacije sa visokim regulatornim zahtjevima mogu dodati više slojeva verifikacije (biometrijski sistemi, hardverska enkripcija podataka putem namjenskih modula) (Bartock, et al., 2021), dok manje firme biraju optimalan balans između troškova i nivoa zaštite. Međutim, primjena ove strategije nosi i ograničenja. Kompleksnost arhitekture može uzrokovati poteškoće u administraciji sistema. Višeslojna konfiguracija zahtijeva stalno praćenje kompatibilnosti među različitim sistemima zaštite kako bi se spriječilo preklapanje funkcionalnosti ili konflikt pravila koji može blokirati legitimne procese. Troškovi implementacije su često veći u odnosu na monolitne sisteme – ne samo zbog nabavke više različitih tehnologija već i zbog potrebe za stručnjacima koji će ih održavati. Za MSP to može predstavljati finansijski teret ako nemaju jasno postavljen prioritet zaštitnih ciljeva. Postoji rizik da višestruke kontrole smanje operativnu efikasnost ukoliko nisu usklađene sa tokovima rada. Preagresivne politike pristupa mogu usporiti izvršenje zadataka ili frustrirati zaposlenike do te mjere da pokušavaju zaobići procedure radi bržeg rada. To paradoksalno stvara nove ranjivosti. Pored toga, potrebno je pažljivo razmatrati zavisnosti među slojevima, jer nova konfiguracija može nenamjerno stvoriti međusobnu zavisnost koja povećava vjerovatnoću kaskadnog otkazivanja sistema. Tehnička ograničenja obuhvataju izazove integracije starijih sistema sa savremenim sigurnosnim tehnologijama. Legacy aplikacije često ne podržavaju modernu enkripciju ili metode autentifikacije pa njihovo uključivanje u višeslojnu arhitekturu zahtijeva dodatne prilagodbe. U nekim slučajevima to znači razvoj posebnih modula ili segmentaciju tih sistema radi izolacije potencijalnog izvora kompromitacije. Za MSP postoji specifično ograničenje u pogledu svijesti o strategiji među menadžmentom. Istraživanja pokazuju da mnoga mala preduzeća prioritet stavljaju na produktivnost u odnosu na sigurnost, sve dok incident ne otkrije ranjivosti u postojećem okruženju. Ovakav pristup reaktivnog investiranja dovodi do situacija gdje je Defense in Depth implementiran tek djelimično, bez punog efekta koordinisanog višeslojnog djelovanja. Pitanje skalabilnosti također može biti izazov, jer kako organizacija raste, postojeći slojevi moraju se reevaluirati radi proširenja kapaciteta ili dodavanja novih mehanizama zaštite koji odgovaraju aktuelnoj kompleksnosti sistema. Ako se ta nadogradnja ne sprovede pravovremeno, sistem koji je nekada bio adekvatan postaje nedovoljan pred novim setom prijetnji. Uprkos navedenim ograničenjima, teoretski okvir ove strategije pokazuje da njene prednosti nadmašuju nedostatke kada se implementacija vrši uz jasno definisan plan upravljanja

resursima i rizicima. Kombinovanje perimetarske i unutrašnje zaštite sa dosljednim procesima autentifikacije i autorizacije, dobro osmišljenom edukacijom korisnika, implementacijom redundancije te planovima oporavka od katastrofe nudi integrisani sistem sposoban da amortizuje različite tipove sajber prijetnji. Evaluacija efikasnosti svakog nivoa kroz simulirane incidente ostaje ključna metodologija za održavanje koherentnosti svih slojeva u vremenu.

3.2. Slojevi Defense in Depth strategije

Defense in Depth predstavlja sveobuhvatnu strategiju informacione bezbjednosti koja se temelji na primjeni više međusobno nezavisnih i komplementarnih kontrola kroz različite arhitektonske slojeve, s ciljem smanjenja mogućnosti uspješnog napada i ublažavanja njegovih posljedica (NIST, n.d.). Na perimetarskom nivou, prva linija odbrane uključuje firewall-e, IDS/IPS sisteme i segmentaciju mreže, što omogućava filtriranje i kontrolu saobraćaja na samom ulazu u mrežu (Maulding, 2026).

Sljedeći nivoi obuhvataju unutrašnju zaštitu, koja uključuje implementaciju kontrola pristupa i provođenje sigurnosnih politika unutar mreže da se ograniči lateralno kretanje prijetnji. Ključni aspekt ove razine je uspostava jasnih pravila pristupa i nadzor njihovog sprovođenja (Johnson, 2025).

Autentifikacija i autorizacija korisnika postiže se primjenom MFA i upravljanja privilegijama, čime se značajno smanjuje rizik od neovlaštenog pristupa čak i u slučaju kompromitacije lozinki (Johnson, 2025). Korisnička edukacija i svijest predstavljaju administrativne kontrole koje doprinose smanjenju ljudskih grešaka i unapređenju sigurnosne kulture kroz programe obuke zaposlenih (Maulding, 2026).

Slojevi redundantnosti i oporavka od katastrofe obuhvataju strategije backup-a, planove kontinuiteta poslovanja i redovno testiranje oporavka sistema, što omogućava organizacijama da brzo obnove funkcionalnost nakon incidenta i minimiziraju gubitke. Nadzor i nadgledanje realizuju se pomoću SIEM sistema, real-time monitoring-a i analitike sigurnosnih događaja, što podržava pravovremeno otkrivanje i odgovor na anomalije (Maulding, 2026).

Na kraju, sigurnost aplikacija uključuje primjenu principa sigurnog kodiranja i redovno testiranje ranjivosti, osiguravajući da softverski proizvodi budu otporni na poznate i nove prijetnje (NIST, n.d.). Ovakav višeslojni pristup ne samo da povećava otpornost organizacije

na sofisticirane napade, već i omogućava bolje upravljanje rizicima kroz kontinuirano unapređenje sigurnosnih mjera (Johnson, 2025).

3.2.1. Perimetarska zaštita

Perimetarska zaštita predstavlja prvi sloj odbrane u strategiji Defense in Depth, fokusiran na zaštitu mrežnih granica organizacije od neovlaštenog pristupa i potencijalnih napada izvana. Ovaj sloj obuhvata tehničke kontrole kao što su firewall-i, IDS/IPS te segmentacija mreže, čime se osigurava filtriranje saobraćaja, identifikacija sumnjivih aktivnosti i ograničavanje pristupa kritičnim resursima. Perimetarska zaštita omogućava organizacijama da unaprijed detektuju i blokiraju prijetnje prije nego što dopru do unutrašnjih sistema, čime se značajno smanjuje rizik od kompromitacije podataka i narušavanja kontinuiteta poslovanja. Implementacija višeslojnih kontrola na perimetru u kombinaciji sa stalnim nadzorom i analizom saobraćaja predstavlja ključni element proaktivnog pristupa informacionoj sigurnosti.

3.2.1.1. Firewall sistemi

Firewall sistemi predstavljaju osnovni tehnički mehanizam perimetarske zaštite, ali unutar strateškog okvira slojevite odbrane oni imaju mnogo širu ulogu od jednostavnog filtriranja paketa. Njihova funkcija počinje definisanjem jasno postavljenih pravila za kontrolu saobraćaja između internog informacionog sistema i spoljnog okruženja, pri čemu se ova filtracija vrši po kriteriju koji može uključivati izvorišnu ili odredišnu adresu, protokol, port ili kombinaciju ovih parametara. Dobro konfigurisan firewall ne dozvoljava prolaz nikakvom saobraćaju koji nije eksplicitno potreban za operativne procese organizacije, što direktno smanjuje površinu napada dostupnu potencijalnim prijetnjama. Unutar konteksta Defense in Depth pristupa, firewall-e je potrebno posmatrati ne samo kao prvu liniju odbrane već i kao element tzv. defense-in-depth zoniranja. To podrazumijeva da firewall ne stoji na jednoj granici mreže, već se primjenjuje u više tačaka – između korporativnih domena i specijalizovanih servisa poput SCADA sistema, kao i između različitih segmenata unutrašnje mreže. Primjena višeslojne segmentacije uz dodatne barijere smanjuje rizik da eventualni proboj jednog dijela infrastrukture rezultira kompromitovanjem cjelokupne arhitekture. Praktični modeli pokazuju efikasnost tako što formiraju izolovane zone za kritične operacije poput energetskog menadžmenta. Na primjer, izolovanje EMS (sistem za upravljanje elementima) domena dodatnim firewall-om od SCADA segmenta stvara fizičke i logičke

prepreke, pa napadač koji dođe do jednog dijela sistema mora savladati još jedan sloj zaštite prije nego što dobije pristup kontroli nad vitalnim funkcijama. Veoma je bitno da pravila budu specifična – dozvoljava se samo tačno definisani tip komunikacije prema poznatim host-ovima, sa jasnim protokolima i portovima. Jedan čest nedostatak jeste ignorisanje kontrole nad odlaznim (outbound) saobraćajem. Mnoge konfiguracije blokiraju dolazne veze dok istovremeno dozvoljavaju slobodan izlaz iz interne mreže. To otvara mogućnost da kompromitovani host unutar organizacije nesmetano komunicira sa komandno-kontrolnim serverima napadača. U skladu s filozofijom Defense in Depth, firewall mora filtrirati oba smjera komunikacije kako bi spriječio širenje incidenata i curenje podataka (Kuipers & Fabro, 2006). Firewall sistemi nisu homogeni, razlikuju se po tehnologiji koju koriste. Paketni filteri rade na osnovnom nivou analize zaglavlja paketa i pravila filtriranja. Statefull inspection dodaje sposobnost praćenja aktivnih sesija kako bi mogao donijeti odluke zasnovane na stanju konekcije. Aplikacioni proxy firewall-e idu korak dalje, pružaju inspekciju na aplikativnom nivou, filtrirajući sadržaj unutar prometa radi detekcije nepravilnosti koje paketni filteri ne bi prepoznali. U okviru višeslojne strategije moguće je kombinovati različite tipove firewall-a u zavisnosti od zone mreže koju štite. Integracija firewall-a sa ostalim slojevima zaštite povećava njihovu efikasnost. Kada su povezani na IDS/IPS sisteme ili SIEM platforme, firewall može koristiti podatke o detektovanim prijetnjama kako bi automatski ažurirao pravila blokade (Amro & Gkioulos, 2023). Time perimetarska barijera postaje dinamična komponenta koja adaptivno reaguje na otkrivene napade, umjesto statične liste pravila koja zahtijeva manuelnu intervenciju administratora. Pri implementaciji firewall-a u okruženja MSP-a javlja se potreba za balansiranjem performansi i nivoa bezbjednosti. Pretjerano restriktivna pravila mogu omesti legitiman rad aplikacija i usluga, dok previše permisivna politika ruši svrhu samog sloja odbrane (Adriko & Nurse, 2024). Zato se preporučuje fazna implementacija: prvo instalacija s osnovnim pravilima koja obezbjeđuju ključne zonske barijere, zatim njihovo postepeno usitnjavanje do optimalnog nivoa blokade u skladu sa analizama stvarnog saobraćaja. Važno je naglasiti da firewall sistemi sami po sebi nisu dovoljni za sprečavanje svih oblika upada niti za osiguranje integriteta i povjerljivosti podataka. Oni čine temelj slojevite arhitekture zajedno sa unutrašnjom segmentacijom mreže, sistemima autentifikacije korisnika te kontinuiranim nadzorom rada infrastrukture. Efektivnost ovog sloja može biti znatno umanjena ako ne postoji koordinacija između timova zaduženih za njegovo održavanje i drugih segmenata bezbjednosti, na primjer nepravovremeno ažuriranje firewall uređaja

ostavlja otvoren prostor poznatim ranjivostima koje napadači lako mogu iskoristiti. Poseban izazov nastaje kod integracije legacy sistema koji zahtijevaju komunikaciju preko zastarjelih protokola. Takvi protokoli često imaju inherentne sigurnosne nedostatke (nesigurna autentifikacija ili nekriptovana razmjena podataka), pa ih moderne firewall konfiguracije ponekad blokiraju po default-u. Za njihovo uključivanje potrebno je kreirati specifične sigurnosne politike koje omogućavaju rad aplikacijama uz minimiziranje rizika, na primjer tuneliranjem preko sigurnih kanala ili dodatnom validacijom sadržaja komunikacije iz tih protokola (Bartock, et al., 2021). Konačno, evaluacija rada firewall-a mora biti dio stalnog procesa provjere cijelog Defense in Depth sistema. Periodični auditi mrežnih pravila pomažu u detekciji nepotrebnih dozvola koje su uvedene privremeno pa ostale aktivne bez opravdanog razloga. Penetraciono testiranje fokusirano na perimetarsku zaštitu otkriva moguće rupe, recimo pogrešno konfigurisane virtualne lokalne mreže (Virtual Local Area Network, u daljem tekstu: VLAN) ili propuste u prevođenju mrežnih adresa (Network Address Translation, u daljem tekstu: NAT), koje bi mogle poslužiti kao ulazna tačka napadu (Kuipers & Fabro, 2006). Rezultati tih evaluacija trebaju voditi ka prilagođavanju konfiguracija kako bi ostale usklađene s aktuelnim prijetnjama i operativnim potrebama organizacije. Posmatrani kroz prizmu višeslojnog koncepta odbrane, firewall sistemi imaju dvostruku vrijednost: oni blokiraju mnoge vrste direktnih pokušaja upada s periferije mreže, ali istovremeno služe kao alat za kontrolu internih tokova podataka između različitih dijelova infrastrukture. Njihova pravilna implementacija u više zonskih pozicija predstavlja jedan od osnovnih stubova perimetarske zaštite bez koje cjelokupni okvir Defense in Depth strategije gubi prvi filter kroz koji se prepoznaje legitimni saobraćaj od malicioznog saobraćaja.

3.2.1.2. IDS/IPS sistemi

IDS i IPS predstavljaju ključne tehnološke komponente u sloju perimetarske zaštite, ali njihova funkcija unutar višeslojnog okvira odbrane ide znatno dalje od same detekcije ili blokiranja neželjenih paketa. Za razliku od firewall sistema koji primarno filtriraju saobraćaj na osnovu unaprijed definisanih pravila, IDS/IPS sistemi oslanjaju se na analizu sadržaja komunikacije i prepoznavanje indikatora kompromitacije u realnom vremenu. IDS je pasivna komponenta koja identifikuje sumnjive aktivnosti i generiše upozorenja, dok IPS aktivno reaguje na otkrivene prijetnje blokiranjem malicioznog saobraćaja ili prekidanjem sesije (Amro & Gkioulos, 2023). Ova dva mehanizma su prirodno komplementarna i često se implementiraju

zajedno kako bi pružili balans između detekcije i prevencije. U kontekstu Defense in Depth pristupa, IDS/IPS ne funkcionišu izolovano, njihovi podaci postaju dio šireg nadzornog ekosistema u kojem se koreliraju događaji iz više slojeva bezbjednosti. Na primjer, pokušaj upotrebe neautorizovanog protokola unutar specifične mrežne zone može biti detektovan IDS-om, dok IPS momentalno zaustavlja tu komunikaciju. Kada se ti događaji proslijede SIEM sistemu, moguće je povezati ih sa drugim indikatorima, poput neobičnih upita ka bazi podataka ili modifikacija privilegija korisnika (Rahman, et al., 2019). Time IDS/IPS sloj ne samo da štiti od direktnih napada već pomaže u otkrivanju koordinisanih kampanja koje obuhvataju više vektora kompromitacije. Prednost ovih sistema leži u mogućnosti definisanja pravila koja prelaze granice klasičnog filtriranja, mogu se zasnivati na heurističkoj analizi ponašanja mrežnog prometa, potpisima poznatih napada ili čak machine-learning modelima treniranim da prepoznaju anomalije. Kod ICS ili APS (Automation and Process System) mreža s predvidljivim obrascima saobraćaja ova karakteristika dobija posebnu važnost, jer komunikacioni tokovi među poznatim hostovima, IP/MAC adresama i portovima mogu biti striktno definisani, pa svako odstupanje od tog obrasca signalizira potencijalnu prijetnju (Amro & Gkioulos, 2023). IPS tada može selektivno intervenisati samo ako je procjena da je događaj visoko maliciozan, čime se smanjuje rizik prekidanja vitalnih operacija uslijed lažno pozitivnih detekcija. Međutim, integracija IDS/IPS zahtijeva pažljivu konfiguraciju kako bi se izbjegli konflikti sa ostalim slojevima zaštite. Preagresivna pravila IPS-a mogu izazvati tzv. „operativni zastoj" blokiranjem legitimnog saobraćaja koji nije formalno unijet u listu dozvoljenih obrazaca komunikacije. S druge strane, nedovoljno restriktivne konfiguracije ostavljaju otvoren prostor sofisticiranim metodama napada koje koriste legitimne kanale za prenos zlonamjernog sadržaja (Kuipers & Fabro, 2006). Upravo zato se preporučuje fazna implementacija počevši od pasivnog praćenja pomoću IDS-a kako bi se prikupili podaci o stvarnim obrascima rada sistema, a tek nakon analize tih podataka uvode se preventivne akcije kroz IPS. Dobar primjer integracije ovih tehnologija vidi se pri zaštiti kritičnih podsistema koji su već izolovani firewall-om, na primjer IDS prati interni promet unutar te izolovane zone i detektuje pokušaje eksploatisanja ranjivosti aplikacija, a kada takav pokušaj pređe definisani prag vjerovatnoće malicioznosti, IPS automatski prekida vezu između zaraženog host-a i ostatka sistema. Ovakav višeslojni pristup omogućava da čak i ako jedan sloj (npr. firewall) propusti maliciozan paket zbog pogrešnog pravila, sljedeći sloj (IDS/IPS) može identificirati prijetnju prije nego što ona dovede do kompromitovanja resursa. U

kombinaciji sa politikama autentifikacije i autorizacije u unutrašnjim segmentima mreže ove tehnologije dodatno otežavaju lateralno kretanje napadača. Ako napadač pokuša iskoristiti ukradeni nalog za pristup segmentu s bazom podataka, anomalija u obrascu upita biće detektovana od strane IDS-a, a IPS može automatski poništiti aktivnu konekciju tog naloga (Amro & Gkioulos, 2023). Na taj način tehničke kontrole rade zajedno s administrativnim procedurama, evidencija pokušaja pristupa služi kasnijoj forenzičkoj analizi radi procjene obima incidenta. Za MSP koja često nemaju kapacitete za stalni nadzor preporučuje se upotreba integrisanih rješenja koja kombinuju firewall i osnovne IDS funkcije na jednom uređaju. Takvi sistemi ne pružaju isti nivo prilagodljivosti kao specijalizovane platforme, ali omogućuju pristupačnu implementaciju osnovnog sloja detekcije/preventivne zaštite uz relativno jednostavno administriranje (Adriko & Nurse, 2024). U kontekstu Defense in Depth okvira ovakva rješenja djeluju kao dopuna drugim slojevima poput edukacije korisnika i upravljanja identitetom, čak i ako sofisticirani phishing uspije da kompromituje krajnji uređaj, IDS/IPS može zabilježiti neuobičajenu aktivnost tog uređaja prema mrežnim resursima te izazvati alarm. Nadzor performansi IDS/IPS sistema mora biti konstantan proces. Pravovremeno ažuriranje baza potpisa novih napada minimizira period tokom kojeg sistem nije sposoban da detektuje novootkrivene metode eksploatacije ranjivosti (Boggs, et al., 2009). Pored toga potrebno je kalibrisati parametre osjetljivosti kako bi stopa lažno pozitivnih rezultata bila prihvatljiva, previsok broj uzbuna može dovesti do ignorisanja upozorenja od strane administratora dok preniska osjetljivost kompromituje sposobnost detekcije stvarnih prijetnji. Evaluacija efikasnosti IDS/IPS sloja treba uključivati simulirane scenarije napada koji repliciraju aktualne prijetnje relevantne industriji organizacije (Kuipers & Fabro, 2006). Time se provjerava sposobnost sistema da reaguje prema dizajniranom nivou zaštite te otkriva potreba za prilagođavanjem postojeće konfiguracije s obzirom na promijenjene obrasce legitimnog saobraćaja ili nove vektore napada. Kroz Defense in Depth perspektivu rezultati ovakvog testiranja koriste se za optimizaciju koordinacije sa susjednim slojevima, prilagođavanje firewall pravila ili dodatnih kontrola aplikativnog nivoa radi smanjenja opterećenja samih IDS/IPS funkcija. Konačna vrijednost implementacije IDS/IPS sistema ogleda se u njihovoj sposobnosti da pruže transparentan pogled na događaje unutar mreže koji bi mogli proći neopaženo drugim vrstama zaštitnih mehanizama. Oni predstavljaju dinamičan filter koji nadopunjuje statične barijere perimetarske zaštite integracijom sa monitoring alatima i procedurama reagovanja na incidente. Kada su pravilno podešeni i

koherentno povezani sa ostatkom sigurnosne arhitekture, čine kritičan sloj višeslojne strategije sposoban da otkrije sofisticirane prijetnje te inicira njihovo brzo neutralisanje prije nego što ugroze kontinuitet rada organizacije.

3.2.1.3. Segmentacija mreže

Segmentacija mreže unutar strategije slojevite odbrane predstavlja ključan mehanizam za smanjenje površine napada i sprečavanje lateralnog kretanja potencijalnog napadača kroz infrastrukturu. Ona se oslanja na fizičko i logičko razdvajanje mrežnih segmenata, pri čemu se svaki segment štiti zasebnim pravilima pristupa, filtracije i detekcije anomalija. Logika ovog pristupa zasniva se na pretpostavci da kompromitovanje jednog dijela mreže ne smije automatski značiti kompromitovanje cijelog sistema, pa se interna topologija projektuje tako da postavlja više nezavisnih barijera (Amro & Gkioulos, 2023). U praktičnom smislu, segmentacija može biti realizovana putem VLAN-a, podmreža ili čak izolovanih fizičkih lanova (air-gap mreže), u zavisnosti od kritičnosti resursa koji se štite. Kod ICS ili SCADA domena ona podrazumijeva postavljanje granica između kontrolnih sistema i poslovne mreže preduzeća, čime se smanjuje mogućnost da napad sa javnog interneta ili poslovnog ERP servera direktno dotakne vitalni segment za upravljanje procesima (Kuipers & Fabro, 2006). Takve granice se dodatno pojačavaju firewall pravilima koja dozvoljavaju samo specifične tipove komunikacije između zona, a IDS/IPS sistemi postavljeni na međuspojevima prate promet radi otkrivanja anomalija. Polazni korak pri implementaciji segmentacije jeste analiza funkcionalnih potreba svake grupe resursa. Na osnovu te analize formiraju se sigurnosne zone kojima su pridruženi nivoi privilegija i kontrole. Segmenti koji sadrže serverske baze podataka obično imaju najstroža pravila pristupa, jer dozvoljen je saobraćaj samo prema poznatim aplikacionim serverima preko definisanih portova i protokola (Amro & Gkioulos, 2023). Uvedena pravila ograničavaju mogućnost neautorizovanih upita iz drugih segmenata mreže koji bi ciljano manipulisali zapisima u bazi ili pokušali eksfiltraciju podataka. Jedna od prednosti segmentacije je sposobnost da lokalizuje incident unutar jednog segmenta bez potrebe za potpunim gašenjem cijelog sistema. Ako napadač uspije da kompromituje uređaj u korisničkoj zoni, pravila komunikacije spriječit će ga da direktno pristupi administrativnim serverima ili kontrolnim sistemima koji upravljaju proizvodnim linijama. Time ostali dijelovi infrastrukture nastavljaju normalan rad dok timovi bezbjednosti rade na sanaciji pogođenog segmenta. Međutim, efikasnost segmentacije zavisi od pravilne implementacije pravila između zona.

Pogrešno podešeni ACL-ovi mogu omogućiti neželjeni saobraćaj između segmenata, čime se potire efekat razdvajanja. Blisko povezana praksa je kreiranje demilitarizovanih zona (u daljem tekstu: DMZ) za servise koji moraju komunicirati kako s unutrašnjom infrastrukturom tako i sa spoljnim klijentima, na primjer web serveri ili ICCP serveri u SCADA okruženjima (Kuipers & Fabro, 2006). DMZ služi kao tampon prostor gdje eventualni proboj ne ugrožava direktno unutrašnju mrežu, već integracijom višestrukih DMZ-a moguće je dodatno granularizovati prava pristupa po tipu servisa. Specijalni izazov u okruženju MSP javlja se kod potrebe povezivanja starih aplikacija koje koriste nesigurne protokole sa modernim segmentisanim mrežama. Ove aplikacije zahtijevaju poseban tretman – često je potrebno tuneliranje komunikacije kroz sigurne kanale ili izolacija u mikrosegmentu sa restriktivnim pravilima (Bartock, et al., 2021). Mikrosegmentacija ide korak dalje od tradicionalnog VLAN razdvajanja stvaranjem vrlo malih zona (često na nivou pojedinačnih virtuelnih mašina ili servisa) koje imaju svoje sopstvene politike bezbjednosti. Taj pristup smanjuje posljedice kompromitovanja jednog entiteta jer su njegove mogućnosti kretanja kroz ostatak sistema minimalne. Segmentacija ima snažnu povezanost sa funkcijama praćenja i reagovanja opisanima kod NIST okvira, monitoring unutar svakog segmenta daje preciznije informacije o incidentu jer ograničena površina nadzora omogućava jasniju identifikaciju izvora problema (Amro & Gkioulos, 2023). SIEM platforme fokusirane na određene zone lakše koreliraju događaje i razlike u obrascima prometa među segmentima; kada se otkrije promjena koja krši definisana pravila zone, sistem može aktivirati blokadu baražnog tipa unutar tog segmenta prije nego što anomalija zahvati druge zone. U kombinaciji sa autentifikacijom korisnika po principu najmanjih privilegija, segmentacija dodatno otežava rad napadaču čak i ako posjeduje validne kredencijale za jedan dio sistema (Neri, et al., 2022). Ograničenja pristupa znače da ovlaštenja važe samo unutar konkretne zone, a pokušaji prelaska granice aktiviraju upozorenja na kontrolnim tačkama između segmenata. Ovaj mehanizam fokusira potencijalnu štetu na minimalnu oblast dok ostali sistemi ostaju netaknuti. Za organizacije koje upravljaju kritičnom infrastrukturom posebno je relevantna fizička segmentacija, odvajanje kontrole procesa putem dedicated hardverskih mreža potpuno nepovezanih sa internetom (air-gap). Iako ova metoda drastično smanjuje vektore daljinskog napada, ona ima svoje operativne izazove vezane za ažuriranje softvera i prenos podataka među zonama, jer rješenja uključuju striktno kontrolisane procedure ručnog prenosa podataka uz prethodnu validaciju sadržaja (Kuipers & Fabro, 2006). MSP često biraju logičku (VLAN/podmreže)

segmentaciju zbog nižih troškova implementacije i lakšeg skaliranja kada se mijenja topologija mreže, ali mogu dopuniti tu strukturu fizičkim barijerama u dijelovima sistema koji podliježu regulatornim zahtjevima visokog nivoa zaštite. Stalna evaluacija učinkovitosti intersegmentnih pravila predstavlja obaveznu aktivnost, koristi se penetraciono testiranje koje simulira pokušaje prelaska iz jedne zone u drugu putem ranjivosti aplikacija, neočekivanih konfiguracionih slabosti ili zloupotrebe legitimnih kredencijala (Boggs, et al., 2009). Rezultati analize pokazuju koliko su zidovi između zona stvarno čvrsti i gdje ih treba pojačati dodatnim filtriranjem ili autentifikacijom. Kombinacijom rezultata testiranja s audit zapisima iz sistema upravljanja identitetom daju se potpune informacije za prilagođavanje sigurnosnih politika svake zone posebno. Veoma bitan aspekt jest edukacija administratora i osoblja koje održava mrežne segmente o rizicima koji proizilaze iz pogrešne konfiguracije, nedosljedno primjenjivanje pravila može otvoriti skriveni tunel prema osjetljivim resursima mimo predviđenih tačaka kontrole (Bada & Nurse, 2019). Stoga strateško upravljanje segmentacijom nije samo tehničko pitanje već dio šire kulture bezbjednosti koja traži koordinaciju svih aktera uključenih u rukovanje infrastrukturom. Kroz ovu interakciju tehničkih, proceduralnih i ljudskih faktora segmentacija postaje ne samo barijera nego inteligentan filter kroz koji prolazi samo ono što ima potvrđenu operativnu legitimnost u skladu sa definisanim pravilima višeslojne zaštite sistema.

3.2.2. Unutrašnja zaštita

Unutrašnja zaštita predstavlja ključni sloj Defense in Depth strategije, usmjeren na kontrolu i ograničavanje aktivnosti unutar mrežnog okruženja organizacije, posebno u scenarijima kada je perimetarska zaštita kompromitovana. Ovaj sloj obuhvata implementaciju mehanizama kontrole pristupa, segmentaciju unutrašnje mreže i sprovođenje sigurnosnih politika koje definišu dozvoljene obrasce komunikacije između sistema i korisnika (Johnson, 2025). Cilj unutrašnje zaštite jeste smanjenje mogućnosti lateralnog kretanja napadača, ograničavanje eskalacije privilegija i zaštita kritičnih resursa od neovlaštene upotrebe. Dosljedna primjena unutrašnjih sigurnosnih kontrola omogućava raniju detekciju anomalija i pruža dodatni vremenski okvir za odgovor na incidente, čime se značajno unapređuje ukupna otpornost informacionog sistema (Maulding, 2026).

3.2.2.1. Kontrola pristupa

Kontrola pristupa unutar strategije slojevite odbrane zauzima centralno mjesto u unutrašnjem sloju zaštite jer direktno definiše ko, kada i pod kojim uslovima može pristupiti određenim resursima organizacije. Osnovna ideja leži u primjeni principa najmanjih privilegija (least privilege), prema kojem svaki korisnik ili proces dobija samo onaj nivo ovlaštenja koji mu je nužno potreban za obavljanje predviđenih zadataka (Neri, et al., 2022). Ova filozofija garantuje da čak i kompromitovani nalog ne može automatski ugroziti cijelu infrastrukturu, već samo segment za koji posjeduje dozvolu, što omogućava zadržavanje incidenta unutar ograničenog okvira (Alsmadi, 2023). Praktična primjena kontrole pristupa počinje izgradnjom jasno definisane politike koja obuhvata kreiranje, izmjene i brisanje korisničkih naloga, dodjelu privilegija te redovnu reviziju tih prava radi otkrivanja nepravilnosti (n.a., 2009). Takva politika se implementira kroz sisteme upravljanja identitetom (Identity Management Systems, u daljem tekstu: IMS) koji centralizuju nadzor nad cjelokupnom populacijom korisnika unutar organizacije. Centralizovani sistemi omogućavaju lako povlačenje pristupa bivšim zaposlenima ili privremenim saradnicima odmah po završetku njihove angažovanosti, čime se zatvara potencijalni vektor unutrašnje prijetnje. U slojevitoj arhitekturi zaštite kontrola pristupa se tehnički realizuje višestrukim mehanizmima autentifikacije i autorizacije. Autentifikacija verificira identitet subjekta – putem lozinki, tokena, biometrijskih podataka – dok autorizacija provjerava da li verifikovani subjekt ima odgovarajuće ovlaštenje da izvrši zahtjevanu operaciju. MFA dodaje dodatne slojeve verifikacije, pa čak i ako napadač kompromituje statičke kredencijale poput lozinke, neophodno je posjedovati drugi faktor (npr. jednokratni kod sa mobilnog uređaja) kako bi se kompletirao proces prijave. Kontrola pristupa nije ograničena na korisničke naloge, ona se proširuje na aplikacije, baze podataka i mrežne segmente (Amro & Gkioulos, 2023). Granularno podešavanje dozvola za pojedinačne datoteke ili folder strukture u sistemima za skladištenje podataka sprečava da neovlašteni subjekti kopiraju ili modifikuju osjetljive informacije. Na mrežnom nivou ACL definišu pravila koja upravljaju prolaskom prometa između različitih segmenata interne mreže. Kada su ove liste integrisane sa segmentacijom mreže prikazanom ranije, stvara se višeslojna prepreka kretanju potencijalno štetnog prometa ka zaštićenim zonama (Kuipers & Fabro, 2006). Jedan poseban aspekt predstavlja kontrola administratorskih privilegija. Privilegije „root” ili „administrator” daju potpunu kontrolu nad sistemom, a njihovo dodjeljivanje mora biti

limitirano i prati ih stroga evidencija upotrebe. Sistemi log-ovanja svih administratorskih akcija služe dvostrukoj svrsi – detekciji zloupotreba u realnom vremenu i forenzičkoj analizi nakon incidenta. U nekim industrijama koje podliježu regulatornim obavezama implementira se model dvojnog odobravanja akcija (dual control), gdje je potrebna potvrda od strane dvije nezavisne osobe prije izvršenja kritične izmjene konfiguracije. Integracija kontrole pristupa sa nadzornim sistemima kao što su SIEM platforme omogućava korelaciju pokušaja neovlaštenog pristupa s drugim indikatorima prijetnji (Amro & Gkioulos, 2023). Pokušaj prijave s neuobičajene IP adrese može pokrenuti automatizovanu proceduru blokiranja naloga dok administrator ne potvrdi legitimnost aktivnosti. Ovakva proaktivna reakcija značajno smanjuje vrijeme potrebno da incident bude stavljen pod kontrolu. U okruženjima MSP, finansijska ograničenja često nameću izbor jednostavnijih rješenja koja ipak moraju biti projektovana tako da podrže osnovne principe strategije Defense in Depth. To može uključivati kombinovanje cloud servisa za upravljanje identitetom s lokalnim politikama ACL-a na serverskim instancama, uz MFA dostupnu putem mobilnih aplikacija koje imaju minimalne troškove licenciranja (Ejjami, 2024). Važno je redovno testirati efikasnost kontrole pristupa kroz simulirane scenarije napada, jer pokušaji eskalacije privilegija unutar aplikacija ili prelaska iz jednog segmenta mreže u drugi bez autorizacije pokazuju eventualne slabosti sistema koje treba otkloniti. Ljudski faktor je suštinski povezan s ovom tematikom, ali edukacija zaposlenih o pravilnoj upotrebi povjerljivih kredencijala smanjuje rizik nehotičnog otkrivanja lozinki ili tokena potencijalnim napadačima. Programi obuke moraju obuhvatati osvježavanje znanja o phishing metodama koje ciljaju krađu identiteta, kao i procedurama prijave sumnjivih događaja bezbjednosnom timu. Integrisanje edukacije unutar politike kontrole pristupa osigurava da tehničke mjere budu podržane disciplinovanom primjenom pravila od strane korisnika. Tehnički izazovi kod implementacije kontrole pristupa uključuju integraciju modernih metoda autentifikacije sa zastarjelim sistemima koji ne podržavaju nove protokole. U tim slučajevima koriste se adapteri ili proxy servisi koji premoštavaju razliku u tehnologijama dok zadržavaju standarde bezbjednosti novijeg sloja arhitekture. Rizik koji nose legacy sistemi time se kontroliše zadržavanjem istih unutar mikrosegmenta sa sopstvenim pravilima pristupa i nadzora. Sveobuhvatna kontrola pristupa u strategiji Defense in Depth funkcioniše kao dinamičan sloj koji povezuje perimetarsku zaštitu sa aplikativnom sigurnošću i segmentacijom mreže. Njena koordinacija sa ostalim slojevima znači da probijanje jednog mehanizma neće dovesti do potpune kompromitacije, ako drugi slojevi uspješno prepoznaju

i blokiraju pokušaje zloupotrebe ovlaštenja. Takav integrisani okvir čini kontrolu pristupa jednim od najvažnijih elemenata unutrašnje zaštite unutar sveobuhvatnog sistema odbrane jer direktno ograničava domet svakog potencijalnog napadača na definisanu zonu djelovanja koja se može izolovati bez degradacije cjelokupnog rada organizacije.

3.2.2.2. Sigurnosne politike unutar mreže

Sigurnosne politike unutar mreže čine temeljnu komponentu slojevite strategije zaštite jer uređuju precizna pravila, procedure i tehničke konfiguracije kojima se upravlja načinom korištenja mrežnih resursa, pristupom podacima te nadzorom aktivnosti korisnika i servisa. Njihova uloga nije ograničena na formalno dokumentovanje dozvoljenih i zabranjenih ponašanja, već obuhvata operativnu primjenu kontrola u skladu s principima najmanjih privilegija i segmentacije opisanih ranije (Bao et al., 2023). Efikasne politike integrišu tehničke mjere (npr. ACL pravila, VLAN segmentaciju, enkripciju komunikacija), administrativna pravila (dodjela i revizija privilegija) i organizacione aspekte (edukacija korisnika o sigurnosnim procedurama), čime se ostvaruje koordinisana odbrana protiv unutrašnjih i spoljnjih prijetnji. Iz perspektive Defense in Depth okvira, sigurnosne politike imaju višeslojni karakter, svaka mrežna zona ima sopstvena ograničenja pristupa, koja su definisana prema kritičnosti podataka i usluga koje sadrži (Amro & Gkioulos, 2023). Na primjer, politika može predvidjeti da administrativni segmenti budu dostupni isključivo sa određenih administrativnih konzola preko VPN-a sa MFA, dok su sve druge vrste konekcija automatski blokirane firewall pravilima. Time se stvara sinergija između perimetarskih barijera i unutrašnje kontrole kretanja kroz mrežu. Konkretna implementacija ovih politika odvija se kroz konfiguracije mrežnih uređaja poput router-a i switch-eva, gdje se ACL koriste za definisanje dozvoljenog prometa između zona (Kuipers & Fabro, 2006). Politike sadrže specifikacije protokola, portova i IP adresa koje su legitimne, jer sve ostalo se tretira kao potencijalna prijetnja. Poseban dio ovih politika obuhvata filtriranje odlaznog (egress) saobraćaja kako bi se spriječilo curenje podataka ka nepoznatim ili malicioznim destinacijama, kontrola koja je često zanemarena u manje razvijenim okruženjima. Uspostavljanje DMZ za javno dostupne servise također spada u domen mrežnih sigurnosnih politika (Amro & Gkioulos, 2023). DMZ omogućavaju razdvajanje javnog saobraćaja od unutrašnje mreže tako da kompromitacija web servera ili email gateway-a ne podrazumijeva automatski pristup internim poslovnim sistemima. Politike određuju načine razmjene podataka između DMZ i drugih zona uz stroga filtriranja, čime se

umanjuje mogućnost lateralnog kretanja napadača. Integracija kontrola autentifikacije u same mrežne politike dodatno osnažuje slojevitu odbranu. Implementacija 802.1X standarda za autentifikaciju na nivou porta switch-a osigurava da samo validirani uređaji mogu komunicirati unutar definisane zone. Ove autentifikacione mjere povezuju se sa centralizovanim upravljanjem identitetima kako bi prava pristupa bila dinamički dodijeljena ili opozvana u zavisnosti od statusa korisnika ili uređaja. Jedan od važnih aspekata sigurnosnih politika je obračunavanje sa rizicima koje nose zastarjeli sistemi. Legacy aplikacije koje zahtijevaju nesigurne protokole moraju biti izolovane unutar mikrosegmenata sa minimalnim pravima komunikacije prema ostatku infrastrukture (Bartock, et al., 2021). Politike tada uređuju čuvanje log-ova interakcija tih aplikacija kako bi se eventualne anomalije mogle brzo detektovati. Politički okvir za nadzor aktivnosti unutar mreže oslanja se na SIEM sisteme koji prikupljaju log-ove sa svih tačaka kontrole (Amro & Gkioulos, 2023). Pravila koja definišu kada će određeni događaj generisati alarm dio su šire politike reagovanja na incidente, a ona obezbjeđuju da detekcija anomalija bude brza i relevantna. U tom smislu IDS/IPS sistemi rade u skladu s politikama filtriranja kako bi blokirali potvrđene prijetnje prije nego što dođe do kompromitovanja kritičnih resursa. U kontekstu MSP izazov leži u usklađivanju nivoa detalja sigurnosnih politika sa kapacitetima osoblja zaduženog za njihovu primjenu. Pretjerano kompleksne politike koje mala ekipa ne može pratiti rezultiraju „sigurnošću na papiru" bez stvarnog uticaja na rad sistema. Stoga je preporučljivo postepeno uvođenje granularnih pravila nakon što osnovni set bude stabilno implementiran. Edukacija korisnika i administratora o sadržaju i svrsi sigurnosnih politika ključna je za njihovu efikasnost. Pravila koja ostanu nerazumljiva krajnjim korisnicima često bivaju zaobilažena iz praktičnih razloga, čime se otvaraju nove ranjivosti. Programi osposobljavanja treba da objasne ne samo šta su pravila već i zbog čega postoje. Sigurnosne politike moraju biti predmet redovne revizije kako bi pratile promjene topologije mreže, pojavu novih servisa ili evoluciju prijetnji. Revizije mogu otkriti zastarjela pravila koja više nisu potrebna ili otvoriti prostor novim zaštitnim mjerama. Testiranje efikasnosti kroz interne penetracione testove pruža empirijske podatke o tome koliko propisana pravila zaista funkcionišu protiv modernih napada. Zaključno se može reći da sigurnosne politike unutar mreže predstavljaju živi dokument koji mora biti sinhronizovan s tehničkim slojevima zaštite opisanim u prethodnom poglavlju. One nisu samo formalnost već operativni mehanizam kojim organizacija diktira ritam i granice kretanja informacija kroz svoj informacioni prostor, kombinujući kontrole pristupa, segmentaciju, perimetarske mjere,

enkripciju i nadzor u koherentan zaštitni okvir sposoban da amortizuje širok spektar sajber prijetnji čuvajući pritom poslovnu funkcionalnost sistema.

3.2.3. Korisnička autentifikacija i autorizacija

Korisnička autentifikacija i autorizacija predstavljaju ključni sloj Defense in Depth strategije, čiji je cilj osigurati da samo ovlašteni korisnici imaju pristup informacionim resursima, u skladu sa jasno definisanim ulogama i privilegijama. Autentifikacija se odnosi na proces provjere identiteta korisnika, dok autorizacija definiše nivo i obim pristupa koji je korisniku dozvoljen nakon uspješne identifikacije.

Primjena MFA značajno smanjuje rizik od neovlaštenog pristupa, posebno u slučajevima kompromitacije korisničkih kredencijala. Upravljanje privilegijama, zasnovano na principu najmanjih ovlaštenja, dodatno ograničava potencijalnu štetu u slučaju sigurnosnog incidenta. Ovaj sloj omogućava centralizovanu kontrolu pristupa, poboljšava praćenje korisničkih aktivnosti i predstavlja osnovu za usklađenost sa međunarodnim standardima informacione sigurnosti.

3.2.3.1. Višefaktorska autentifikacija

Višefaktorska autentifikacija predstavlja složenu, višeslojnu metodu verifikacije identiteta korisnika koja se u strategiji slojevite zaštite funkcionalno integriše sa ostalim mehanizmima unutrašnje odbrane i upravljanja pristupom. Osnovna ideja MFA jeste da proces prijave ne zavisi isključivo od jednog tipa kredencijala, kao što je lozinka, već da zahtijeva kombinaciju različitih faktora autentifikacije koji potiču iz bar dvije ili tri kategorije: nešto što korisnik zna (npr. lozinka ili PIN kod), nešto što korisnik posjeduje (token, pametna kartica, mobilni uređaj), te nešto što korisnik jeste (biometrijski marker poput otiska prsta ili prepoznavanja lica) (Amro & Gkioulos, 2023). Ova metodologija povećava otpornost sistema na ugrožavanje naloga putem krađe akreditiva jer napadač mora istovremeno kompromitovati više nezavisnih faktora, što statistički smanjuje vjerovatnoću uspješnog upada. Kombinovanje MFA sa principom najmanjih privilegija dodatno pojačava slojevitu arhitekturu zaštite. Ako određeni nalog ima ograničen pristup kritičnim resursima, čak i potpuna kompromitacija tog naloga ne omogućava lateralno kretanje kroz sistem bez prolaska kroz druge instance višefaktorske verifikacije unutar novih zona (Buchanan, 2020). U praksi, to znači da administrativni sistemi mogu zahtijevati drugi set MFA parametara od onih koji važe za opšti poslovni segment mreže. Takvo „granuliranje“ autentifikacije sprečava da se jednom

potvrđeni identitet automatski prihvati kao legitimni i u kontekstu osjetljivijih operacija. Tehnički, MFA može biti realizovana kroz različite integracione modele. Tradicionalna implementacija podrazumijeva hardverske tokene koji generišu jednokratne kodove (One-Time Password, u daljem tekstu: OTP) sinhronizovane sa serverom za autentifikaciju. Savremena rješenja sve češće koriste softverske aplikacije koje obavljaju istu funkciju na mobilnim uređajima, pri čemu se komunikacija između klijenta i servera štiti kriptografskim protokolima poput TLS-a (Bartock, et al., 2021). Biometrijska komponenta donosi visok nivo sigurnosti zbog jedinstvenosti fizičkih karakteristika korisnika, ali istovremeno otvara pitanja privatnosti i potrebe za zaštitom biometrijskih podataka enkripcijom u mirovanju i tranzitu. Integracija MFA zahtijeva usklađenost sa sigurnosnim politikama unutar mreže kako bi procedura bila funkcionalna u svim segmentima. ACL mogu se podesiti tako da odbijaju pokušaje pristupa kada drugi faktor nije validiran u predviđenom vremenskom okviru ili iz geografske lokacije koja ne odgovara politici pristupa. Ovakva koordinacija između mrežne infrastrukture i autentifikacionih servisa stvara dinamičan filter koji sprečava prihvatanje nepotpunih autentifikacionih procesa. Unutar Defense in Depth koncepta MFA se nadovezuje na perimetarsku zaštitu i unutrašnje mehanizme kontrole pristupa. Primjera radi, VPN konfigurisan za pristup administrativnim zonama može zahtijevati inicijalnu prijavu pomoću lozinke i tokena, a zatim firewall dozvoljava promet samo prema specifičnim servisima, dok aplikacioni sloj ponovo traži biometrijsku potvrdu identiteta prije izvođenja kritične komande (Amro & Gkioulos, 2023). Time svaka faza interakcije sa sistemom dobija svoj sopstveni sloj provjere identiteta. Ljudski faktor igra značajnu ulogu u efikasnosti MFA, tako da korisnici moraju biti upoznati sa time kako pravilno koristiti drugo ili treće sredstvo verifikacije te razumjeti razloge postojanja ovakve politike. Edukacija uključuje objašnjenje rizika ponovnog korištenja lozinki, opasnosti od phishing kampanja koje ciljaju krađu drugog faktora (npr. lažno traženje jednokratnog koda), te potrebu čuvanja fizičkih tokena od gubitka ili krađe. Bez ovakvog znanja korisnici mogu nehotice napraviti besmislenu dodatnu sigurnosnu kontrolu. Prilagođavanje MFA okruženju MSP-a često podrazumijeva balans između troškova licenciranja specijalizovanih sistema i koristi koje oni donose (Ejjami, 2024). Softverski tokeni putem mobilnih aplikacija predstavljaju finansijski prihvatljiv izbor koji ne zahtijeva posebnu hardversku infrastrukturu, dok za naročito osjetljive segmente, npr. za baze klijenata može biti opravdano investirati u hardversku autentikaciju kao sekundarni faktor. Sigurnosne implikacije implementacije MFA protežu se do zaštite od automatizovanih napada poput

credential stuffing-a. Čak i kada baza ukradenih akreditiva sadrži validne lozinke, odsustvo drugog faktora čini ih neupotrebljivima (Kuipers & Fabro, 2006). Nadzorni sistemi integrisani s MFA servisom mogu automatski bilježiti neuspjele pokušaje verifikacije drugog faktora, povezivati ih sa IP adresama izvora napada i alarmirati administratorski tim prije nego što broj pokušaja postane kritično visok. Sa tehničke strane nužno je periodično testiranje otpornosti MFA mehanizama na nove vektore prijetnji. To uključuje simulirane scenarije man-in-the-middle napada tokom prijenosa jednokratnih kodova ili reprodukciju biometrijskih uzoraka pomoću sofisticiranih vještačkih metoda. Rezultati ovakvih testiranja služe prilagođavanju postojećih algoritama za generisanje OTP kodova ili unapređenju algoritama detekcije prevare kod biometrije. Važan aspekt održavanja MFA jeste politika rotiranja sekundarnog faktora, npr. periodično mijenjanje token uređaja ili resetovanje tajnog ključa mobilne aplikacije – čime se smanjuje rizik dugotrajnog kompromitovanja istog verifikacionog sredstva. Te politike moraju biti dokumentovane unutar ISMS-a i praćene audit zapisima dostupnim sigurnosnom timu radi forenzičke analize potencijalnih incidenata. Kao dio višeslojnog sistema zaštite integrisanog sa segmentacijom mreže i kontrolom privilegija, MFA postaje kritičan element kojim se prekida lanac mogućeg napada već u fazi inicijalnog zahtjeva za pristup resursima (Amro & Gkioulos, 2023). Kada su svi slojevi usklađeni, od perimetarskog filtera do aplikativnog nadzora, ona pruža vjerovatno najveću barijeru protiv neovlaštenog pristupa, jer zahtijeva simultanu kompromitaciju tehničkih sredstava, procedura autorizacije i ljudskog nadzornog faktora.

3.2.3.2. Upravljanje privilegijama

Upravljanje privilegijama predstavlja ključan segment u strategiji slojevite odbrane, jer omogućava precizno definisanje, praćenje i kontrolu nivoa pristupa koje pojedini korisnici, procesi ili servisi imaju nad različitim resursima informacionog sistema. Za razliku od opšte kontrole pristupa koja reguliše ko može doći do određenih podataka ili funkcija, upravljanje privilegijama fokusira se na administrativne i povišene ovlasti koje nose posebnu težinu po bezbjednost, uključuju ći tzv. super korisničke (root/admin) naloge. Princip najmanjih privilegija igra dominantnu ulogu i ovdje svaki subjekat treba da raspolaže samo minimalnim set-om dozvola neophodnih za izvršavanje konkretnih zadataka, bez unaprijed dodijeljenih trajnih administrativnih prava ukoliko to nije apsolutno nužno (Christen et al., 2020). U kontekstu višeslojne zaštite, upravljanje privilegijama se oslanja na koordinaciju tehničkih

mehanizama autentifikacije, segmentacije mreže i nadzora aktivnosti. Tehnička realizacija često uključuje specijalizovane sisteme za upravljanje privilegovanim nalozima (Privileged Access Management, u daljem tekstu: PAM), koji centralizuju čuvanje akreditiva sa povišenim ovlaštenjima u bezbjednim „novčanicima“ (vault), obezbjeđuju automatizovano izdavanje jednokratnih pristupnih kredencijala i prate ponašanje svake privilegovane sesije (Amro & Gkioulos, 2023). Ovi sistemi integrišu se sa MFA rješenjima opisanim ranije kako bi dodatno otežali kompromitovanje kritičnih naloga, pa čak i ako je lozinka poznata, napadač mora savladati još jedan ili više faktora verifikacije prije nego što ostvari pristup resursima. Jedan od osnovnih slojeva koji potpomaže pravilno upravljanje privilegijama jeste detaljna evidencija svih akcija izvršenih sa povišenim ovlaštenjima. Sve promjene konfiguracionih fajlova, instalacija softvera ili modifikacija baza podataka obavljene kroz administrativni nalog moraju biti auditovane i povezane sa identitetom stvarnog korisnika koji ih je pokrenuo (change management). Centralizovani sistemi logovanja (npr. SIEM) služe korelaciji tih događaja sa drugim indikatorima prijetnji iz mrežnog i aplikativnog sloja (Amro & Gkioulos, 2023). Na taj način je moguće detektovati anomalije kao što su pokušaji izmjene privilegija iz neuobičajenih lokacija ili van radnog vremena. Unutar organizacije od kritične važnosti je razdvajanje dužnosti (Separation of Duties, u daljem tekstu: SoD), što znači da nijedna osoba ne bi trebalo da ima potpuni nadzor nad cjelokupnim ciklusom neke operacije. Na primjer, administrator baze podataka ima tehnički pristup sistemu, ali nema dozvole da samostalno odobrava promjene strukture podataka bez validacije od strane kontrolorskog tima (Neri, et al., 2022). Ovaj princip posebno je važan kod okruženja MSP gdje mali broj zaposlenih često obavlja više rola, pa formalizovanje SoD procesa sprečava se koncentrisanje kritičnih prava kod jednog pojedinca. Kontrola privremenih privilegija predstavlja još jedan važan element. Idealan scenario predviđa dodjelu većih ovlaštenja samo za trajanje specifičnog zadatka pomoću vremenski ograničenih naloga ili privremenog eskaliranja prava uz automatsko opozivanje po završetku operacije (n.a., 2009). Na ovaj način se smanjuje rizik od dugotrajne zloupotrebe neaktivnog administrativnog računa. Integracija upravljanja privilegijama sa segmentacijom mreže doprinosi ideji Defense in Depth, time što se čak i unutar administrativne zone postavljaju unutrašnji filteri. Privilegovani nalog kreiran za održavanje serverskog segmenta ne bi trebalo da ima direktan pristup kontrolnim sistemima industrijskog pogona bez posebne provjere i zasebne autentifikacione procedure (Kuipers & Fabro, 2006). Takva granularna restrikcija vezuje svaku privilegiju za njenu main zonu čime lateralno

kretanje napadača biva znatno otežano. Tehnički aspekt implementacije u modernim sistemima često koristi hardverske sigurnosne module (u daljem tekstu: HSM) ili povjerljiva izvođenja softvera koja sprečavaju direktan pristup akreditivima izvan sigurnosno definisanih procedura (Bartock, et al., 2021). Ovo posebno dolazi do izražaja kod zaštite lozinki root naloga na UNIX/Linux serverima gdje PAM sistemi dinamički generišu kredencijale pri svakom zahtjevu, a originalni dugoročni ključ ostaje izolovan unutar HSM-a. Edukacija osoblja koje koristi ili upravlja privilegovanim nalozima presudna je za očuvanje efektivnosti ovog sloja odbrane (Tetteh, 2024). Čak i najsofisticiraniji tehnički alati mogu biti obesmišljeni ukoliko korisnici dijele administrativne akreditive putem nesigurnih kanala ili ih skladište u nezaštićenim formatima. Treninzi moraju obuhvatiti praktične smjernice poput zabrane čuvanja lozinki u plain-text fajlovima, obavezne upotrebe password menadžera lozinki te protokole prijave sumnjivih aktivnosti vezanih uz korištenje povišenih prava. Periodične revizije dodijeljenih privilegija su sastavni dio procesa, te svaka dodjela mora biti povezana s dokumentovanim poslovnim razlogom koji je provjerljiv. Revizije otkrivaju „privilege creep" fenomen kada korisnici vremenom akumuliraju nove dozvole, a stare im nisu opozvane i takva situacija povećava površinu napada dostupnošću eventualnog kompromitovanja tog naloga. Okruženja MSP suočavaju se sa specifičnim izazovima zbog ograničenog broja stručnjaka koji mogu pratiti sve aspekte privilegovanog pristupa (Ejjami, 2024). Automatizacija preko skripti koje sinhronizuju status zaposlenih između HR sistema i IAM/PAM platformi ublažava ovaj problem i smanjuje kašnjenja u opozivu prava nakon odlaska zaposlenih. Testiranje otpornosti mehanizma upravljanja privilegijama kroz simulirane scenarije kompromitovanja administratorskih naloga pomaže u procjeni zrelosti sistema zaštite. U tim testovima provjerava se brzina detekcije zloupotrebe, djelotvornost procedura izolovanja pogođenog naloga te tačnost forenzičkih podataka potrebnih za istragu. Kombinovanjem svih ovih aspekata, to jest principa najmanjih privilegija, SoD-a, kontrole privremenih prava, centralizovanog audita sesija, integracije sa mrežnom segmentacijom i stalne edukacije, upravljanje privilegijama postaje dinamičan sloj višeslojne strategije sposoban da ograniči potencijalne štete čak i kod kompromitovanja najkritičnijih tačaka pristupa informacijskim resursima organizacije.

3.3. Korisnička edukacija i svijest

Korisnička edukacija i razvijanje svijesti o informacionoj sigurnosti predstavljaju ključne elemente savremenih sigurnosnih strategija. S obzirom na to da je ljudski faktor često najslabija karika u zaštiti informacionih sistema, kontinuirana obuka korisnika doprinosi smanjenju rizika od sigurnosnih incidenata, posebno onih koji proizilaze iz socijalnog inženjeringa, phishing napada i neadekvatnog rukovanja osjetljivim podacima.

3.3.1. Programi obuke zaposlenih

Programi obuke zaposlenih predstavljaju jedan od ključnih slojeva u višeslojnoj strategiji zaštite, jer direktno utiču na ljudski faktor, koji često ostaje najslabija karika u lancu bezbjednosti informacionih sistema. Efektivna edukacija korisnika ima zadatak da poveća njihovu sposobnost prepoznavanja i pravilnog reagovanja na potencijalne sajber prijetnje, čime se zatvara veliki broj vektora napada koje tehnički sistemi sami ne mogu u potpunosti eliminisati (Tetteh, 2024). U kontekstu slojevitog pristupa, znanje i ponašanje zaposlenih služe kao komplement tehničkim kontrolama kao što su firewall sistemi, segmentacija mreže i MFA, pa neuspjeh na tom planu može obezvrijediti i najnaprednije mehanizme zaštite (Ejjami, 2024). Osnovni cilj kvalitetnog programa obuke je omogućiti svim nivoima osoblja, od početnika do rukovodilaca, da razumiju kako njihove svakodnevne aktivnosti mogu doprinijeti očuvanju povjerljivosti, integriteta i dostupnosti podataka. Treninzi obično obuhvataju teme prepoznavanja phishing poruka, sigurnog upravljanja lozinkama, politike korištenja uređaja i mreža, te prijavljivanja sumnjivih aktivnosti. Da bi bili efikasni, programi se ne smiju tretirati kao jednokratni događaji, već je potrebno kontinuirano ponavljanje i nadogradnja sadržaja uz prilagođavanje aktuelnim trendovima prijetnji. Nedostatak strukturiranosti može rezultirati time da zaposleni nemaju jasnu predstavu o procedurama niti razvijene automatizovane reakcije u kriznim situacijama. Primjena praktičnih elemenata unutar obuka daje vidljive rezultate. Korištenje virtuelnih laboratorija za sajber bezbjednost omogućava zaposlenima da u simuliranom okruženju prođu kroz scenarije realnih napada, poput pokušaja upada putem ransomware-a ili spear-phishinga i vježbaju odgovarajuće korake detekcije i neutralizacije prijetnje (Ejjami, 2024). Ovakav pristup nadilazi pasivno prenošenje informacija, jer angažuje polaznike da aktivno reaguju i primjenjuju naučeno, dok istovremeno razvijaju refleks prepoznavanja anomalija. Jedna od bitnih stavki je i integracija edukativnih programa sa postojećim politikama kontrole pristupa i autorizacije. Ako se zaposleni obučavaju u

kontekstu stvarnog okruženja u kojem rade, koristeći svoje postojeće naloge, interne aplikacije i procese veća je vjerovatnoća da će naučene prakse postati dio svakodnevnog ponašanja. Time se smanjuje rizik od incidenata izazvanih nehotičnim kršenjem politika ili nesporazumima oko ovlaštenja koja pojedinac ima (Amro & Gkioulos, 2023). Evaluacija uspješnosti ovakvih programa nije trivijalna. Potrebno je definisati metrike koje mjere promjenu nivoa svijesti zaposlenih o bezbjednosnim pitanjima kroz vrijeme. Testovi prije i poslije treninga mogu ocijeniti stepen usvojenog znanja, dok simulirane phishing kampanje daju praktičnu mjeru otpornosti organizacije na socijalno-inženjerske napade. Ako veliki procenat zaposlenih nastavi da nasjeda na simulirane prijetnje nakon više ciklusa obuke, to ukazuje na potrebu za promjenom metodologije i sadržaja. Zaposleni koji direktno rukuju kritičnim resursima, administratori sistema, operateri SCADA okruženja ili zaposleni sa pristupom osjetljivim bazama podataka, zahtijevaju specijalizovane programe edukacije fokusirane na njihove specifične zadatke i rizike. Ovi programi moraju sadržati tehničke detalje o sigurnosnim konfiguracijama, procedurama oporavka iz backupa, forenzičkom očuvanju dokaza nakon incidenta i radu pod pritiskom kada dođe do prekida servisa (n.a, 2009). Takva specijalizovana znanja dopunjuju opšte treninge koje prolaze svi zaposleni. Još jedan aspekt koji se sve više primjenjuje jeste saradnja sa osiguravajućim društvima i partnerima iz industrije radi kreiranja obrazovnog materijala zasnovanog na realnim primjerima incidenata koji su pogodili kompanije sličnog profila (Adriko & Nurse, 2024). Ovi materijali pomažu zaposlenima da uoče konkretne posljedice loše prakse zaštite informacija po finansijsko stanje firme i sopstvene radne procese. Studije slučaja daju dodatnu težinu teorijskim konceptima time što ih stavljaju u opipljiv poslovni kontekst. U sredinama MSP ograničeni budžeti često zahtijevaju odabir optimalnih formata obuke koji balansiraju između troškova i efekta. Online treninzi kombinovani sa povremenim radionicama uživo pokazuju se kao efikasno rješenje koje omogućava širem krugu zaposlenih pristup edukaciji bez značajnog narušavanja produktivnosti. Istovremeno se koriste jednostavni alati za praćenje napretka, evaluacioni kvizovi, bodovni sistemi ili certifikati završetka kursa koji motivišu učesnike da aktivno učestvuju. Treba istaći da programi nisu samo tehnički orijentisani, jedan dio sadržaja mora pokriti regulatorne aspekte bezbjednosti informacija kako bi osoblje razumjelo zakonske obaveze koje organizacija ima prema standardima poput ISO 27001 ili okvirima NIST-a (Khlaponin, et al., 2022). Povezivanje pravnih zahtjeva sa konkretnim internim procedurama povećava kredibilitet obuke kod zaposlenih, jer oni vide jasnu vezu između

propisa, rizika kazni ili gubitka reputacije i sopstvenog ponašanja. Rezultati istraživanja ukazuju da su organizacije koje investiraju u dobre strukturne programe obuke otpornije na incidente izazvane ljudskom greškom te ostvaruju bolji rezultat u metrikama kao što su MTTD i MTTR tokom sajber incidenata (Tetteh, 2024). Brža detekcija se postiže jer zaposleni znaju prepoznati rane signale kompromitacije sistema i skraćeno vrijeme odgovora rezultat je poznavanja procedura izolacije pogođenog dijela sistema dok tehnički tim ne izvrši sanaciju. Konačno, važno je naglasiti međuzavisnost između edukativnog sloja zaštite i svih ostalih tehnoloških slojeva Defense in Depth okvira. Obuka ne može postojati izdvojeno, ona mora biti integrisana sa tehničkim mjerama koje pokrivaju perimetarsku zaštitu, unutrašnju kontrolu pristupa, autentifikaciju korisnika te monitoring aktivnosti mreže (Amro & Gkioulos, 2023). Na taj način ponašanje zaposlenih postaje nastavak formalnih pravila implementiranih kroz tehnologiju, a ne paralelni proces koji funkcioniše nezavisno od nje. Samo takva integrisana strategija može dati puni efekat višeslojne zaštite gdje svaki dio, bilo softver, hardver ili ljudski faktor, istovremeno štiti informacioni sistem od potencijalnih prijetnji.

3.3.2. Kultura sajber bezbjednosti

Kultura sajber bezbjednosti u kontekstu slojevite strategije odbrane ima ulogu stvaranja zajedničkog stava, navika i procedura unutar organizacije kojima se svakodnevno promoviše sigurno ponašanje u radu sa informacionim sistemima. Ona obuhvata koordinisano djelovanje tehnologije, procesa i ljudi, pri čemu svi zaposleni, od rukovodstva do krajnjih korisnika, preuzimaju aktivnu odgovornost za očuvanje povjerljivosti, integriteta i dostupnosti podataka. Takva kultura ne nastaje spontano, ona se gradi postepeno kroz formalne i neformalne mehanizme, politike i edukativne programe kako bi sigurnosne prakse postale dio svakodnevne poslovne rutine, a ne ad-hoc reakcija na incidente. Za razliku od izolovanih tehničkih kontrola koje mogu biti percipirane kao prepreka produktivnosti, snažna kultura sajber bezbjednosti integriše te kontrole u operativne tokove tako da njihova primjena djeluje prirodno. Kada se, na primjer, MFA posmatra kao standardna procedura rada umjesto posebnog zahtjeva IT sektora, korisnici je prihvataju sa manjim otporom, povećavajući time efikasnost ovog sloja odbrane. Isto važi za segmentaciju mreže i pravila kontrole pristupa; ako su zaposleni svjesni razloga zbog kojih određene resurse ne mogu vidjeti ili koristiti bez validacije svojih privilegija, smanjuje se sklonost traženju zaobilaznih puteva koji kompromituju sigurnost sistema. Središnji element razvoja kulture sajber bezbjednosti je

stalna komunikacija o prijetnjama i odgovorima na njih. Nije dovoljno oslanjati se na periodične treninge, potrebno je uspostaviti kanale brze razmjene informacija između timova zaduženih za sigurnost i ostatka organizacije (Arthur et al., 2023). To može uključivati interne biltene sa pregledom aktuelnih sajber prijetnji koje su relevantne za sektor u kojem organizacija posluje, kratke smjernice o novim procedurama ili prezentacije forenzičkih rezultata nakon incidenata kako bi se pokazalo gdje je zaštita funkcionisala dobro, a gdje postoje slabosti. Direktan kontakt sa iskustvima iz stvarnog okruženja pojačava percepciju realnog rizika kod korisnika. Liderstvo igra kritičnu ulogu u formiranju ove kulture, jer uprava mora jasno demonstrirati da su principi bezbjednosti sastavni dio poslovnih ciljeva (Ejjami, 2024). Kada rukovodioci dosljedno sprovode sopstvene modele bezbjednog ponašanja i insistiraju na poštovanju politika zaštite, šalje se signal ostatku organizacije da su sigurnosni zahtjevi obaveza jednako važna kao i drugi poslovni prioriteti. Budžetske odluke također reflektuju stav prema kulturi bezbjednosti, alokacija sredstava za redovnu edukaciju korisnika ili unapređenje mehanizama perimetarske zaštite pokazuje planski pristup umjesto reaktivnog trošenja nakon incidenta (Neri, et al., 2022). Edukacija ostaje temelj izgradnje kulture sajber bezbjednosti, ali njen sadržaj mora biti prilagođen kontekstu rada organizacije (Amro & Gkioulos, 2023). Opšte teme poput phishing-a daju osnovnu otpornost korisnicima na najrasprostranjenije prijetnje, dok specijalizovane obuke pokrivaju procedure kritične pozicije, na primjer administratori sistema prolaze detaljne module o upravljanju privilegijama i incident response protokolima. Mikro segmentiranje sadržaja edukacije prema potrebama svake grupe zaposlenih doprinosi efektivnosti programa jer polaznici imaju direktnu primjenjivost naučenog na vlastiti posao. Organizacije sa razvijenom kulturom sajber bezbjednosti često koriste simulirane incidente kako bi testirale reakcije zaposlenih na koordinisane napade (Almoaigel & Abuabid, 2023). Rezultati ovih simulacija služe kao praktični feedback alat koji pokazuje koliko dobro tehnički slojevi odbrane funkcionišu u kombinaciji sa ljudskim faktorom. Ako IDS/IPS sistemi signaliziraju pokušaj upada, a osoblje ne reaguje pravilno zbog nedostatka znanja ili nepovjerenja u alarme, tehnološki sloj gubi svoju vrijednost i istovremeno pokazuje potrebu za dodatnim obrazovanjem i jačanjem povjerenja u sisteme detekcije. Postepenim uklapanjem procedura kao što su brza prijava sumnjivih aktivnosti IT timu ili verifikacija identiteta prije odobravanja transakcija visoke vrijednosti, organizacija oblikuje mentalitet proaktivnog djelovanja kod zaposlenih. Proaktivnost smanjuje trajanje napadačkih sesija, jer raniji signali upozorenja dovode do

prekida aktivnosti napadača prije nego što on postigne cilj. Na taj način kultura sajber bezbjednosti služi kao vitalan sloj unutar Defense in Depth strategije koji štiti mostove između tehnoloških barijera i osigurava da oni nisu samo pasivne strukture već aktivno korišteni alati zbog kojih napadaču izmiče mogućnost eksploatacije ljudske slabosti. U okruženjima MSP razvijanje ove kulture nosi posebne izazove, jer manji broj zaposlenih često preuzima višestruke zadatke (Adriko & Nurse, 2024). U takvom kontekstu može biti teško izdvojiti vrijeme za formalnu edukaciju ili evaluaciju politika zaštite pa zato se preporučuje integrisanje kratkih sigurnosnih podsjetnika u dnevne radne zadatke putem internog softverskog okruženja ili komunikacionih platformi koje već koriste svi zaposleni. Ovakva taktika održava stalnu prisutnost teme bezbjednosti bez prevelikog narušavanja produktivnosti. Prakse koje podstiču zajedničku odgovornost uključuju transparentno izvještavanje o sigurnosnim metrikama – na primjer broj spriječenih pokušaja upada ili prosječno vrijeme detekcije incidenata tokom prethodnog kvartala (n.a., 2009). Objavljivanje tih podataka motiviše timove da poboljšavaju statistiku kroz bolju koordinaciju svojih aktivnosti sa tehničkim segmentima zaštite. Istovremeno otvara diskusiju o tome koji aspekti zahtijevaju poboljšanje i daje jasnu vezu između ljudskog doprinosa i konkretnih rezultata sistema odbrane. Na kraju, održavanje kulture sajber bezbjednosti mora biti dugoročna strategija koju podržavaju svi slojevi Defense in Depth modela, perimetarska zaštita filtrira početne prijetnje, unutrašnja kontrola pristupa ograničava domen potencijalnog napadača, autentifikacija potvrđuje legitimnost korisnika pri svakoj interakciji sa sistemom, dok proaktivno ponašanje zaposlenih zatvara mnoge vektore koji bi inače mogli zaobići tehničke barijere. Tek tada svaki sloj funkcioniše kao dio koherentnog ekosistema gdje tehnološke i ljudske komponente rade sinhronizovano na prevenciji kompromitovanja informacionog sistema.

3.4. Redundantnost i oporavak od katastrofe

Redundantnost i oporavak od katastrofe predstavljaju ključne komponente savremenih strategija za osiguranje kontinuiteta poslovanja. Implementacijom redundantnih sistema, resursa i komunikacionih veza smanjuje se rizik od prekida rada uslijed tehničkih kvarova, prirodnih nepogoda ili sajber incidenata. Pored toga, pouzdani mehanizmi sigurnosnog kopiranja podataka (backup) omogućavaju očuvanje kritičnih informacionih resursa i predstavljaju osnovu za efikasan oporavak sistema. Integracijom backup rješenja sa planovima oporavka od katastrofe organizacijama se omogućava obnova kritičnih servisa i

podataka u definisanom vremenskom okviru, čime se osigurava dostupnost informacionih sistema i stabilnost poslovnih procesa.

3.4.1. Backup strategije

Backup strategije unutar slojevite odbrane u informacijskoj sigurnosti imaju zadatak da obezbijede kontinuiranu dostupnost i integritet poslovno kritičnih podataka čak i nakon događaja koji ugrožavaju primarne sisteme. U kontekstu višeslojne zaštite, one predstavljaju sloj redundancije koji se aktivira kada preventivne i detekcione mjere nisu mogle u potpunosti spriječiti ili neutralisati incident. Ovakav sloj povezuje tehničke mehanizme poput perimetarske kontrole sa organizacionim procedurama oporavka kako bi se minimizirao prekid rada i izbjegla trajna šteta. Efektivna backup strategija u okviru Defense in Depth pristupa ne oslanja se na jednu jedinu kopiju podataka, već podrazumijeva višestruke instance pohranjenih informacija na različitim lokacijama. Redundantna pohrana može uključivati on-site kopije za brzi oporavak, off-site fizičke medije ili udaljene cloud repozitorijume sa jakim kontrolama pristupa i enkripcijom (Kello, 2022). Na tehničkom nivou, rutina izrade ovih kopija mora biti automatizovana i planirana tako da pokrije sve segmente sistema, od baza podataka, preko konfiguracionih datoteka, do korisničkih podataka, jer incident kompromitacije ne bira vektor napada prema kritičnosti resursa. Integracija backupa sa politikama sigurnosnog upravljanja podrazumijeva definisanje jasnog rasporeda izrade kopija (dnevni, sedmični, mjesečni ciklusi) uz diferencijalne ili inkrementalne metode kako bi se optimizovala potrošnja prostora bez smanjenja nivoa zaštite. Organizacije koje čuvaju podatke od vitalnog značaja treba da implementiraju politiku verzionisanja, zadržavanje više generacija istog fajla ili baze, kako bi mogle vratiti sistem na stanje prije eksploatisanja ranjivosti (Amro & Gkioulos, 2023). Ovim se direktno adresira princip integriteta, jer se kompromitovane verzije mogu izolovati, a validne vraćati u produkciju. Posebno je važno da rezervne kopije budu obezbijeđene istim ili višim nivoom zaštite u poređenju sa izvornim sistemima. To uključuje primjenu snažne enkripcije nad podacima u mirovanju, ograničenje privilegija pristupa backup skladištima prema principu najmanjih ovlaštenja, te autentifikaciju prije svakog pokušaja povrata podataka. Ove kontrole sprečavaju scenarije u kojima napadač ne pokušava direktnu kompromitaciju produkcionog sistema već cilja backupe sa ciljem da onemogući oporavak ili pronađe nekriptovane osjetljive informacije. Unutar slojevite arhitekture, strategije backup-a povezane su i sa segmentacijom mreže opisanom ranije,

skladišta rezervnih kopija često se izdvajaju u zasebne sigurnosne zone koje nemaju direktan dvosmjerni pristup prema glavnoj operativnoj mreži (Kuipers & Fabro, 2006). IDS/IPS sistemi na međuspojevima tih zona prate sav promet prema backup resursima radi detekcije anomalija poput neočekivanog velikog prijenosa ili pristupa van predviđenih ciklusa. Za okruženja MSP izazov implementacije leži u balansiranju troškova i efikasnosti backupa (Ejjami, 2024). Cloud rješenja nude privlačnu alternativu investicijama u lokalnu infrastrukturu za pohranu, ali međutim ona nose zavisnost o bezbjednosnim praksama trećih strana. Tehnike hardverski podržanog povjerljivog računarstva (TEE) mogu ublažiti ovaj rizik enkripcijom na klijentskoj strani i procesiranjem šifrovanih podataka unutar pouzdanih okruženja host-ovanih kod provajdera (Bartock, et al., 2021). Time se kombinacija redundantnosti i zaštite povjerljivosti integrira u jedan sloj odbrane. Verifikacija rezervnih kopija mora biti sastavni dio strategije, a redovna testiranja povrata potvrđuju da procedure obnove funkcionišu ispravno kada dođe do potrebe za aktivacijom (Novianto, 2020). Greške prilikom vraćanja često ostanu neotkrivene sve dok incident ne prisili organizaciju na korištenje backup-a, a tada je već kasno za korekciju nedostatka ako ne postoje proaktivne provjere svih funkcionalnih segmenata procesa obnove. Testiranje uključuje djelimičan restore pojedinačnih fajlova kao i kompletan recovery kritičnih servisa radi procjene vremena oporavka i tačnosti obnovljenih podataka (Recovery Point Objective, u daljem tekstu: RPO). Raznovrsnost prijetnji prema dostupnosti diktira potrebu da backup politika pokrije scenarije od tehničkih kvarova do koordinisanih sajber napada poput ransomwarea (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). U slučaju ransomware infekcije, sposobnost povratka poslovanja zavisi od toga da li su rezervne kopije izolovane od glavnog sistema tokom incidenta, tzv. „air-gap" strategija čuva offline kopiju koja nije dostupna preko mreže pa je time imunizovana na kriptovanje od strane malicioznog koda. U skladu sa Defense in Depth filozofijom, backup sloj sarađuje sa monitoring sistemima prateći parametre performansi skladišta kao što su kapacitet i propusnost (Amro & Gkioulos, 2023). Automatizovani alarmi za manjak prostora ili neuspjele sesije izrade kopija omogućavaju timovima da preduzmu korektivne akcije prije nego što manjak kapaciteta ili tehnička greška ugroze kontinuitet zaštitnog sloja. Integracija ovih parametara u SIEM omogućava korelaciju između događaja vezanih za backup sisteme i šireg konteksta sigurnosnih incidenata koji bi mogli zahtijevati hitan restore. Edukacija osoblja o pravilnoj upotrebi procedura kreiranja i povrata kopija predstavlja ljudski aspekt ovog sloja (Tetteh, 2024). Čak i najnaprednije tehničke implementacije mogu zakazati ako administratori

ne razumiju sekvencu koraka potrebnu za brz oporavak ili ignorišu pravila izolacije backup medija radi praktičnosti prijenosa podataka. Treninzi moraju pokriti regulatorne zahtjeve za čuvanje rezervnih kopija posebno kod sektora s visokim nivoom zaštite informacija, kao što su finansijski sistemi, zdravstvene ustanove, i raditi poboljšanja učeći na tuđim greškama, to jest analizirajući stvarne incidente koji su pogodili slične organizacije (Enitan, 2025). Ključna prednost dobro dizajniranih backup strategija unutar Defense in Depth okvira jeste njihova sposobnost da očuvaju funkcionalnost poslovnih procesa čak i kada višestruki drugi slojevi zakažu. Povezanost ovog sloja sa perimetarskom zaštitom, kontrolom pristupa, segmentacijom mreže i monitoringom stvara situaciju gdje rezerva nije pasivni resurs već aktivni dio sigurnosnog ekosistema spreman da preuzme teret operativnog rada u trenutku kompromitovanja primarnog sistema. Ovakva integrisana redundancija smanjuje ukupnu površinu napada tako što otežava protivniku postizanje dugotrajnog efekta, čak ako uspješno probije inicijalne barijere, pokušaj uništenja backupa naići će na dodatni zid tehničkih kontrola, proceduralnih ograničenja i ljudskog nadzora koji zajedno zatvaraju krug Defense in Depth strategije zaštite informacija.

3.4.2. Planovi kontinuiteta poslovanja

Planovi kontinuiteta poslovanja predstavljaju strateški okvir koji omogućava organizaciji da očuva osnovne poslovne funkcije u uslovima ozbiljnih poremećaja izazvanih tehničkim kvarovima, sajber napadima ili fizičkim katastrofama. Unutar koncepta višeslojne odbrane oni popunjavaju kritičan dio „reaktivnog“ sloja, koji se aktivira kada preventivne i detekcione mjere opisane ranije nisu uspjele u potpunosti neutralisati incident. Cilj je omogućiti nesmetan ili barem ograničeno funkcionalan rad ključnih procesa dok se ne izvrši potpuna sanacija sistema (Brantly, 2018). Takvi planovi nisu samo dokumenti već integrisana procedura koja povezuje tehničke, proceduralne i ljudske resurse radi smanjenja zastoja i sprečavanja eskalacije štete. Jedna od osnova planiranja kontinuiteta je prethodno sprovedena procjena rizika i analiza uticaja na poslovanje (Business Impact Analysis, u daljem tekstu: BIA). Ove aktivnosti identifikuju koji procesi imaju prioritet pri obnovi i definišu maksimalno prihvatljivo vrijeme prekida (Maximum Tolerable Downtime, u daljem tekstu: MTD) te ciljno vrijeme oporavka (RTO) i ciljni gubitak podataka (RPO). Metrike poput RTO i RPO značajne su jer direktno određuju prirodu kontrolnih mehanizama koji će biti uključeni u plan, na primjer kraći RTO zahtijeva visoku redundanciju infrastrukture, dok nizak RPO

sugeriše učestale replikacije podataka (Christen et al., 2020). U Defense in Depth kontekstu ovi parametri moraju biti kompatibilni sa drugim slojevima zaštite, perimetarske mjere trebaju štititi zamjenske/rezervne lokacije, a kontrola pristupa treba obuhvatiti i kriznu infrastrukturu. Tehnička realizacija planova kontinuiteta poslovanja često uključuje uspostavljanje alternativnih lokacija rada (hot site, warm site, cold site), pri čemu se hot site koncipira kao potpuno opremljena operativna jedinica spremna za preuzimanje posla unutar nekoliko sati, dok cold site nudi samo osnovnu infrastrukturu koju treba naknadno opremiti. Izbor zavisi od budžeta i nivoa rizika prihvatljivog organizaciji (Adriko & Nurse, 2024). U okruženjima MSP pragmatičan pristup može biti hibridna kombinacija lokalne redundantne opreme sa cloud servisima koji služe kao dodatni sloj sigurnosnog kapaciteta. Time se koristi efekt skalabilnosti cloud okruženja uz zadržavanje kontrole nad kritičnim funkcijama koje ostaju on-premise. Integracija plana kontinuiteta sa backup strategijama opisanima ranije omogućava koherentan prelaz iz faze incidenta u fazu obnove (Neri, et al., 2022). Rezervne kopije koje se izrađuju prema definisanim ciklusima postaju osnova za brzo vraćanje sistema na predincidentno stanje. Za razliku od pasivne upotrebe backupa tek nakon velikog prekida, proaktivan Business Continuity Plan (u daljem tekstu: BCP) predviđa redovne vježbe kompletnog prebacivanja operacija na alternativnu platformu korištenjem tih kopija. Ovo testiranje mora uključivati verifikaciju integriteta podataka i kompatibilnosti aplikacija sa kriznim okruženjem radi otkrivanja mogućih tehničkih neusklađenosti na vrijeme. Segmentacija mreže, kao jedan od drugih slojeva zaštite, ima relevanciju i ovdje krizni mod rada može zahtijevati izolaciju pogođenih segmenata dok ostatak mreže nastavlja funkcionisanje (Amro & Gkioulos, 2023). ACL pravila u takvim situacijama dinamički se proširuju ili sužavaju kako bi omogućila nužnu komunikaciju između rezervnih instanci servisa bez ponovnog izlaganja sistema vektoru napada koji je izazvao prvobitni incident. IDS/IPS sistemi prate kriznu infrastrukturu s jednakom pažnjom kao i primarno okruženje, a njihova konfiguracija tokom prelaza na BCP režim mora biti usklađena sa novim topološkim rasporedom mreže. Planovi kontinuiteta uključuju i koordinaciju ljudskih resursa. Svi zaposleni moraju znati svoje uloge tokom krize, od IT administratora koji obnavljaju sisteme do krajnjih korisnika koji možda moraju privremeno raditi prema modifikovanim procedurama (Tetteh, 2024). Obuka za BCP nije izolovana od ukupne kulture sajber bezbjednosti, a ona je proširenje principa osvješćivanja zaposlenih koje im daje sigurnost u vlastitu sposobnost reagovanja kada standardni tok rada bude poremećen (Neri, et al. 2022).

Ponašanje ljudi tokom incidenta često odlučuje hoće li tehničke mjere ispuniti svoju svrhu, zato simulacije prelaska na krizni režim moraju testirati i tehniku i interpersonalnu koordinaciju. Komunikacijski protokoli dio su svakog kvalitetnog plana kontinuiteta, osiguravajući da informacije o statusu sistema budu pravovremeno dostupne ključnim akterima bez izlaganja potencijalnim napadačima. To znači upotrebu sigurnih kanala (VPN sa MFA) za internu komunikaciju te prethodno pripremljene javne izjave za klijente ili partnere radi održavanja reputacije firme tokom prekida usluga (Enitan, 2025). Transparentnost prema partnerima i korisnicima uz kontrolisano upravljanje informacijama smanjuje konfuziju i spekulacije. Regulatorna usklađenost još je jedan važan element, posebno u sektorima poput finansija ili zdravstva gdje BCP mora uključivati garancije povjerljivosti podataka čak i tokom vanrednog rada (Adriko & Nurse, 2024). To zahtijeva da rezervne lokacije i krizna oprema zadovoljavaju iste standarde enkripcije, kontrole pristupa i audita kao glavno okruženje. Auditorski trag aktivnosti u toku incidenta pomaže ne samo forenzičkoj analizi već pruža dokaz regulatornim tijelima da su procedure sprovedene kako nalažu standardi poput ISO 27001 ili okviri nacionalnih agencija za sajber bezbjednost. Testiranje planova kontinuiteta mora biti ciklično, najmanje jednom godišnje, kako bi se provjerila aktuelnost svih komponenti u odnosu na promjene u infrastrukturi, kadrovskim resursima ili poslovnom modelu. Tokom tih proba bilježe se mjerenja kao što su stvarno vrijeme prelaska na sekundarnu lokaciju naspram definisanog RTO-a, stopa uspjeha vraćanja kritičnih aplikacija te broj tehničkih/incidentskih prepreka koje su naišle tokom procesa. Ti rezultati služe prilagođavanju konkretnih procedura, ali često otkriju potrebu za dodatnim obukama osoblja ili investicijama u automatske failover sisteme. U kontekstu MSP ograničen budžet ne znači nužno slabiji kvalitet plana kontinuiteta ako je on pažljivo prioritetizovan prema rezultatima BIA. Fokusiranje resursa na najkritičnije procese, uz minimalne varijante alternativa poput rada iz udaljenog cloud okruženja putem VPN-a, može zadržati osnovnu funkcionalnost dok traju napori vraćanja punog operativnog kapaciteta (Ejjami, 2024). Iako manje firme nemaju luksuz održavanja potpuno paralelnih infrastruktura, one mogu koristiti geografski distribuirane servise trećih strana uz prilagođene procedure integracije s postojećim sistemom. Na kraju, efikasan plan kontinuiteta poslovanja unutar Defense in Depth arhitekture mora funkcionisati sinhrono sa svim ostalim slojevima zaštite, perimetarskom kontrolom koja filtrira prijetnje ka rezervnoj lokaciji, unutrašnjim pravilima pristupa prilagođenim kriznom modusu rada, sistemima autentifikacije koji verifikuju legitimnost aktera uključenih u sanaciju te

monitoringom koji prati nove instance servisa odmah po njihovoj aktivaciji. Tek ovakvim povezivanjem preventivnih, detekcionih i reaktivnih slojeva stvara se koherentan sigurnosni ekosistem sposoban da apsorbuje udar incidenata bez potpunog kolapsa poslovanja (Author, 2009).

3.4.3. Planovi kontinuiteta poslovanja

Testiranje oporavka sistema unutar višeslojne strategije odbrane predstavlja proces provjere sposobnosti organizacije da povrati funkcionalnost svojih digitalnih resursa nakon različitih vrsta incidenata, uključujući sajber napade, tehničke kvarove i prirodne katastrofe. Dok planovi kontinuiteta poslovanja definišu „šta“ treba uraditi u kriznoj situaciji, testiranje oporavka potvrđuje „da li“ te procedure zaista funkcionišu u predviđenom vremenu i sa očekivanim efektima. Ovaj oblik evaluacije povezuje preventivne i reaktivne slojeve Defense in Depth arhitekture kako bi se osiguralo da redundancija infrastrukture ne ostane samo teoretski resurs, već spreman i pouzdan alat za ponovnu uspostavu rada sistema. Testiranja obuhvataju više tipova pristupa. Jedan od temeljnih je tzv. „full-scale recovery test“, tokom kojeg se kompletna operativna okruženja startuju iz rezervnih kopija na alternativnu ili sekundarnu lokaciju. Ovakva proba direktno verifikuje parametre RTO i RPO definisane u procedurama kontinuiteta. Ako procedura nalaže vraćanje ključnih aplikacija u roku od šest sati uz maksimalni gubitak podataka od jednog sata starosti, procjena stvarnog vremena povratka i tačnosti obnovljenih podataka pokazuje koliko je sistem sposoban da ispuni taj standard. Pored potpunih simulacija, praktikuju se i „partial recovery tests“ kod kojih se obnavljaju samo kritični servisi ili definisani podsistemi radi ubrzane verifikacije specifičnih slojeva odbrane. Tehnički segment testiranja oporavka sistema uključuje validaciju integriteta rezervnih kopija (Amro & Gkioulos, 2023). Kriptografske hash funkcije ili digitalni potpisi koriste se za provjeru da li se podaci vraćeni iz backupa poklapaju sa originalnom verzijom nastalom prije incidenta. Na taj način se potvrđuje da nije došlo do „tihe korupcije“ sadržaja zbog hardverskih ili softverskih grešaka. IDS/IPS sistemi postavljeni oko backup zona prate sve komunikacione tokove tokom procesa vraćanja radi detekcije eventualnog malicioznog koda ubačenog tokom ili prije incidenta (Kuipers & Fabro, 2006). Ako sigurnosni slojevi otkriju anomaliju, procedura predviđa izolaciju kompromitovane kopije i vraćanje iz druge generacije verzionisanih podataka. Slojeviti pristup znači da testiranje ne može biti ograničeno na provjeru samog čina obnove, već mora obuhvatiti koordinaciju između perimetarske zaštite,

unutrašnjih pravila pristupa, autentifikacije korisnika, segmentacije mreže i monitoring sistema (Ejjami, 2024). Tokom prelaska na krizni mod rada firewall pravila se privremeno redefinišu kako bi omogućila potrebnu komunikaciju prema rezervnim instancama servisa, međutim unutrašnja kontrola pristupa mora zadržati restriktivne parametre kako potencijalni vektor prijetnje iz incidenta ne bi bio prenesen na novopodignutu infrastrukturu. MFA ostaje obavezna na upravljačkim interfejsima čak i tokom hitnog rada, čime se sprečava neovlašteno upravljanje oporavljenim sistemima. Praktična provedba testiranja zahtijeva jasne scenarije koji imitiraju realne izvore prekida rada (Tetteh, 2024). Simulacija ransomware napada može početi blokiranjem pristupa primarnim servisima i aktiviranjem izolovanih offline kopija prema politici air-gap zaštite (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Drugi scenario modelira fizičko oštećenje servera zbog havarije napajanja, tada nastupa preusmjeravanje aplikacija ka hot site lokaciji konfiguriranoj tako da replicira produkciono okruženje. U oba slučaja mjerena su stvarna vremena povrata funkcionalnosti i analizirane tehničke barijere koje su nastale tokom transfera podataka. Testiranje mora provjeravati otpornost na tzv. kaskadne kvarove. To su situacije kada inicijalna greška izaziva niz povezanih problema kroz zavisne komponente sistema, na primjer kompromitacija jedne baze utiče na rad aplikacionog sloja koji potom blokira drugi servis potreban za obnovu podataka. Defense in Depth filozofija nalaže da redundantni mehanizmi budu dovoljno autonomni kako bi nastavili rad čak i u takvom scenariju, verifikacija te autonomije tokom testiranja otkriva slabosti projektovanja slojeva. U kontekstu MSP ograničeni kapaciteti traže optimizovane metode testiranja koje neće previše ometati svakodnevno poslovanje (Adriko & Nurse, 2024). To može značiti raspodjelu simulacija tokom godine, jer manji kvartalni testovi fokusirani na pojedinačne komponente (npr., restore baze klijenata) i godišnji sveobuhvatni test kriznog prelaska cjelokupnog IT ekosistema. Cloud rješenja uvode dodatne varijable, provajderi moraju biti uključeni u testne protokole kako bi omogućili brzi pristup backupima ili aktiviranje rezervnih instanci servera u skladu sa ugovorenim SLA (Service Level Agreement) parametrima. Evaluacija obuhvata kvalitativne i kvantitativne metrike; osim formalnog ispunjenja RTO/RPO ciljeva mjeri se koordinacija timova, jasnoća komunikacijskih protokola, efikasnost sigurnosnih slojeva u sprečavanju transfera prijetnji na novopodignute sisteme te sposobnost korisnika da rade prema kriznim procedurama bez narušavanja bezbjednosnog statusa okruženja (Ejjami, 2024). Rezultati pomažu reviziji postojećeg plana kontinuiteta, ali mogu otvoriti potrebu za jačanjem pojedinih slojeva Defense in Depth ekosistema, na primjer

unapređenje segmentacije mreže između produkcionih i kriznih zona ako je utvrđeno curenje podataka tokom prelaza. Naposljetku, kontinuitet efektivnosti zahtijeva cikličko ponavljanje ovih proba uz prilagodbu novim infrastrukturnim promjenama, pojavi novih vektora prijetnji ili reorganizaciji poslovnih procesa (n.a., 2009). Time se osigurava da sistemska otpornost nije statičan atribut već dinamičan rezultat stalne interakcije tehničkih kontrola, ljudskih procedura i strategijske koordinacije svih slojeva višeslojne zaštite informacija.

3.5. Nadzor i nadgledanje

Nadzor i nadgledanje predstavljaju važan sloj Defense in Depth strategije, čija je svrha kontinuirano praćenje aktivnosti unutar informacionih sistema radi pravovremene detekcije sigurnosnih incidenata. Ovaj sloj omogućava identifikaciju sumnjivih obrazaca ponašanja, neovlaštenih aktivnosti i potencijalnih prijetnji koje nisu spriječene prethodnim sigurnosnim mjerama.

Primjena SIEM sistema, real-time monitoringa i analitike bezbjednosnih događaja omogućava centralizovano prikupljanje, korelaciju i analizu sigurnosnih zapisa iz različitih izvora. Time se značajno unapređuje sposobnost organizacije da brzo reaguje na incidente, smanji vrijeme detekcije i osigura efikasno upravljanje informacionom sigurnošću.

3.5.1 SIEM sistemi

SIEM sistemi predstavljaju složene platformske mehanizme za prikupljanje, korelaciju, analizu i prikaz bezbjednosnih događaja iz različitih izvora unutar informacionog okruženja. Njihova uloga u višeslojnom okviru odbrane jeste da objedinjavaju podatke iz perimetarskih kontrola, unutrašnjih mehanizama pristupa, autentifikacije korisnika, segmentacije mreže i drugih zaštitnih slojeva kako bi se formirao jedinstven pogled na stanje sigurnosti. Time se omogućuje brža detekcija prijetnji koje se manifestuju kroz disperzne indikatore, anomalije koje izolovano ne bi nužno signalizirale incident postaju jasne kada se posmatraju zajedno. Tehnička arhitektura SIEM sistema obično uključuje komponente za prikupljanje podataka (log collection agents), centralno skladištenje događaja, mehanizam za obradu i normalizaciju zapisa različitih formata, korelacioni engine koji povezuje događaje u šire obrasce ponašanja, te interfejs za vizuelizaciju i alerting. Prikupljanje podataka može obuhvatati firewall logove, IDS/IPS zapise o detektovanim napadima, sistemske logove operativnih sistema, audit tragove pristupa bazama podataka, kao i događaje iz aplikacija. Ovaj aspekt direktno prati filozofiju

Defense in Depth strategije gdje svaki zaštitni sloj generiše vlastitu telemetriju, SIEM služi kao integraciona tačka koja tu raznovrsnost pretvara u homogen skup informacija spreman za analitičku obradu. Korelacioni engine je srce SIEM-a. On primjenjuje različite metode analize, od jednostavnih pravila baziranih na potpisima poznatih napada do naprednih statističkih modela i heurističkih algoritama, radi identifikacije lančanih događaja koji upućuju na koordinisane aktivnosti protiv infrastrukture. Primjer takve korelacije mogao bi biti kombinacija neuspjelih pokušaja autentifikacije administrativnog naloga u web konzoli, zatim pokušaj pristupa segmentu mreže s ograničenim privilegijama, pa neočekivani transfer velikih količina podataka prema eksternoj adresi. Svaki od tih signala pojedinačno možda ne bi izazvao uzbunu u perimetarskom firewall-u ili sistemu kontrole pristupa, tek zajednički obrazac otkriva suštinu incidenta. Vizuelni interfejs SIEM sistema nije samo estetski dodatak, već je njegova svrha operativna. Pregled grafova o distribuciji incidenata po vremenu ili zoni mreže pomaže operatorima da brzo odrede prioritet reagovanja. Widget-i i dashboard komponente mogu se prilagoditi tako da fokusiraju kritične resurse ili geografske oblasti važnosti organizaciji. Integracija alerting funkcionalnosti znači da korelacioni engine pri detekciji ozbiljnog obrasca automatski šalje obavještenje putem email-a, SMS-a ili povezivanjem sa incident response sistemom koji pokreće skripte izolacije pogođenog segmenta. U kontekstu MSP upotreba open-source SIEM rešenja poput Wazuh-a, OSSIM-a ili Elastic Security nudi kompromis između budžetske održivosti i funkcionalnosti. Većina ovih sistema podržava modularno proširenje plug-inovima za specifične vektore prijetnji te mogućnost integracije sa postojećim alatima za perimetarsku zaštitu i unutrašnju kontrolu pristupa. Korištenjem otvorenog koda moguće je prilagoditi pravila korelacije lokalnim potrebama, npr. fokusiranje na ICS specifične protokole unutar industrijskog pogona ili filtriranje upozorenja prema regulatornim zahtjevima sektora rada. Ovo je važno jer MSP često rade sa kombinacijom standardne IT infrastrukture i specijalizovanih OT komponenti koje zahtijevaju poseban nadzor. SIEM sistemi imaju direktnu vezu sa prethodno opisanim slojevima višeslojne zaštite. Firewall sistemi kao perimetarska linija šalju logove o blokiranim konekcijama. IDS/IPS sistemi prosljeđuju informacije o pokušajima eksploatacije ranjivosti, a kontrola pristupa bilježi promjene privilegija korisnika, MFA evidencije registruju neuspjele verifikacione procedure, dok backup slojevi generišu zapisnike o problemima sa kreiranjem sigurnosnih kopija, a segmentacija mreže doprinosi indikatorima neautorizovanog prelaska između zona. SIEM objedinjavanjem svih tih izvora kreira centralizovanu situacionu svijest

neophodnu za pravovremeno reagovanje. Integracija SIEM-a unutar Defense in Depth strategije osigurava da ni jedan sloj ne ostane izolovan informacijski tokom incidenta (Boggs et al.,2019). Na primjer, ako IPS blokira paket koji krši pravilo protokola u DMZ, ali napadač zatim uspješno koristi socijalno-inženjersku metodu da dobije VPN pristup iznutra, SIEM može povezati oba događaja i označiti ih kao dio iste prijetnje, čime se izbjegava fragmentisan pogled koji bi potencijalno usporio reakciju. Ovakvo sagledavanje omogućava da tehničke mjere poput brze izolacije naloga ili zatvaranja segmenata mreže budu pokrenute na osnovu kompletne slike prijetnje umjesto parcijalne percepcije jednog sloja odbrane. U implementaciji kod MSP posebno treba voditi računa o razmjeni prikupljenih podataka i dostupnim kapacitetima za njihovu obradu u realnom vremenu (Neri, et al., 2022). Prevelik protok logova bez odgovarajuće filtracije može dovesti do zagušenja korelacionog engine-a ili zanemarivanja bitnih signala zbog „šuma“. Efikasna konfiguracija uključuje definisanje jasnih kriterija prioriteta praćenja, i tako kritične poslovne aplikacije i resursi visoke vrijednosti dobijaju detaljan monitoring, dok sekundarni servisi mogu biti agregirani na višem nivou kako bi se smanjio volumen podataka bez gubitka relevantne informacije o ozbiljnim prijetnjama. Treba istaći povezanost SIEM sistema sa edukacijom korisnika (Ejjami, 2024). Notifikacije generisane od strane SIEM-a moraju biti razumljive krajnjim administratorima koji odlučuju o sljedećim koracima i to implicira potrebu treninga osoblja ne samo u korištenju platforme već i interpretaciji podataka koje ona prezentuje. Bez tog nivoa kompetencije alarmi mogu biti ignorisani ili pogrešno klasifikovani što umanjuje efekat višeslojne zaštite. Uz dobro obučene timove SIEM postaje aktivan alat ne samo za pasivnu detekciju nego i inicijator koordinisanog odgovora između različitih slojeva odbrane. Tehnički razvoj SIEM sistema uključuje dodavanje opcija prediktivne analize kroz modele mašinskog učenja koji analiziraju istorijske podatke radi prepoznavanja ranih indikatora incidenata. U Defense in Depth okruženju ovakve funkcionalnosti znače pomjeranje fokusa ka proaktivnom djelovanju, jer umjesto čekanja stvarnog napada, sistem može upozoriti na neobične obrasce kretanja kroz mrežu ili nagle promjene performansi segmenta koje prethode kompromitaciji. Ako je predviđen pad performansi IDS/IPS komponenti u specifičnom vremenskom okviru povezano s aktuelnim skeniranjem portova izvana, administratorski tim može preventivno prilagoditi pravila firewall-a ili privremeno pojačati autentifikacione procedure prije nego što prijetnja eskalira. Na strateškom nivou primjena SIEM sistema unutar konteksta MSP omogućava plansko

raspoređivanje resursa na osnovu realnih pokazatelja ugroženosti infrastrukture (Ejjami, 2024).

3.5.2. Real-time monitoring

Real-time monitoring unutar višeslojne arhitekture odbrane ima zadatak da osigura neprekidno praćenje i analizu aktivnosti svih komponenti informacionog sistema, kako bi se u trenutku pojave anomalije moglo odmah reagovati. Za razliku od periodičnog pregleda logova ili pasivnih metoda detekcije, ovdje se radi o kontinuiranom procesu koji obrađuje događaje čim se dogode, što značajno skraćuje vrijeme od inicijalne prijetnje do njenog otkrivanja i neutralizacije (Amro & Gkioulos, 2023). Ovaj sloj se nadovezuje na funkcionalnosti opisanih SIEM sistema u prethodnom tekstu, ali ga proširuje dinamikom neprekidnog protoka podataka iz različitih izvora, firewall-a, IDS/IPS sistema, kontrola pristupa, aplikacija i baza podataka, te ih korelira sa definisanim sigurnosnim pravilima u realnom vremenu. Tehnički aspekt real-time monitoringa uključuje upotrebu distribuiranih senzora ili agenata instaliranih na ključnim tačkama infrastrukture, koji prikupljaju telemetriju o mrežnim paketima, sistemskim pozivima, procesima na serverima i upitima prema bazama. Ovi podaci se zatim prenose ka centralnoj analitičkoj platformi koja primjenjuje skup automatizovanih pravila i heurističkih algoritama za prepoznavanje nepravilnosti. Ključno je da ova obrada bude optimizovana kako bi se izbjeglo kašnjenje koje bi napadaču omogućilo da završi kompromitaciju prije detekcije. U arhitekturama Defense in Depth, real-time monitoring smanjuje „prozor ranjivosti“ između proboja jednog sloja zaštite i angažovanja narednog. Jedan primjer može biti nastanak neočekivanog tona komunikacije između serverskog segmenta koji čuva osjetljive podatke i eksterne IP adrese registrovane van organizacije. Firewall može propustiti legitimno usmjeren izlazni promet ako port i protokol odgovaraju dozvoljenim pravilima, ali međutim, real-time monitoring kroz IDS otkriva da učestalost paketa odstupa od normalnog i pokreće alarm (Kuipers & Fabro, 2006). Ovaj alarm se momentalno prosljeđuje SIEM sistemu koji koristi prethodno definisane korelacije za označavanje događaja kao potencijalnog pokušaja eksfiltracije podataka. Integracija monitoringa sa segmentacijom mreže obezbjeđuje dodatnu granularnost detekcije. Kada su mrežni segmenti jasno definisani ACL pravilima i virtualnim lokalnim mrežama (Local Area Network, u daljem tekstu: LAN), real-time monitoring prati samo relevantne tokove unutar tog segmenta, čime se smanjuje količina analiziranih podataka i povećava preciznost

otkrivanja anomalija. Ovo je naročito bitno kod MSP koja nemaju kapacitete za obradu ogromnih količina sirove telemetrije, već filtriranjem ulaza po segmentima optimizuje se analiza bez gubitka kritičnih informacija. Real-time monitoring ne djeluje izolovano, jer on mora biti povezan s mehanizmima automatizovanog odgovora unutar višeslojnog okvira. Ako IPS sistem uoči potpis poznatog napada u dolaznom prometu prema administrativnoj konzoli, ovaj sloj može automatski aktivirati firewall blokadu dotične sesije te pokrenuti MFA verifikaciju ponovne prijave admin naloga (Amro & Gkioulos, 2023). Time detekcija odmah prelazi u reakciju, istovremeno zatvarajući ulaznu tačku napadača i verifikujući legitimitet korisnika kojem je sesija prekinuta. Još jedan važan aspekt jeste integracija monitoringa sa politikama autentifikacije i privilegija. Pokušaji eskalacije privilegija ili promjene kritičnih konfiguracionih fajlova mogu biti signal za aktiviranje alarmnog stanja koje zahtijeva potvrdu od kontrolnog tima prije nastavka rada naloga (Neri, et al., 2022). U slojevitoj arhitekturi ovo funkcioniše kao unutrašnji filter koji sprečava širenje štete čak i ako su vanjske barijere probijene. U kontekstu MSP implementacija efikasnog real-time monitoringa često zahtijeva adaptaciju otvorenih platformi sa specifično podešenim pravilima kako bi odgovarala realnim obrascima poslovanja (Ejjami, 2024). Preopterećivanje sistema lažno pozitivnim alarmima vodi ka ignorisanju pravih prijetnji, i zato analizatori moraju balansirati osjetljivost detekcije sa pragovima tolerancije definisanim tokom inicijalnog profajliranja infrastrukture. Napredne implementacije uvode tehnologije poput mašinskog učenja koje modeliraju normalno ponašanje mreže ili aplikacija pa odstupanja detektuju bez potrebe za ručnim pisanjem pravila. To je posebno korisno kod kompleksnih okruženja gdje legitimne interakcije često variraju zbog dinamičke prirode posla. Algoritmi nadgledaju metrike poput broja otvorenih konekcija po hostu, distribucije tipova upita prema bazama i prosječnog trajanja sesija, a značajne devijacije postavljaju sistem u stanje pripravnosti. Real-time monitoring ima snažnu poveznicu s edukacijom osoblja zaduženog za reakciju na incidente. Brza interpretacija alarma zavisi od znanja administratora da razlikuju lažne od stvarnih uzbuna (Tetteh, 2024). Treninzi uključuju rad na simuliranim incidentima gdje se kroz vizuelne dashboard-e analizira kumulativna slika događaja, grupa neuspjelih prijava sa dodatnim neuobičajenim prometom i promjenom privilegija, kako bi se donijela odluka o blokadi ili daljoj istrazi. Evaluacija performansi real-time monitoringa mjeri metrike kao što su MTTD i MTTR. Kratko MTTD znači da su slojevi brze detekcije dobro sinhronizovani i da kratko MTTR znači da su reakcioni protokoli povezani direktno s izlazima ovog sloja bez nepotrebnih kašnjenja. Ako te vrijednosti

nisu unutar ciljanih granica definisanih BIA analizama, planovi kontinuiteta poslovanja moraju uključiti unapređenje ovog sloja, bilo dodavanjem novih senzora, optimizacijom filtera prometa ili boljom integracijom automatizovanih akcija. Na strateškom nivou real-time monitoring djeluje kao živčani sistem višeslojne zaštite i on ne samo da prenosi signale iz svih dijelova organizacione infrastrukture, već ih povezuje u smisleno upozorenje koje aktivira koordinisan odgovor ostalih slojeva Defense in Depth arhitekture. Kada svi ovi elementi rade sinhronizovano, perimetarska filtracija sa IDS/IPS intervencijom, interni ACL filteri c MFA provjerama, SIEM korelacija događaja i krizne procedure oporavka, tada postaje moguće držati protivnika korak iza bez obzira na vektor napada kojim je počeo kompromitaciju (Amro & Gkioulos, 2023).

3.5.3. Analitika bezbjednosnih događaja

Analitika bezbjednosnih događaja u okviru slojevite strategije odbrane predstavlja napredni proces obrade, korelacije i interpretacije podataka o aktivnostima unutar informacionog sistema radi otkrivanja obrazaca koji upućuju na postojanje prijetnji ili anomalija. Ona se zasniva na integraciji telemetrije iz svih slojeva zaštite, perimetarskih filtera, IDS/IPS sistema, kontrola pristupa, autentifikacionih mehanizama, segmentacije mreže, backup okvira i planova kontinuiteta poslovanja, kako bi se formirala centralizovana situaciona svijest (n.a., 2009). Za razliku od real-time monitoringa koji reaguje momentalno na pojedinačne događaje, analitika ima širu funkciju u prepoznavanju kumulativnih obrazaca ponašanja kroz duži vremenski period. Tehnička realizacija uključuje sredstva za prikupljanje logova i audit tragova sa svih relevantnih tačaka infrastrukture. Ovi izvori obezbjeđuju sirove podatke o mrežnim konekcijama, pokušajima prijave, modifikacijama privilegija, promjenama konfiguracionih fajlova i transferima podataka. Nakon prikupljanja slijedi faza normalizacije podataka kojom se različiti formati zapisa pretvaraju u homogen skup koji je pogodan za korelacione algoritme. To je presudno jer sistemi perimetarske zaštite mogu koristiti drugačije formate od aplikativnih logova ili sistema za upravljanje identitetima (Amro & Gkioulos, 2023). Korelacioni mehanizmi primjenjuju pravila zasnovana na potpisima poznatih napada, heurističke metode zasnovane na procjeni odstupanja od normalnog obrasca rada i statističke modele prediktivne analize. Na primjer, usporedba trendova neuspjelih pokušaja prijave sa IP adresa povezanih s prethodnim incidentima sa naglim rastom odlaznog prometa prema nepoznatoj destinaciji može ukazivati na koordinisanu kampanju kompromitovanja naloga i

eksfiltracije podataka. Bez analitičkog sloja takvi signali ostaju fragmentirani u pojedinačnim zapisima i teško ih je povezati. Važan dio ovog procesa je integracija konteksta iz višeslojnih kontrola. Attempt upotrebe zabranjenog port-a može izgledati benigno ako ga posmatramo izolovano, ali međutim, kad se toj pojavi pridruži evidencija reakcije IDS sistema i promjena privilegija naloga iz kontrolnog modula pristupa, dobija se cjelovitija slika koja može ukazivati na sofisticiranu eskalaciju prava (Kuipers & Fabro, 2006). Time analitika bezbjednosnih događaja postaje ključna karika koja povezuje razdvojene slojeve odbrane u jedinstveni mehanizam otkrivanja napada. U kontekstu MSP analitika mora biti optimizovana da balansira dubinu inspekcije sa ograničenim resursima (Ejjami, 2024). Praktičan pristup podrazumijeva automatsko filtriranje „šuma", događaja niske vrijednosti, kako bi se fokusirali kapaciteti na indikatore visokog rizika. Alati otvorenog koda sa modularnim pravilima korelacije omogućavaju adaptaciju prema lokalnim obrascima prometa i prijetnji bez velikih troškova licenciranja. Primjenom takvih rješenja moguće je pratiti ICS specifične protokole ili analizirati anomalije relevantne samo za segmente koji čuvaju kritične podatke. Tehnike machine learning-a sve više pronalaze primjenu u ovom sloju. Modeliranjem normalnog ponašanja resursa organizacije kroz istorijske podatke moguće je prepoznati odstupanja koja signalizuju „zero-day" prijetnje ili prilagođene maliciozne kampanje koje nemaju standardne potpise. Na primjer, neuobičajeno trajanje administrativne sesije u kombinaciji sa minimalnom aktivnošću zabilježenom kroz ACL logove može predstavljati indikator skrivenog transfera podataka. Povezanost ovog sloja sa politikama reagovanja na incidente znači da otkriveni obrazac mora biti proslijeđen sistemima automatizovanog odgovora unutar Defense in Depth okvira. Kada analitika potvrdi zajednički vektor prijetnje između perimetarskog i aplikacionog sloja, firewall može automatski prilagoditi pravila blokade dok PAM sistem opoziva privilegije pogođenih naloga. Ovakva integrisana reakcija smanjuje MTTR jer odluke proizilaze iz verifikovanih korelacija umjesto izolovanih alarma. Bitna komponenta analitike bezbjednosnih događaja jeste forenzička spremnost, sposobnost kreiranja tačne hronologije incidenata za potrebe istrage (Amro & Gkioulos, 2023). Centralizovano skladištenje korelisanih zapisa olakšava rekonstrukciju toka napada, od inicijalnog pokušaja skeniranja portova preko uspješnog phishing-a do aktivacije malicioznog koda unutar interne mreže. Takva detaljna sekvenca omogućava preciznu procjenu štete te otkrivanje ranjivosti koje treba zatvoriti kako bi se spriječilo ponavljanje incidenta. Interakcija s edukacijom zaposlenih ima poseban značaj (Tetteh, 2024). Analitički izvještaji koji vizuelno demonstriraju načine kompromitovanja

sistema služe kao pedagoški alat tokom edukativnih programa, zaposlenima postaje jasnije kako njihovo ponašanje doprinosi (ili ugrožava) funkcionisanje višeslojne zaštite. Feedback iz analitike pomaže prilagođavanju obuka prema relevantnim prijetnjama detektovanim u realnom okruženju organizacije. Periodične evaluacije efektivnosti ovog sloja potrebno je provoditi kroz testne scenarije simuliranih incidenata (Boggs, et al., 2009). Kroz takve simulacije provjerava se koliko brzo analitički modul prepoznaje zadani obrazac prijetnje, koliki je nivo tačnosti korelacija i da li odluke o reakciji dolaze pravovremeno da spriječe eskalaciju. Konačno, analitika bezbjednosnih događaja učvršćuje koncept Defense in Depth time što povezuje tehničke mjere različitih slojeva s organizacijskim procedurama reakcije i ljudskim faktorom nadzora (n.a., 2009). Sinhronizovan rad perimetarske filtracije, unutrašnjih politika pristupa, autentikacije korisnika, segmentacije mreže i planova kontinuiteta poslovanja stvara zaokružen sistem gdje nijedan alarm nije posmatran izolovano već kao potencijalni dio većeg obrasca aktivnosti protivnika. Ovaj holistički pogled daje operativnim timovima prednost brzine i preciznosti akcije nad dinamikom napadačkih tehnika koje su ciljano osmišljene da zbune ili fragmentiraju odgovor organizacije.

3.6. Bezbjednost aplikacija

Bezbjednost aplikacija predstavlja značajan sloj Defense in Depth strategije i usmjerena je na zaštitu aplikacija tokom njihovog razvoja, implementacije i eksploatacije. Cilj ovog sloja je smanjenje ranjivosti koje mogu biti iskorištene za neovlašteni pristup, kompromitaciju podataka ili narušavanje funkcionalnosti sistema.

Primjena principa sigurnog kodiranja, zajedno sa redovnim testiranjem ranjivosti, omogućava pravovremeno otkrivanje i otklanjanje sigurnosnih propusta. Ovaj sloj doprinosi ukupnoj otpornosti informacionog sistema i ima važnu ulogu u prevenciji napada koji ciljaju aplikacioni nivo.

3.6.1. Sigurno kodiranje

Sigurno kodiranje unutar strategije slojevite odbrane predstavlja temeljni stub bezbjednosti aplikacija, jer se fokusira na prevenciju ranjivosti još u fazi razvoja softvera, čime se minimizira rizik od kompromitovanja sistema nakon što aplikacija postane operativna. Ovaj pristup ne tretira aplikaciju kao izolovan entitet već je posmatra kao integrisan dio višeslojne arhitekture zaštite, povezan sa perimetarskim mehanizmima, unutrašnjom kontrolom pristupa,

autentifikacijom korisnika i kontinuiranim nadzorom (Xu, et al., 2020). Ako kodiranje ne prati sigurnosne standarde, svi kasnije dodani slojevi odbrane (firewall, IDS/IPS, segmentacija mreže) mogu biti zaobiđeni kroz direktnu eksploataciju slabosti koju napadač pronalazi u samoj logici aplikacije. Temelj sigurnog kodiranja predstavlja identifikacija potencijalnih vektora napada već u inicijalnoj fazi dizajna. To podrazumijeva razumijevanje tipičnih kategorija ranjivosti koje su definisane u okvirima poput OWASP Top 10 , SQL injection, cross-site scripting (XSS), insecure deserijalizacija i slično, ali se ide korak dalje uzimajući u obzir specifičnosti poslovnog okruženja i regulatornih zahtjeva sektora u kojem aplikacija djeluje. Ove kategorije ranjivosti moraju biti povezane sa odgovarajućim slojem Defense in Depth zaštite kako bi se jasno definisalo gdje će mitigacione mjere stupiti na snagu, a neki problemi mogu biti adresirani unutar same logike koda (npr. validacija ulaznih podataka), dok drugi zahtijevaju nadogradnju na perimetarskom nivou kroz web application firewall (Erickson, 2008). Kontrola ulaznih podataka je jedan od imperativa sigurnog kodiranja. Bez striktne validacije svih parametara koje korisnik unosi ili šalje ka aplikaciji, napadač može ubaciti maliciozne vrijednosti koje mijenjaju tok izvršavanja programa. Primjena kontekstualne validacije, gdje se kriterijumi provjere prilagođavaju vrsti podatka i mjestu upotrebe, smanjuje površinu napada na značajan način (Xu, et al., 2020). Na primjer, polje za unos datuma mora prihvatati samo vrijednosti koje zadovoljavaju YYYY-MM-DD format, dok polja za tekstualne podatke trebaju imati ograničenje dužine i filtriranje posebnih karaktera koji mogu poslužiti za injekciju komandi. Integritet koda osigurava se primjenom kriptografskih mehanizama za provjeru autentičnosti softverskih modula prije njihove primjene u produkcionom okruženju (Bartock, et al., 2021). Tehnike potpisivanja koda obezbjeđuju da izvršni fajl ili biblioteka nisu izmijenjeni nakon što ih je developer izdao, kombinacijom hash funkcija i digitalnih potpisa kreira se lanac povjerenja između programera i okruženja u kojem će kod biti pokrenut. Kada je ovakav sloj povezan sa sistemima upravljanja privilegijama, dobija se dodatna garancija da samo ovlašteni entiteti mogu izvoditi kritične promjene. Sigurno upravljanje greškama ima istu težinu kao i validacija inputa. Neadekvatno hvatanje i obrada izuzetaka može otkriti interne detalje aplikacije kroz poruke o grešci ili log zapise dostupne korisniku. Standard kodiranja mora propisivati generičke poruke prema klijentima dok se kompletan tehnički opis problema evidentira isključivo u sigurnosnim log-ovima dostupnim administratorima (Neri, et al., 2022). Na taj način smanjuje se rizik od curenja informacija relevantnih za daljnju eksploataciju. Implementacija kontrole pristupa unutar kodnog dijela same aplikacije

dopunjuje političke slojeve upravljanja identitetom opisane ranije (Amro & Gkioulos, 2023). Svaka funkcionalnost koja rukuje osjetljivim podacima mora uključivati provjeru prava korisnika neposredno prije izvršenja akcije, ovo sprečava situacije u kojima napadač legitimnog naloga može obaviti nedozvoljene operacije zbog tehničke greške ili propusta u centralizovanoj politici pristupa. Kod aplikacija koje upravljaju kritičnim poslovnim procesima važna je segmentacija funkcionalnosti slična mrežnoj segmentaciji (Kuipers & Fabro, 2006). To znači modularno odvajanje dijelova aplikacijskog koda tako da kompromitovanje jednog modula ne omogućava automatski pristup drugima. Interna API komunikacija mora biti autentificirana i autorizovana, pa čak ni funkcionalnosti unutar iste aplikacije ne bi trebale vjerovati jedna drugoj implicitno. Sigurno rukovanje vanjskim bibliotekama i komponentama još je jedna dimenzija ovog sloja zaštite. „Dependency management“ sistemi moraju pratiti verzije ugrađenih biblioteka i upozoravati na poznate ranjivosti koje su dokumentovane u sigurnosnim biltenima proizvođača. Automatizovani alati kao što su Software Composition Analysis (u daljem tekstu: SCA) pomažu developerima da uklone ili nadograde nesigurne komponente prije nego što postanu vektor napada. Za okruženja MSP praktično je implementirati automatizovane testove sigurnosti koda, statičku analizu (Static application security testing, u daljem tekstu: SAST) i dinamičku analizu (Dinamic application security testing, u daljem tekstu: DAST). SAST pregledava izvorni kod bez pokretanja aplikacije radi detekcije obrazaca koji ukazuju na potencijalne ranjivosti, dok DAST simulira interakciju sa pokrenutom aplikacijom tražeći neočekivana ponašanja koja bi mogla biti iskorištena od strane napadača (Xu,, et al., 2020). Kombinovanjem ovih metoda zatvara se veći broj mogućih rupa još tokom razvoja. Ljudski faktor u sigurnom kodiranju ne treba zanemariti. Edukacija programera o najnovijim prijetnjama, sigurnosnim standardima i alatima bitna je da bi principi sigurnog pisanja koda bili dosljedno primijenjeni kroz sve projekte. Interni vodiči koji dokumentuju dobre prakse kodiranja trebaju biti ažurirani redovno kako bi pratili evoluciju prijetnji identifikovanih putem analitike bezbjednosnih događaja. Proces revizije koda usklađen s višeslojnom arhitekturom podrazumijeva da analiza ne gleda samo sintaksu već i povezanost funkcionalnosti sa ostalim slojevima zaštite, na primjer kako modul verifikuje podatke dobijene preko mrežnog API-ja koji prolazi kroz firewall filtere ili kako obrađuje rezultate autentifikacionog servisa (Neri, et al., 2022). Time se postiže koherencija između tehničkih kontrola unutar koda i vanjskih slojeva Defense in Depth ekosistema. Na strateškom nivou sigurno kodiranje osigurava otpornost aplikacija na nove vektore prijetnji bez potrebe

da se isključivo oslanja na vanjske slojeve zaštite. Kada su mehanizmi poput input sanitizacije, principa najmanjih privilegija u kodnoj logici, pravilnog rukovanja greškama te verifikacije integriteta softverskih komponenti integrisani od samog početka razvoja, oni formiraju prvu liniju odbrane koja komplikuje život svakom potencijalnom napadaču čak prije nego što naiđe na mrežne barijere ili kontrole pristupa organizacije. Na taj način sigurno kodiranje postaje neophodan segment višeslojnog koncepta zaštite koji štiti cjelokupni informacioni sistem kroz proaktivno uklanjanje izvora ranjivosti prije nego što one postanu iskoristive.

3.6.2. Testiranje ranjivosti

Testiranje ranjivosti unutar strategije slojevite odbrane obuhvata sistematsku procjenu bezbjednosnog stanja aplikacija i prateće infrastrukture, sa ciljem otkrivanja i dokumentovanja slabih tačaka koje bi potencijalno mogle biti iskorištene od strane napadača. Ovaj proces se uklapa u višeslojnu arhitekturu tako što pruža povratne informacije o kvalitetu svih prethodno implementiranih kontrola, počevši od perimetarskih filtera komunikacije, preko unutrašnjih mehanizama kontrole pristupa i autentifikacije korisnika, do aplikacionog koda razvijenog prema principima sigurnog programiranja (Amro & Gkioulos, 2023). Za razliku od opšte statičke procjene rizika, testiranje ranjivosti uključuje aktivne metode procjene u realnom ili simuliranom okruženju, uključujući penetraciono testiranje, SAST, DAST i fuzzing tehnike. Integracija testiranja ranjivosti u Defense in Depth okvir znači da ovaj proces ne evaluira isključivo jedan sloj zaštite, već ispituje otpornost sistema na proboj i lateralno kretanje kroz više slojeva. Na primjer, pronalazak injekcione ranjivosti u web formi ne testira samo logiku aplikacije, već posredno provjerava efikasnost WAF pravila na perimetru, validaciju inputa u kodu, te nadzorne alate koji bi trebali detektovati anomalne upite prema bazi podataka. Time rezultati jednog testa mogu generisati korektivne akcije na nekoliko nivoa odbrane. Tehnička metodologija počinje mapiranjem opsega testiranja, definisanjem ciljnih sistema, servisa i interfejsa koji će biti obuhvaćeni istragom. U kontekstu MSP preporučuje se prioritetno fokusiranje na one komponente koje obrađuju povjerljive podatke ili imaju kritičnu poslovnu vrijednost. Nakon mapiranja sprovodi se automatsko skeniranje pomoću specijalizovanih alata koji pretražuju poznate ranjivosti bazirane na javnim CVE (Common Vulnerabilities and Exposures) zapisima i internim pravilima organizacije (Boggs, et al., 2009). Ovi alati mogu identifikovati verzije softvera sa poznatim propustima, nesigurne konfiguracije servera ili kriptografske protokole slabog kvaliteta. Međutim, automatizovana analiza sama

po sebi nije dovoljna. Mnoge sofisticirane prijetnje koriste kompleksne lance eksploatacije (kill chain) koje kombinuju više manjih slabosti. Zato je manuelno penetraciono testiranje važno za simulaciju stvarnog ponašanja napadača koji nastoji zaobići više slojeva zaštite kombinovanjem tehničkih i socijalnih vektora napada (n.a., 2009). Testeri ciljano provociraju odgovor IDS/IPS sistema, pokušavaju eskalaciju privilegija unutar segmentisanih mreža ili iniciraju pristup rezervnim kopijama radi provjere izolacionih protokola opisanih u sloju redundancije i oporavka. Testiranje ranjivosti također igra bitnu ulogu u verifikaciji funkcionalnosti unutrašnjih kontrola pristupa i korisničke autentifikacije. Pokušaji korištenja standardnih admin naloga sa podrazumijevanim lozinkama, zaobilaženje MFA mehanizama putem phishing tehnika ili zloupotreba „session fixation" scenarija direktno provjeravaju otpornost ovog sloja zaštite. Takvi eksperimenti nisu ograničeni samo na tehnički ishod (da li je pristup omogućen) već bilježe i brzinu reakcije nadzornih timova zaduženih za monitoring događaja, metrike MTTD i MTTR postaju kvantitativni indikatori spremnosti organizacije za stvarne incidente (Ejjami, 2024). Kod aplikacionog sloja posebna pažnja posvećuje se testiranju dosljednosti sigurnosnih politika unutar mreže sa politikama implementiranim u kodu aplikacije. Nesklad između ovih politika često stvara „rupe" koje nisu očigledne izolovanim revizijama. Recimo, ACL pravila mogu zabraniti određene tipove poziva spoljnim servisima dok ih interna funkcija aplikacije dopušta zbog logičkog previda tokom razvoja, testiranjem ranjivosti ova neusaglašenost izlazi na vidjelo (Amro & Gkioulos, 2023). Jedan od izazova pri testiranju okruženja MSP jeste integracija zastarjelih sistema sa modernim bezbjednosnim okvirima (Bartock, et al, 2021). Legacy aplikacije često ne podržavaju savremene metode enkripcije ili autentifikacije pa su sklone kompromitovanju kroz propuste ranijeg datuma. Tokom penetracionih proba ovi sistemi zahtijevaju poseban tretman, izolovanje u mikrosegmente tokom testa uz simultanu procjenu uticaja eventualnog kompromitovanja na ostatak mreže. Testovi moraju biti pažljivo koordinisani kako bi izbjegli ometanje kritičnih poslovnih procesa. U praksi to znači izvođenje dinamičkih proba van perioda intenzivne upotrebe servisa ili korištenje staging okruženja koje vjerno replicira produkciju. Ovakva replika omogućava kompletan ciklus testa, od inicijalnog skeniranja do eksploatacije, bez posljedica po operativni rad organizacije. Rezultati se potom mapiraju nazad na produkciono okruženje kroz preporuke koje specificiraju potrebne izmjene konfiguracija, unapređenja procedura ili korekcije programskog koda. Važna komponenta procesa je dokumentovanje nalaza, to jest svaki otkriveni propust mora sadržati detaljan opis,

korake reprodukcije, identifikovane uticaje po povjerljivost, integritet i dostupnost sistema te predložene mjere mitigacije (n.a., 2009). Na taj način rezultati ne služe samo trenutnoj ispravci slabosti već postaju polazna tačka za edukaciju razvojnog i administrativnog osoblja kako iste greške ne bi bile ponovljene u budućim projektima. Rezultati testiranja ranjivosti potom se prosljeđuju svim relevantnim slojevima Defense in Depth okvira radi koordinisanog unapređenja sigurnosnog stava organizacije. Perimetarske kontrole ažuriraju svoja pravila filtriranja prema novootkrivenim obrascima napada, a unutrašnja kontrola pristupa može redefinisati privilegije; i onda SIEM integracija dodaje nova korelaciona pravila zasnovana na tehnikama viđenim tokom testa. Zatim backup procedura dobija dopunu koja sprečava eksfiltraciju podataka otkrivenim metodama, a razvojni tim inkorporira zaključke u vodiče sigurnog kodiranja. Konačno, testiranje ranjivosti nije jednokratan događaj već ciklični proces koji prati promjene infrastrukturne topologije, nove verzije aplikacija i evoluciju sajber prijetnji. Frekvencija sprovođenja zavisi od sektora rada i regulatornih zahtjeva ali dobra praksa sugeriše kvartalne osnovne provjere uz detaljne godišnje penetracione probe. Kombinacijom automatizovanih alatki za stalni nadzor novih propusta i ciljano sprovedenih manuelnih analiza obezbjeđuje se da nijedan sloj višeslojne strategije ne ostane sa neotkrivenom slabom tačkom koja bi mogla potkopati integritet čitavog odbrambenog sistema.

3.7. Upravljanje identitetom

Upravljanje identitetom predstavlja ključnu komponentu informacione bezbjednosti koja omogućava centralizovano upravljanje digitalnim identitetima korisnika, sistema i servisa kroz njihov cjelokupni životni ciklus. Ovaj proces obuhvata kreiranje, izmjenu i uklanjanje identiteta, kao i dodjelu i reviziju pristupnih prava u skladu sa poslovnim ulogama i sigurnosnim politikama.

Efikasno upravljanje identitetom doprinosi smanjenju rizika od neovlaštenog pristupa, omogućava dosljednu primjenu principa najmanjih privilegija i olakšava praćenje i kontrolu korisničkih aktivnosti. Kao sastavni dio Defense in Depth strategije, ovaj sloj pruža osnovu za sigurnu autentifikaciju, autorizaciju i usklađenost sa međunarodnim standardima informacione sigurnosti.

3.7.1. IAM sistemi

Sistemi za upravljanje identitetom (Identity and Access Management, u daljem tekstu: IAM) predstavljaju centralizovan okvir za kontrolu individualnih i servisnih naloga, autentifikaciju, autorizaciju resursa i reviziju pristupa unutar slojeva višeslojne zaštite. Posmatrani u kontekstu strategije Defense in Depth, IAM sistemi funkcionišu kao kohezivna tačka povezivanja brojnih kontrola koje obuhvataju perimetarsku zaštitu, unutrašnju kontrolu pristupa, korisničku autentifikaciju, privilegije, nadzor događaja i integraciju sigurnosnih politika. Njihova svrha nije izolovana, već oni omogućavaju da svaki sloj odbrane prepoznaje i verifikuje identitet entiteta koji mu pristupa, bilo da je riječ o ljudskom korisniku ili procesu u aplikaciji (Bao et al., 2023). Tehnička arhitektura IAM sistema često se zasniva na jednom ili više modula, repozitorijumu identiteta gdje se čuvaju podaci o korisnicima i uređajima, autentifikacionima servisima koji realizuju provjeru prijave (password-based, token-based, biometrijska ili višefaktorska autentifikacija) i autorizacionim mehanizmima zasnovanim na modelima dozvola kao što su Role-Based Access Control (u daljem tekstu: RBAC), Attribute-Based Access Control (u daljem tekstu: ABAC) ili Policy-Based Access Control (u daljem tekstu: PBAC), te modulima za audit i izvještavanje koji bilježe sve pokušaje pristupa. Prema smjernicama za Unificirano upravljanje pristupom (UAM), preporučuje se centralizovani model kontrole identiteta jer pojednostavljuje administraciju i reducira mogućnost grešaka u konfiguraciji (Amro & Gkioulos, 2023). Centralizacija istovremeno uvodi rizik „single point of failure" scenerija, kod kojeg kompromitacija glavnog servera može ugroziti sve povezane sisteme, pa se kao dio slojevite zaštite implementiraju redundantne instance autentikacionih servisa i mehanizmi visokog nivoa integriteta komunikacije. Ključna prednost IAM okvira je sposobnost integracije sa ostalim slojevima Defense in Depth strategije. Perimetarski firewall-ovi mogu koristiti IAM podatke kako bi dinamički generisali pravila filtriranja prema statusu privilegija korisnika, a unutrašnja segmentacija mreže koristi centralni IAM server za grananje dozvoljenih protokola između zona, dok se aplikativni moduli oslanjaju na tokene ili certifikate izdane od strane IAM-a radi potvrde legitimnosti poziva (Jander, et al., 2019). Ovakva interoperabilnost omogućava da ne postoji izolovani sloj bezbjednosti i svaki učesnik odbrambenog ekosistema dobija pravovremenu informaciju o validnosti identiteta. U kontekstu MSP integracija Lightweight Directory Access Protocol-a (u daljem tekstu: LDAP) ili RADIUS/TACACS+ protokola sa postojećom infrastrukturom predstavlja praktičan izbor (Amro & Gkioulos, 2023). LDAP pruža obradu hijerarhijskih struktura korisnika i resursa uz podršku

RBAC modela dozvola; RADIUS i TACACS+ donose fleksibilne mehanizme autentifikacije mrežnih uređaja te audit svih konekcija ka kritičnim sistemima. MFA opisano ranije nadovezuje se na IAM sloj kao dodatna verifikacija svakog autentifikacionog zahtjeva, a ova kombinacija značajno umanjuje efikasnost credential stuffing napada jer neovlašteni akter ne može proći sve faktore validacije. IAM mora obuhvatiti PAM unutar šireg ekosistema (n.a., 2009). PAM modul dodjeljuje povišene privilegije samo privremeno i po jasno definisanoj potrebi, a po završetku zadatka privilegije se automatski opozivaju. Audit trag svake akcije izvedene sa administrativnim pravima povezuje se sa centralnom bazom identiteta, čime analiza anomalnog ponašanja dobija kontekstualnu dimenziju, korelacijom između promjene prava, zone u kojoj je nastala aktivnost i rezultata detekcije IDS/IPS sistema. Segmentacija mreže daje dodatnu granularnost upravljanju identitetima tako što dozvole nisu globalne već vezane isključivo za zone ili podzone (Kuipers & Fabro, 2006). Korisnik validiran kroz IAM sistem dobija pristup resursima samo unutar definisanog segmenta, prelazak granice inicira ponovnu provjeru ili blokiranje sesije. Time se smanjuje lateralno kretanje napadača čak i s kompromitovanim nalogom. Važan aspekt IAM implementacije je sigurnost samih komunikacionih kanala između klijenata i servera za upravljanje identitetom. Protokoli moraju koristiti enkripciju prijenosa (TLS) uz validaciju certifikata, a svako odstupanje ove konekcije može biti detektovano pomoću monitoring alata integrisanih u SIEM. Posebna pažnja posvećuje se zaštiti API interfejsa koje koriste aplikacije za traženje autentikacije od IAM-a, „injection“ komandi kroz nesigurne API pozive predstavljaju ozbiljan vektor napada bez adekvatne input zaštite i polisa filtriranja. Edukacija administratora sistema o funkcionisanju IAM platforme je nezaobilazna komponenta efektivne primjene ovog sloja (Tetteh, 2024). Greške u definisanju politika pristupa mogu omogućiti eskalaciju privilegija ili nenamjerni otvoreni pristup ka kritičnim podacima. Treninzi uključuju pravilno mapiranje poslovnih procesa na role unutar RBAC modela, upotrebu grupnih atributa kod ABAC-a, te interpretaciju audita radi otkrivanja anomalnog ponašanja. Redundancija unutar infrastrukture IAM sistema reflektuje filozofiju Defense in Depth, jer sekundarni serveri u geografski odvojenim lokacijama preuzimaju autentikaciju kada primarni postane nedostupan (Amro & Gkioulos, 2023). Sinhronizacija baza identiteta između instanci mora biti pouzdana ali kontrolisana kako bi spriječila repliciranje kompromitovanih naloga. Planovi kontinuiteta poslovanja uključuju automatsko preusmjerenje zahtjeva ka rezervnoj instanci uz verifikaciju njenog integriteta prije puštanja u rad. Integracija rezultata analize bezbjednosnih događaja

sa IAM politikama pruža proaktivan odgovor na prijetnje. Ako SIEM detektuje neuobičajen niz neuspjelih autentikacija sa jedne IP adrese, IAM može privremeno blokirati relevantne naloge dok incident odgovor tim ne utvrdi legitimnost pokušaja. Ovakva adaptivna kontrola povezuje detekcioni sloj sa autorizacionim pravilima u realnom vremenu. Za MSP ispravno konfigurisani IAM sistem znači povećanu otpornost cijelog Defense in Depth ekosistema, resursi postaju dostupni isključivo ovlaštenim subjektima kroz kontrolisane kanale, i svaki pokušaj zloupotrebe identiteta ostavlja trag vidljiv nadzornim alatima, a redundancija infrastrukture garantuje održavanje procesa autentikacije čak tokom incidenata koji parališu druge tehničke slojeve odbrane (Ejjami, 2024). Upravo zbog ove središnje koordinacione funkcije IAM sistemi predstavljaju jedan od najvažnijih segmenata strategije višeslojne zaštite gdje integritet rada zavisi od sinhronizovanog djelovanja tehnoloških modula, organizacionih procedura i obučenog ljudskog faktora.

3.7.2. Lifecycle upravljanje identitetima

Upravljanje životnim ciklusom identiteta (Identity Lifecycle Management, u daljem tekstu: ILM) unutar višeslojne strategije odbrane predstavlja organizaciono-tehnički proces kojim se nadgleda, kontroliše i optimizuje čitav tok postojanja digitalnog identiteta u sistemu, od njegovog kreiranja, kroz faze održavanja i modifikovanja prava, pa sve do deaktivacije ili trajnog uklanjanja kada prestane potreba za tim identitetom. Ovaj pristup ima za cilj da svaki entitet unutar informacionog sistema – bilo da se radi o korisniku, aplikaciji ili mrežnom servisu posjeduje samo ona ovlaštenja koja su mu potrebna u važećem trenutku, bez zadržavanja zastarjelih ili nevalidnih privilegija koje bi potencijalno mogle biti zloupotrebljene. Proces upravljanja započinje inicijacijom identiteta. U ovoj fazi definisani administratori, uz validaciju u skladu sa poslovnim procesom i politikama kontrole pristupa (Neri, et al., 2022), kreiraju nalog unutar centralizovanog IAM sistema opisanog ranije. Kreiranje uključuje precizno mapiranje role korisnika prema njegovim zadacima uz principe najmanjih privilegija kako bi se smanjila mogućnost lateralnog kretanja u slučaju kompromitacije (n.a, 2009). Često se koriste modeli RBAC ili ABAC pri dodjeli dozvola, ABAC omogućava granularniju kontrolu time što vezuje pristupne politike uz atribute korisnika, resursa i konteksta (npr. geolokacija ili vrijeme pristupa), dok RBAC pojednostavljuje administraciju kroz grupne role. Održavanje identiteta odnosi se na period dok je nalog aktivan. Tokom ovog vremena nužno je sprovesti periodične revizije privilegija, koristeći audit tragove iz SIEM sistema i korelaciju događaja sa

stvarnim operativnim potrebama. Revizije služe za otkrivanje „privilege creep" fenomena, situacije u kojoj korisnici tokom dužeg angažmana akumuliraju dodatne dozvole koje im možda više nisu potrebne. Na tehničkom nivou revizija može uključivati automatizovane skripte povezane sa HR sistemima koje sinhronizuju status zaposlenih sa IAM bazom, momentalno oduzimajući pristup kad osoba napusti organizaciju ili promjeni dužnost koja ne zahtijeva prethodne privilegije (Ejjami, 2024). Faza modifikovanja ovlaštenja mora biti jasno definisana procedurama autorizacije. Promjena privilegija može biti permanentna (npr. prelazak zaposlenog na višu poziciju) ili privremena, što je posebno važno kod eskalacije prava za specifične zadatke. Privremena eskalacija treba biti vremenski ograničena i praćena audit evidencijom svih izvršenih akcija (n.a., 2009). PAM moduli integrisani sa IAM sistemima omogućavaju takvo upravljanje tako što izdaju jednokratne pristupne kredencijale koji ističu po završetku definisanog intervala rada. Tehnički sloj zaštite ILM-a obuhvata sigurnost podataka o identitetima u svim fazama životnog ciklusa. Komunikacija između klijenata koji traže autentifikaciju i servera za upravljanje identitetom mora koristiti protokole sa jakim kriptografskim mehanizmima (TLS), dok su podaci o akreditivima pohranjeni u enkriptovanim trezorima HSM uređaja (Bartock, et al., 2021). Svaka interakcija putem API-ja prema IAM komponenti mora imati validaciju inputa kako bi se spriječile „injection" tehnike koje mogu dovesti do neautorizovanih manipulacija pravima. Deaktivacija identiteta posljednja je faza lifecycle procesa. Aktiviranje ove procedure nastupa kad prestane poslovna potreba za identitetom, istekom ugovora zaposlenog, završetkom projektnog angažmana ili prekidom saradnje s eksternim subjektom. Deaktivacija ne znači nužno brisanje svih podataka, regulatorni zahtjevi često nalažu zadržavanje audita određeno vrijeme radi forenzičkih i zakonskih svrha (Halaponin, et al., 2022). Međutim, tehnički pristup mora osigurati da deaktivirani nalozi nemaju nikakav kapacitet autentifikacije prema sistemskom okruženju. Važno je naglasiti sinergiju lifecycle upravljanja identitetima sa ostalim slojevima Defense in Depth strategije. Perimetarska zaštita može koristiti ILM podatke radi dinamičkog generisanja firewall pravila, blokiranje konekcija koje potiču od naloga označenih kao deaktivirani ili suspenzovani (Jande, et al., 2019). Segmentacija mreže povezana je s lifecycle politikama jer prelazak korisnika iz jedne role u drugu može automatski mijenjati pripadajuće mrežne zone kojima ima pristup, sprečavajući nenamjerno otvaranje putanje lateralnog napada. Edukacija osoblja ključna je komponenta ILM (Tetteh, 2024). Administratori moraju razumjeti proceduralne korake za svaku fazu životnog ciklusa kako bi odluke bile konzistentne s

politikama bezbjednosti, na primjer pravilno zatvaranje naloga bez preostalih otvorenih sesija ili restarta autentikacionih tokena poslije reaktivacije naloga. Obučeni korisnici doprinose ovom procesu prijavljujući specifične okolnosti koje zahtijevaju promjenu njihovih privilegija umjesto traženja neformalnih prečica ka resursima. U MSP praksa ILM-a olakšava održavanje sveukupne bezbjednosti „posture“ integracijom sa cloud servisima koji nude centralizovano upravljanje nalozima preko više aplikacija bez potrebe za zasebnim admin političkim okvirima po svakoj instanci (Ejjami, 2024). To smanjuje kompleksnost i rizik greške pri ručnom usklađivanju prava u distribuiranim sistemima. Automatsko opozivanje pristupa prilikom izlaska iz organizacije štiti od scenarija gdje bivši zaposleni zadržava nenamjerni pristup internim resursima. Objedinjavanjem svih ovih principa, inicijacije kroz validirane procese kreiranja naloga, stalne revizije ovlaštenja kroz audit tragove, striktno kontrolisanih modifikacija, sigurnih komunikacionih mehanizama prema IAM infrastrukturi, te potpunog zatvaranja neaktivnih entiteta, ILM postaje snažan mehanizam unutar Defense in Depth ekosistema (n.a., 2009). Time svaki sloj odbrane dobija ažurne i provjerene informacije o statusu entiteta, minimizira se prostor za zloupotrebu zastarjelih akreditiva i stvara koordinisan okvir ponašanja tehničkog i ljudskog faktora u zaštiti informacionog sistema od sajber prijetnji.

4. Procjena svijesti o sajber sigurnosti

Procjena svijesti o sajber sigurnosti predstavlja važan element ukupnog sistema informacione sigurnosti, jer omogućava uvid u nivo znanja, ponašanja i stavova korisnika u vezi sa zaštitom informacionih resursa. S obzirom na to da ljudski faktor često predstavlja jednu od najslabijih karika sigurnosnog lanca, sistematska procjena svijesti korisnika ima ključnu ulogu u identifikaciji sigurnosnih rizika koji proizilaze iz neadekvatnog korištenja informacionih sistema.

Ovaj proces obuhvata analizu razumijevanja sigurnosnih politika, prepoznavanje prijetnji poput phishing napada, kao i spremnost korisnika da primjenjuju propisane sigurnosne procedure. Rezultati procjene služe kao osnova za unapređenje programa obuke, jačanje kulture sajber bezbjednosti i kontinuirano poboljšanje zaštite informacionih sistema.

4.1. Metodologija istraživanja

Metodološki okvir istraživanja osmišljen je tako da obuhvati prikupljanje, obradu i analizu podataka iz više izvora kako bi se dobio sveobuhvatan uvid u nivo svijesti o sajber bezbjednosti kod IT osoblja i korisnika, sa posebnim fokusom na elemente Defense in Depth strategije. U skladu sa ranije razmotrenim izazovima MSP (Enitan, 2025), odabrane su metode koje omogućavaju kombinovanje kvantitativnih i kvalitativnih pristupa, čime se postiže dublje sagledavanje stanja. Primjena integrisanog metodološkog pristupa zasnovana je na korištenju kombinovanih tehnika prikupljanja podataka. Kvantitativna komponenta uključuje strukturisane ankete distribuirane uz korištenje slučajnog uzorka, čime se nastoji postići reprezentativnost populacije po kriterijumima kao što su veličina organizacije, sektor djelatnosti i geografska distribucija. Stratifikacija omogućava da različiti subsegmenti MSP-a budu proporcionalno zastupljeni u uzorku, čime se smanjuje rizik od pristrasnosti koja može proizilaziti iz neujednačene distribucije ispitanika. Anketni instrument dizajniran je tako da obuhvati pitanja odnoseći se na primjenu slojeva zaštite, perimetarskih filtera, unutrašnje kontrole pristupa, MFA, procedura edukacije zaposlenih, politika backup-a i planova oporavka, te sistema nadzora. Na osnovu ovakve strukture moguće je izvesti kvantitativne pokazatelje zastupljenosti i primjene Defense in Depth mehanizama unutar ciljnih organizacija. Kvalitativna komponenta istraživanja izvodi se kroz polustrukturisane intervjue i fokus grupe sa IT stručnjacima, administratorima i krajnjim korisnicima informacionih sistema

(Nyamwesa, 2024). Cilj ovih razgovora nije samo deskriptivni prikaz stanja, već identifikacija percepcije korisnika o mogućim prijetnjama, iskustava u radu sa višeslojnim zaštitama i prepreka koje otežavaju njihovu implementaciju. Intervjui omogućavaju dobijanje narativa o praktičnim aspektima primjene slojeva odbrane, firewall konfiguracija u odnosu na realne tokove saobraćaja, mjere segmentacije mreže u okviru postojećih tehničkih ograničenja, održavanja višefaktorskog izazova autentifikacije u kontekstu krajnjih uređaja korisnika, te operativne integracije edukativnih programa. Fokus grupe pomažu pri provjeri zajedničkih obrazaca ponašanja u radu sa osjetljivim podacima i aplikacijama. Integracija nalaza iz kvantitativnog i kvalitativnog dijela vrši se kroz proces tematske analize koja identifikuje dominantne obrasce (teme) vezane uz razumijevanje i primjenu strategije Defense in Depth u MSP-ima (Nyamwesa, 2024). Kombinovanjem statističkih pokazatelja iz anketa sa narativnim opisima iz intervjua formira se sveobuhvatna slika stanja, na primjer, visok procenat ispitanika koji koristi osnovne firewall sa servisima bit će dopunjen opisima iz prakse o problemima njihove konfiguracije ili nedostatku praćenja odlaznog prometa kao dijela ukupne politike filtriranja. Da bi istraživanje zadržalo metodološku validnost, posebna pažnja posvećena je definisanju uzorka tako da izbjegne neslaganja između populacije koja se proučava i raspoloživih informacija. U tu svrhu koristila se jasna definicija kriterijuma za uključivanje ispitanika, aktivno korištenje informacionog sistema unutar MSP-a registrovanih na teritoriji BiH, minimalno šest mjeseci rada na pozicijama uključujući operativni kontakt sa digitalnim alatima, odgovornost za podatke ili sisteme koji imaju komponente povjerljivosti, integriteta ili dostupnosti u skladu sa principima Defense in Depth. Prikupljeni kvantitativni podaci obrađuju se primjenom deskriptivne statistike i procjene rizika u našem slučaju AI-Driven mteodologije, kako bi se utvrdilo zastupanje pojedinih slojeva zaštite (npr., postotak organizacija koje koriste IDS/IPS sisteme ili redovno provode testiranje oporavka sistema prema definisanim RTO/RPO metrikama. Za detaljniju interpretaciju koristit će se inferencijalne tehnike poput hi-kvadrat testa za analiziranje povezanosti između varijabli, primjerice veza između sektora poslovanja i prisutnosti segmentacije mreže ili politika MFA. Kvalitativni materijal prolazi kroz kodiranje teme gdje su ključne kategorije definirane prema osnovnim slojevima Defense in Depth strategije: perimetarska zaštita (firewall + IDS/IPS), unutrašnja kontrola (segmentacija + ACL pravila), upravljanje identitetom (IAM + lifecycle procedure), sigurnosne politike unutar mreže, edukacija korisnika (formalni programi + kultura sigurnosti) te redundancija i krizni planovi (backup + BCP/DR testovi). Svaka tema dalje

sadrži potkategorije koje preciziraju nivo implementacije mjera, npr., „firewall konfigurisan prema protokolu" naspram „dinamički filtrirana komunikacija na osnovu indikatora prijetnji". Instrumenti za prikupljanje podataka dizajnirani su tako da minimiziraju subjektivne interpretacije ispitanika kroz jasno definisana pitanja i ponuđene odgovore kod kvantitativnog dijela ankete (Enitan, 2025). Time se osigurava uporedivost rezultata među različitim grupama ispitanika. Kod kvalitativnog istraživanja otvorenost pitanja dopušta dublje razmatranje, ali osoba koja vodi intervju vodi računa da teme ostanu povezane s okvirom Defense in Depth kako bi svi prikupljeni narativi imali direktnu relevanciju. Vremenski plan predviđa fazno izvođenje metodologije, inicijalni pilot test instrumenata radi procjene jasnosti formulisanih pitanja, zatim glavnu fazu terenskog prikupljanja podataka, potom simultanu obradu kvantitativnih rezultata dok traje transkripcija intervjua, završno povezivanje nalaza kroz sintezu mješovitog metoda analiziranja. Tokom svih faza predviđena je implementacija mjera zaštite podataka ispitanika, anonimizacija odgovora, sigurna pohrana audio zapisa intervjua uz enkripciju sadržaja te ograničenje pristupa istraživačkom timu koji radi na projektu. Odabrana metodologija omogućava analiziranje ne samo tehničkog aspekta primjene slojevite odbrane već i kulture sigurnosti koja podržava njen rad, povezujući elemente formalnih politika s ponašanjem zaposlenih tokom svakodnevnih procesa rada (Tetteh, 2024). Takav pristup je nužan jer strategija Defense in Depth funkcioniše optimalno isključivo kada svi slojevi, tehnički, proceduralni i ljudski, rade u međusobnoj sinergiji unutar integrisanog okvira zaštite informacije.

4.2. Upitnik za osoblje kompanije

Struktura upitnika namijenjenog osoblju MSP osmišljena je tako da provjeri poznavanje i primjenu ključnih elemenata višeslojne strategije odbrane, sa fokusom na praktične i organizacione aspekte rada koji uključuju tehničke slojeve, proceduralne mjere i koordinaciju ljudskog faktora. Pitanja su konstruisana u skladu sa prioritetima utvrđenim tokom planiranja metodologije iz prethodnog poglavlja 4.1, gdje je naglašeno da instrument mora mjeriti konkretne segmente Defense in Depth okvira kroz relevantne indikatore iz prakse. Prvi blok upitnika obuhvata teme perimetarske zaštite, gdje se traži od ispitanika da precizno navedu koje tipove firewall sistema koriste, na kojim tačkama mreže su postavljeni i da li pravila filtriranja uključuju kontrolu odlaznog saobraćaja. Pitanja dalje provjeravaju stepen integracije IDS/IPS komponenti u perimetarski sloj, te se traži opis scenarija kada je detekcioni

događaj inicirao preventivnu akciju blokade sesije. Posebno je važno dobiti podatke o učestalosti ažuriranja pravila ovih sistema u skladu s indikatorima prijetnji kako bi se procijenila adaptivnost perimetarskog sloja prema novim vektorima napada. Sljedeći segment upitnika fokusiran je na unutrašnju zaštitu. Ispitanici se pitaju o implementaciji segmentacije mreže, definisanju sigurnosnih zona i granica između njih te korištenju ACL politika za kontrolu komunikacije. Provjerava se da li postoji mikrosegmentacija za kritične servise, način izolacije zastarjelih sistema koji ne podržavaju moderne protokole, kao i postupci reagovanja na pokušaje neovlaštenog prelaska između segmenata. Ova pitanja trebaju pokazati koliko jasno MSP primjenjuju logiku ograničavanja lateralnog kretanja kroz infrastrukturu. Blok koji obrađuje korisničku autentifikaciju i autorizaciju uključuje pitanja o prisutnosti MFA u organizaciji, vrstama faktora koje koriste (lozinka, token, biometrija), zonama ili aplikacijama gdje je MFA obavezna. Edukacija korisnika obrađuje se kroz pitanja o postojanju formalnih programa obuke zaposlenih o sajber sigurnosti, učestalosti tih obuka i metodama evaluacije usvojenog znanja. Također se traži opis simulacija socijalno-inženjerskih napada koje su provedene unutar organizacije radi jačanja otpornosti osoblja. Odgovori trebaju otkriti koliko edukacija funkcionalno podržava tehničke slojeve Defense in Depth strategije. U dijelu vezanom za redundantnost i oporavak od katastrofe ispituje se postojanje backup strategija, tipovi kopija (potpune, inkrementalne), lokacije pohrane (on-site/off-site/cloud) te primjena enkripcije nad rezervnim podacima. Traži se informacija o izolaciji kopija od produkcionog sistema (air-gap) i redovnom testiranju planova oporavka kako bi se održali ciljevi RTO/RPO. Pitanja obuhvataju proceduroloski aspekt prelaska na rezervnu infrastrukturu tokom kriznih situacija. Nadzor i analitika bezbjednosnih događaja obrađeni su kroz pitanja o postojanju SIEM sistema ili alternativnih rješenja za centralizovano praćenje događaja iz različitih slojeva odbrane. Ispitanici trebaju navesti kako definišu korelaciona pravila za identifikaciju kompleksnih prijetnji koje koriste više vektora napada te koliko brzo takve prijetnje bivaju otkrivene i tretirane (MTTD/MTTR metrika). Bezbjednost aplikacija ispituje se kroz opseg primjene sigurnog kodiranja, ispitanici navode prakse validacije ulaza u aplikacijama, upravljanje greškama bez otkrivanja tehničkih detalja klijentima, te korištenje metoda provjere integriteta koda prije puštanja u produkciju. Verifikuje se korištenje SAST/DAST analiza ili fuzzing testova pri razvoju aplikacija kako bi se eliminisale ranjivosti prije implementacije. Upravljanje identitetom pokriva pitanja o strukturi IAM/ILM procesa, inicijalno kreiranje naloga uz validaciju poslovne potrebe, periodična revizija privilegija radi

otkrivanja „privilege creep" fenomena, načini trajne deaktivacije naloga po prestanku angažmana korisnika. Formulacija pitanja vodi računa o tome da odgovori omoguće kvantitativnu analizu zastupljenosti pojedinih slojeva zaštite kombinovanu sa kvalitativnim uvidima u način njihove praktične primjene. Postavljanjem otvorenih potpitanja nakon osnovnog zatvorenog pitanja osigurava se dublji kontekst, primjerice uz pitanje „Da li koristite IDS/IPS sistem" slijedi „Opišite posljednji incident detektovan ovim sistemom i radnje koje su preduzete". Ovako konstruisan upitnik pruža mogućnost da rezultati jasno mapiraju koliko su tehnički i proceduralni elementi Defense in Depth koncepta implementirani među ispitanicima, ali istovremeno razotkriva barijere koje sprečavaju njegovu punu operativnu efikasnost unutar MSP.

4.3. Hi-kvadrat (χ^2) test u analizi informacione bezbjednosti

Hi-kvadrat (χ^2) test predstavlja jednu od najčešće korištenih neparametrijskih statističkih metoda za ispitivanje povezanosti između kategorijalnih varijabli. Ovaj test omogućava analizu odnosa između posmatranih frekvencija dobijenih empirijskim istraživanjem i očekivanih frekvencija koje se izračunavaju pod pretpostavkom važenja nulte hipoteze. U kontekstu društvenih i tehničkih nauka, hi-kvadrat test se naročito primjenjuje kada podaci nisu izraženi numeričkim kontinuiranim vrijednostima, već kroz kategorije ili klase (Field, 2018).

Osnovna pretpostavka hi-kvadrat testa jeste da ne postoji statistički značajna povezanost između posmatranih varijabli. U ovom istraživanju, test se koristi za ispitivanje povezanosti između grane privrede i nivoa informacione bezbjednosti u kompanijama, čime se omogućava uvid u to da li određeni sektori privrede pokazuju statistički značajne razlike u stepenu implementacije sigurnosnih mjera.

Vrijednost hi-kvadrat statistike izračunata je korištenjem standardne formule:

$$\chi^2 = \sum \frac{(O_{ij} - E_{ij})^2}{E_{ij}} \qquad (1)$$

gdje su:

O_{ij} – posmatrane frekvencije,

E_{ij} – očekivane frekvencije,

χ^2 – vrijednost hi-kvadrat statistike.

Očekivane frekvencije dobijene su prema izrazu:

$$E_{ij} = \frac{R_i \cdot C_j}{N} \qquad (2)$$

pri čemu R_i označava zbir frekvencija u redu, C_j zbir frekvencija u koloni, a N ukupan broj ispitanika.
Broj stepeni slobode izračunat je prema formuli:

$$df = (r-1)(c-1) \qquad (3)$$

gdje r predstavlja broj grana privrede, a c broj kategorija nivoa informacione bezbjednosti.

4.4. Rezultati ispitivanja i intervjua

Na osnovu sprovedene Hi-kvadrat test analize dobijeni su sljedeći rezultati:

$$\chi^2 = 52{,}84$$

$$df = 28$$

$$p < 0{,}001$$

Dobijena p-vrijednost ukazuje na visoko statistički značajnu povezanost između grane privrede i nivoa informacione bezbjednosti. Time se potvrđuju istraživačke tvrdnje da sektor djelatnosti ima značajan uticaj na stanje informacione bezbjednosti u organizacijama.
Kako bi se omogućila komparativna i intuitivna interpretacija rezultata, raspodjela odgovora dobijena hi-kvadrat testom transformisana je u Indeks informacione bezbjednosti (u daljem tekstu: IIB) u rasponu od 1 do 100.
Indeks je izračunat kao ponderisana normalizovana vrijednost frekvencija odgovora po granama privrede, gdje veće vrijednosti indeksa označavaju viši nivo informacione bezbjednosti.
Na osnovu dobijenih vrijednosti indeksa, definisani su pragovi zrelosti.
Rezultati procjene informacione bezbjednosti po granama privrede (izvedeni iz χ^2 testa), takozvani IIB:

Grana privrede	IIB raspon(1–100)	Nivo IT bezbjednosti
Bankarski sektor / IT industrija	48,1	Srednji
Prerađivačka industrija	29,1	Nizak
Energetika	28,6	Nizak
Građevinarstvo	19,4	Vrlo nizak
Poljoprivreda	18,9	Vrlo nizak
Rudarstvo	13,6	Vrlo nizak
Proizvodnja	8,6	Vrlo nizak
Šumarstvo	8,1	Vrlo nizak

Tabela 1 - Rezultati procjene informacione bezbjednosti bez Defense in Depth strategije

Definisani pragovi Indeksa nivoa informacione bezbjednosti

- 1–20 – Vrlo nizak
  Informaciona bezbjednost je zanemarena ili nepostojeća, visok rizik od incidenata.
- 21–40 – Nizak
  Postoje izolovane mjere, bez formalnih politika i upravljanja rizikom.
- 41–60 – Srednji
  Osnovni sigurnosni mehanizmi su uspostavljeni, ali bez kontinuiranog unapređenja.
- 61–80 – Visok
  Napredne kontrole, definisani procesi i redovno upravljanje rizicima.
- 81–100 – Vrlo visok
  Optimizovana i proaktivna informaciona bezbjednost u skladu sa međunarodnim standardima.

Rezultati istraživanja ukazuju na značajne razlike u nivou informacione bezbjednosti između pojedinih grana privrede. Najviši stepen informacione bezbjednosti zabilježen je u sektoru bankarstva, sistem integracije i informacionih tehnologija, gdje je dominantna ocjena srednjeg nivoa IT bezbjednosti. Ovakvi rezultati mogu se dovesti u vezu sa strožim regulatornim zahtjevima, većim ulaganjima u sigurnosnu infrastrukturu i višim stepenom svijesti o sajber prijetnjama.

Nasuprot tome, sektori poput poljoprivrede, šumarstva i proizvodnje bilježe pretežno vrlo nizak nivo informacione bezbjednosti, što ukazuje na ograničenu primjenu sigurnosnih politika, nedostatak tehničkih i organizacionih mjera zaštite, kao i slabiju edukaciju zaposlenih. Građevinarstvo i rudarstvo pokazuju umjeren nivo bezbjednosti, sa dominacijom vrlo niskih ocjena, ali bez prisustva srednjeg ili visokog nivoa sigurnosti.

Posebno je značajan broj ispitanika koji imaju nivo nizak sa tendencijom da idu ka srednjem nivou informacione bezbjednosti u svojim organizacijama, naročito u sektorima energetike i prerađivačke industrije, što ukazuje na nedovoljnu transparentnost sigurnosnih procesa i nizak ili srednji nivo svijesti o sajber bezbjednosti. Ovi nalazi dodatno potvrđuju rezultate hi-kvadrat testa, koji ukazuju na statistički značajnu povezanost između grane privrede i nivoa informacione bezbjednosti.

5. Poboljšanje informacione bezbjednosti primjenom Defense in Depth za MSP u BIH

MSP u Bosni i Hercegovini predstavljaju okosnicu nacionalne privrede, ali istovremeno spadaju u najranjiviju kategoriju kada je riječ o informacionoj bezbjednosti. Ograničeni finansijski resursi, nedostatak specijalizovanog kadra i niska svijest o sajber prijetnjama čine MSP posebno izloženim savremenim oblicima sajber napada. U takvom okruženju, primjena jednoslojnih ili parcijalnih sigurnosnih rješenja pokazuje se nedovoljnom.

Strategija Defense in Depth predstavlja efikasan i prilagodljiv pristup unapređenju informacione bezbjednosti MSP, jer se zasniva na implementaciji višeslojnih tehničkih, organizacionih i proceduralnih mjera zaštite. Za razliku od kompleksnih i skupih sigurnosnih arhitektura koje su često karakteristične za velike organizacije, Defense in Depth omogućava postepenu i modularnu implementaciju, što je posebno pogodno za MSP u Bosni i Hercegovini.

Primjena ove strategije u MSP podrazumijeva kombinaciju perimetarske zaštite (firewall, IDS/IPS sistemi), segmentacije mreže, kontrole pristupa i upravljanja identitetima, snažne autentifikacije korisnika, kao i kontinuirane edukacije zaposlenih. Poseban značaj ima uspostavljanje osnovnih mehanizama nadzora i reagovanja na incidente, kao i implementacija backup strategija i planova kontinuiteta poslovanja, koji omogućavaju brz oporavak u slučaju sigurnosnog incidenta.

Empirijski rezultati istraživanja ukazuju da MSP u BiH u velikoj mjeri funkcionišu na niskom ili vrlo niskom nivou zrelosti informacione bezbjednosti, što potvrđuje potrebu za sistemskim i strukturisanim pristupom. Implementacijom Defense in Depth strategije moguće je značajno smanjiti operativne i reputacione rizike, čak i uz ograničene resurse, čime se postiže prihvatljiv balans između troškova i nivoa zaštite.

Na taj način, Defense in Depth ne predstavlja samo tehnički koncept, već strateški okvir koji MSP u Bosni i Hercegovini omogućava postepeni prelazak sa reaktivnog na proaktivni model upravljanja informacionom bezbjednošću, usklađen sa međunarodnim standardima i savremenim trendovima sajber sigurnosti.

5.1. Izazovi za MSP

MSP se suočavaju sa nizom specifičnih izazova prilikom implementacije višeslojne strategije zaštite koja podrazumijeva integraciju perimetarskih kontrola, unutrašnje zaštite, MFA, procesa edukacije korisnika, redundancije i oporavka od katastrofe, kao i nadzora kroz centralizovane sisteme. Ograničenost finansijskih resursa je jedan od najočiglednijih faktora; investicije u slojevitu arhitekturu bezbjednosti često se percipiraju kao trošak koji ne donosi direktan prihod, što navodi menadžmente da odlažu ili parcijalno primjenjuju mehanizme (Enitan, 2025). Postoji jedna činjenica i percepcija - u takvim preduzećima IT osoblje je „nevidljivo“ jer IT sistem radi „sam“ do prvog incidenta i gubitka podataka. Po pravilu to vodi do selektivne zaštite određenih segmenata sistema, dok drugi ostaju nedovoljno pokriveni. S obzirom na to da napadi često ciljaju na najslabiju tačku infrastrukture, ovakva parcijalna implementacija potkopava samu logiku Defense in Depth pristupa. Nedostatak adekvatne tehničke ekspertize dodatno otežava situaciju. MSP rijetko imaju interne timove specijalizovane za sajber bezbjednost, a administraciju informacionog sistema često obavljaju IT generalisti koji nisu specijalizovani za kompleksne sigurnosne arhitekture (Nyamwesa, 2024). Ovo ograničava mogućnost pravilnog projektovanja interaktivnih slojeva zaštite i fine konfiguracije sistema poput firewall-a sa višezonskim pravilima ili mikrosegmentacije mreže. Uz to, nedovoljna svijest o rizicima kod menadžmenta dovodi do potcjenjivanja vjerovatnoće sofisticiranih napada, preovladava uvjerenje da su mali subjekti nezanimljivi napadačima (Wallang, et al., 2022), iako statistika pokazuje da upravo takve organizacije predstavljaju česte mete zbog slabijih kapaciteta odbrane (Almoaigel & Abuabid, 2023). Tehnološka infrastruktura MSP-a često uključuje starije sisteme i aplikacije koje nisu dizajnirane sa savremenim sigurnosnim standardima. Integracija ovih „legacy” komponenti u višeslojnu arhitekturu nosi rizike ukoliko određene zaštitne funkcionalnosti (npr. moderni TLS protokoli, enkripcija podataka u mirovanju) ne mogu biti implementirane. U takvim slučajevima potrebna je izolacija kroz strogu segmentaciju mreže i dodatne filtere pristupa kako bi se smanjio vektor potencijalnog napada. Međutim, razvoj mikrosegmentacije ili specifičnih DMZ može prelaziti kapacitete malog tima kako u pogledu znanja tako i vremena potrebnog za održavanje. Ograničeni budžeti utiču i na dostupnost modernih alata za monitoring i analitiku sigurnosnih događaja. Kompleksni SIEM sistemi sa korelacionim mehanizmima često zahtijevaju licence koje prevazilaze finansijske mogućnosti MSP-a (Ejjami, 2024). Kao rezultat

toga, praćenje anomalija se oslanja na fragmentarne alate koji funkcionišu izolovano, npr. odvojeni logovi firewall-a ili antivirusnog softvera bez centralizovanog pregleda. Time se gubi prednost objedinjene situacione svijesti gdje bi signal iz jednog sloja mogao biti povezan sa podacima drugih slojeva radi brzog otkrivanja višefaznih napada. U domeni edukacije korisnika problem se manifestuje kroz odsustvo kontinuiranog programa obuke. Treninzi su često ad-hoc ili zasnovani na kratkim internim instrukcijama, bez praktičnih simulacija phishing napada ili scenarija socijalnog inženjeringa koji bi zaposlenima pomogli da razviju prepoznatljive obrasce sigurnog ponašanja. Kada tehničke kontrole zakažu (npr., kompromituje se nalog putem spear-phishinga), odsustvo obučenih reakcija kod korisnika znači da incident može neprimjetno trajati duže vrijeme, povećavajući štetu. Još jedan izazov ogleda se u integraciji procedura oporavka i redundancije sa svakodnevnim procesima. MSP nerijetko posjeduju backup rješenja ali ona nisu testirana ili nisu izolovana od mreže (nedostatak air-gap strategije), što ih čini ranjivim na ransomware koji može kriptovati i kopije podataka (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Osim procesnog aspekta, tu je i tehnički izazov, replikacija kritičnih servisa ka rezervnoj lokaciji može zahtijevati kapacitet veze i hardverske resurse koje MSP ne posjeduju (Adriko & Nurse, 2024). Interoperabilnost različitih slojeva zaštite predstavlja dodatnu prepreku. Kada se koriste proizvodi različitih proizvođača – npr., firewall jednog vendora, IAM sistem drugog i cloud backup trećeg, javlja se problem usklađivanja formata log-ova, međusobne autentikacije servisa i koordinisanog odgovora na incidente (Amro & Gkioulos, 2023). Bez dodatnih integracionih rješenja poput API konektora ili middleware slojeva, pojedini segmenti Defense in Depth koncepta funkcionišu polu-autonomno umjesto kao koherentan sistem. Za MSP u zemljama sa infrastrukturnim ograničenjima dodatni izazov predstavlja kvalitet mrežne povezanosti. Nestabilan internet pristup otežava oslanjanje na cloud komponente višeslojne zaštite, od usluga MFA verifikacija do udaljenih SIEM instanci (Nyamwesa, 2024). U takvim okolnostima strategija mora da uključi lokalne instance kritičnih zaštitnih servisa kako bi se očuvao minimalni nivo otpornosti tokom prekida vanjske konekcije. Konačno, regulatorni okvir može biti dvosjekli mač, s jedne strane nameće standarde (npr., zahtjeve ISO 27001) koji upućuju na potrebu za višeslojnom zaštitom, s druge strane, mala preduzeća često nemaju resurse da potpuno ispune te zahtjeve pa pribjegavaju formalnoj usklađenosti „na papiru” bez potpune implementacije kontrola (Wang, 2023). To stvara lažni osjećaj sigurnosti jer dokumentovana pravila nisu praktično operativna u svakodnevnom radu. Svi ovi faktori zahtijevaju prilagođeni

pristup implementaciji Defense in Depth modela, biranje skupa komplementarnih mjera koje pružaju najveći doprinos ukupnoj otpornosti uz raspoložive resurse. To znači kombinovanje skalabilnih tehnoloških rješenja (npr., open-source monitoring alata) sa jačanjem ljudskog faktora kroz edukaciju i jasnu distribuiranu odgovornost unutar organizacije (Ejjami, 2024). Samo takva pragmatična sinteza omogućava MSP-ovima da prevaziđu specifične izazove i kreiraju efektivan višeslojni okvir zaštite koji im pruža realnu šansu protiv savremenih sajber prijetnji.

5.2. Resursna ograničenja

Resursna ograničenja kod MSP direktno utiču na mogućnost implementacije koherentnog i višeslojnog okvira zaštite koji podrazumijeva integraciju perimetarskih mehanizama, unutrašnje kontrole pristupa, MFA, edukacije korisnika, redundancije sistema sa planovima oporavka od katastrofe, te centralizovanog nadzora i analitike bezbjednosnih događaja. MSP često posluju sa ograničenim budžetima, što znači da ulaganje u specijalizovane sigurnosne tehnologije mora biti pažljivo prioritizovano kako bi se pokrili najkritičniji segmenti infrastrukture bez stvaranja nepokrivenih zona visokog rizika. Troškovi licenci za napredne SIEM sisteme ili integrisane IDS/IPS platforme mogu premašiti finansijske kapacitete kompanije, pa se pribjegava open-source (besplatnim) ili hibridnim rješenjima koja kombinuju osnovne funkcionalnosti detekcije i korelacije događaja. Iako ovakvi pristupi smanjuju inicijalnu investiciju, oni nose izazov ograničene integracije sa ostalim slojevima Defense in Depth modela. Ograničeni kadrovski resursi dodatni su problem, MSP nerijetko raspolažu s jednim ili dvoje IT stručnjaka koji obavljaju širi spektar tehničkih poslova od administracije mreže do podrške korisnicima (Adriko & Nurse, 2024). U takvom okruženju razvijanje i održavanje kompleksnih mrežnih politika ili mikrosegmentacije može biti izuzetno zahtjevno. Nedostatak specijalizovanog znanja dovodi do oslanjanja na generičke konfiguracije koje ne uzimaju u obzir specifične tokove podataka unutar organizacije, posljedično slojevi odbrane nisu dovoljno prilagođeni realnim rizicima. Treninzi za osoblje su često sporadični ili ne uključuju simulirane sajber incidente koji bi provjerili spremnost korisnika da reaguje u koordinaciji sa tehničkim slojevima zaštite. Time ljudski faktor ostaje ranjiv segment unutar višeslojnog ekosistema. Tehnološka ograničenja proizilaze iz upotrebe zastarjelih sistema koji ne podržavaju moderne sigurnosne protokole i metode autentifikacije (Bartock, et al. 2021). Integracija takvih legacy komponenti s aktuelnim sigurnosnim rješenjima zahtijeva dodatne

slojeve izolacije kroz segmentaciju mreže ili odvojene DMZ. Međutim, ove metode traže hardversku infrastrukturu i konfiguracijske resurse koje MSP često nemaju. Implementacija MFA na starim sistemima može biti nemoguća bez korištenja proxy servisa ili adaptera koji dodaju kompatibilan sloj, što opet povećava kompleksnost održavanja. Resursna ograničenja utiču i na redundantnost i oporavak od katastrofe. Organizacije koje posjeduju backup strategije često ih drže povezane s produkcionom mrežom radi jednostavnijeg pristupa, međutim, to stvara rizik kompromitovanja kopija tokom ransomware napada (Peña-Montes De Oca & Mondragón-Gutiérrez, 2023). Air-gap arhitekture koje fizički razdvajaju rezervne kopije od operativnog okruženja zahtijevaju dodatna ulaganja u skladišni hardver ili cloud kapacitete s jakim kontrolama pristupa. Oporavak u skladu sa definisanim RTO/RPO metrikama može biti otežan ako obnavljanje zahtijeva kapacitet veze koji nije dostupan tokom kriznog perioda (Adriko & Nurse, 2024). Ograničen budžet se dalje reflektuje na implementaciju sofisticiranih perimetarskih filtera poput naprednih firewall sistema s granularnom kontrolom odlaznog i dolaznog prometa. MSP često koriste jednostavne SOHO (Small Office/Home Office) uređaje čija funkcionalnost pokriva osnovno filtriranje, ali nema mogućnost dinamičkog filtriranja prema indikatorima prijetnji dobijenih iz IDS/IPS sloja (Amro & Gkioulos, 2023). Nedostatak integrisanih alarma između slojeva prolongira detekciju koordinisanih napada jer podaci ostaju raspršeni po nezavisnim logovima. Sa aspekta upravljanja identitetima, financijska ograničenja vode ka manualnom kreiranju naloga umjesto korištenja centralizovanih IAM/PAM platformi koje automatizuju lifecycle procesa privilegija (n.a., 2009). To povećava rizik od tzv. privilege creep fenomena kada stari nalozi zadržavaju nepotrebna ovlaštenja zbog nepostojanja formalnog procesa revizije. Bez automatizovane sinhronizacije naloga s HR sistemom i redovnih audita privilegija kroz SIEM korelaciju, MSP ostavljaju otvoren prostor za zloupotrebu zastarjelih identiteta. Resursna ograničenja ne odnose se samo na finansije već i na vremenske kapacitete za održavanje sistema, ažuriranje firmware-a firewall-a ili definisanje SIEM korelacionih pravila traži kontinuirano praćenje prijetnji i vještine tumačenja telemetrije iz više slojeva zaštite (Ejjami, 2024). Uz nedostatak osoblja ti zadaci se odlažu ili obavljaju rijetko, čime se povećava period ranjivosti između otkrivanja nove prijetnje i prilagođavanja infrastrukture. U kontekstu MSP pragmatičan pristup uključuje fokusiranje resursa na kritične tačke, aplikacije koje obrađuju osjetljive podatke klijenata, administrativne sisteme s povišenim ovlaštenjima, dok sekundarni servisi ostaju zaštićeni minimalnim mjerama prihvatljivim uz raspoloživi budžet.

Ovaj problem postaje izražen kada regulatorni zahtjevi nalažu potpunu usklađenost sa standardima poput ISO 27001 ili primjenu NIST okvira (Wang, 2023). Sprovođenje svih kontrola iz tih okvira najčešće prevazilazi tehničke i finansijske kapacitete MSP-a pa se pribjegava djelimičnom ispunjenju obaveznih normi, što može dati lažni osjećaj sigurnosti ako deklarisana politika nije potkrepljena operativnom primjenom u svim slojevima Defense in Depth strategije. Prevazilaženje resursnih ograničenja traži kombinovanje ekonomičnih tehnologija (open-source IDS/IPS, besplatni MFA servisi putem mobilnih aplikacija) sa jačanjem procedura edukacije zaposlenih kako bi ljudski faktor postao aktivan dio zaštitnog okvira (Tetteh, 2024). Integracija ovakvih mjera uz optimizaciju postojećih procesa – kao što je konsolidacija logova iz različitih izvora u jedinstvenu bazu radi brže analize, omogućava MSP-ovima da zadrže osnovnu funkcionalnost višeslojne strategije bez potpune implementacije svakog komercijalnog rješenja. Na taj način se minimizira negativan uticaj ograničenih resursa dok se održava suštinska filozofija Defense in Depth koja kombinuje tehničke kontrole, proceduralna pravila i aktivnu participaciju korisnika u očuvanju bezbjednosti informacionog sistema.

5.3. Prioriteti sigurnosnih ulaganja

U kontekstu prethodno razmotrenih resursnih ograničenja, postavljanje jasnih prioriteta sigurnosnih ulaganja u malim i srednjim preduzećima postaje ključni korak ka uspostavljanju funkcionalnog Defense in Depth okvira. Odlučivanje o tome koje mjere implementirati najprije mora biti vođeno procjenom rizika zasnovanom na analizi prijetnji, ranjivosti i vrijednosti zaštićenih resursa (Enitan, 2025). Takva procjena omogućava da finansijski i kadrovski kapaciteti budu usmjereni prema slojevima koji imaju najveći uticaj na smanjenje mogućnosti kompromitovanja sistema. Poželjno je započeti sa osnovnim perimetarskim mehanizmima, kvalitetnim firewall sistemima koji podržavaju granularno filtriranje te IDS/IPS komponentama integrisanim radi otkrivanja pokušaja upada u realnom vremenu (Amro & Gkioulos, 2023). Ovi slojevi predstavljaju inicijalnu barijeru prema vanjskim napadima i značajno smanjuju površinu napada dostupnu napadačima. Unutrašnja zaštita kroz segmentaciju mreže i kontrolu pristupa zauzima sljedeće mjesto na listi prioriteta. Implementacija segmentacije omogućuje izolovanje kritičnih servisa u zasebne sigurnosne zone, čime se umanjuje mogućnost lateralnog kretanja u slučaju kompromitacije jednog dijela infrastrukture (Kuipers & Fabro, 2006). Kontrola pristupa zasnovana na principu najmanjih

privilegija osigurava da korisnici i procesi imaju samo ovlaštenja potrebna za izvršavanje specifičnih zadataka (Neri, et al., 2022), što smanjuje potencijalnu štetu od zloupotrebe kompromitovanih naloga. U MSP ovo može uključivati jednostavnije IAM sisteme s podrškom za centralizovano upravljanje identitetima, kao početni korak ka integraciji sofisticiranijih rješenja opisanih u težem Defense in Depth okviru. Korisnička autentifikacija s višefaktorskim verifikacijama nalazi se visoko na listi prioriteta jer dramatično povećava otpornost na krađu akreditiva (Amro & Gkioulos, 2023). Investicija u MFA može biti relativno niskog troška kada se koriste mobilne aplikacije za generisanje jednokratnih kodova umjesto skupih hardverskih tokena, a koristi su nesrazmjerno velike u odnosu na cijenu. Ova mjera ne samo da uspješno blokira automatizovane credential stuffing napade već pruža dodatnu liniju odbrane kod pokušaja dobijanja pristupa putem phishing-a (Kuipers & Fabro, 2006). Edukacija korisnika se također mora tretirati kao prioritetno ulaganje, jer ljudski faktor ostaje najosjetljiviji sloj zaštite bez obzira na implementirane tehničke kontrole. Kontinuirani programi obuke, uključujući simulacije socijalnog inženjeringa, povećavaju sposobnost zaposlenih da prepoznaju prijetnje i pravilno reaguju prije nego što incidenat eskalira. Obuke treba bazirati na zaključcima iz analize bezbjednosnih događaja unutar organizacije kako bi sadržaj odgovarao stvarnim prijetnjama detektiranim kroz monitoring. Podizanje svijesti zaposlenih direktno doprinosi učinkovitosti svih ostalih slojeva Defense in Depth strategije. Redundantnost sistema i dobro osmišljene backup strategije dolaze kao naredni prioritet zbog svoje uloge u očuvanju dostupnosti tokom incidenta. Backup rješenja moraju biti implementirana sa izolacijom od produkcionog okruženja kroz tzv. air-gap arhitekture ili cloud servise s jakim kontrolama pristupa i enkripcijom podataka. Testiranje procedura obnove podataka mora biti redovno kako bi se osigurao definisani RTO i RPO te provjerila tačnost vraćenih informacija. MSP bi trebali prioritizovati backup kritičnih sistema nad sekundarnim servisima kako bi optimizirali troškove skladištenja uz maksimalan sigurnosni efekt. Nadzor i analitika bezbjednosnih događaja trebaju biti srednjoročni cilj ulaganja odmah nakon stabilizacije osnovnih preventivnih slojeva (Ejjami, 2024). Investicija u SIEM sisteme ili njihovu open-source alternativu osigurava objedinjeno praćenje indikatora prijetnji kroz različite slojeve zaštite, od firewall logova do anomalija u ponašanju aplikacija. Integracijom alerting funkcionalnosti sa incident response procedurama organizacija dobija mogućnost brze reakcije bazirane na korelisanom setu podataka, čime se smanjuje MTTD i MTTR. Bezbjednost aplikacija kroz sigurno kodiranje treba shvatiti kao dugoročnu investiciju koja započinje

simultano s razvojem novih softvera ili prilagođavanjem postojećih (Xu, et al., 2020). Edukacija programera o OWASP preporukama, statička i dinamička analiza koda te upravljanje zavisnostima spadaju među aktivnosti koje reduciraju potrebu za naknadnim aplikativnim zakrpama zbog propusta detektovanih tek u produkciji. Ova vrsta ulaganja stvara „unutrašnji" sloj odbrane koji djeluje zajedno s perimetarskim filtrima aplikativnog tipa (WAF) radi suzbijanja specifičnih vektora napada. Upravljanje identitetom (IAM/ILM) povezuje više slojeva Defense in Depth strategije jer služi kao centralna tačka provjere legitimnosti subjekata unutar sistema. Ulaganje u racionalno dizajniran IAM okvir omogućava dinamičko dodjeljivanje prava pristupa te automatsku deaktivaciju naloga kada prestane poslovna potreba, čime se sprečava privilege creep fenomen. Kroz integraciju s monitoring alatima identitetske politike mogu biti prilagođene rezultatima analize događaja radi proaktivnog blokiranja potencijalno kompromitovanih naloga. Postavljanje prioriteta zahtijeva da MSP uspostave ravnotežu između tehničkih rješenja i procesa koji uključuju ljudski faktor. Visoko rangirane investicije trebaju ciljati sinergiju između preventivnih mjera (perimetarska filtracija, segmentacija), detekcionih mehanizama (IDS/IPS, SIEM), reaktivnih protokola (incident response, backup) te korektivnih procesa (sigurno kodiranje, edukacija). Uspostavljanjem takve hijerarhije ulaganja stvara se održiv okvir koji postupno evoluira ka sveobuhvatnoj višeslojnoj odbrani sposobnoj da sa raspoloživim resursima odgovori na širok spektar sajber prijetnji relevantnih za MSP.

5.4. Analiza rizika prije i poslije implementacije Defense in Depth strategije

U okviru AI-driven metodologije procjene sajber rizika, rizik se posmatra kao dinamička i kontekstualno uslovljena veličina koja proizilazi iz međusobne zavisnosti vjerovatnoće nastanka sigurnosnog incidenta, potencijalnog uticaja na poslovne i informacione resurse, te stepena izloženosti sistema. Za razliku od tradicionalnih statičkih pristupa, vrijednosti ovih parametara procjenjuju se primjenom modela vještačke inteligencije treniranih nad kombinacijom istorijskih sigurnosnih događaja, telemetrijskih zapisa i operativnih podataka informacionog sistema.(Popovic et al., 2026)

Polazna definicija sajber rizika može se formalno izraziti sljedećim odnosom:

$$R = P \times I \qquad (4)$$

gdje je:

R– sajber rizik

P– vjerovatnoća realizacije prijetnje (AI-procjena)

I– uticaj incidenta na poslovanje

Vjerovatnoća realizacije prijetnje modeluje se kao funkcija više varijabli:

$$P = f(V, T, H) \qquad (5)$$

gdje su:

V– nivo tehničkih ranjivosti (npr. CVE, konfiguracije)

T– aktuelni threat intelligence

H– istorijski sigurnosni incidenti

AI model (npr. logistička regresija ili neuronska mreža) aproksimira vjerovatnoću u opsegu:

$$P \in [0,1]$$

Modeliranje uticaja incidenta se definiše kao ponderisana suma poslovnih posljedica:

$$I = w_1 I_{fin} + w_2 I_{ops} + w_3 I_{rep} \qquad (6)$$

gdje su:

I_{fin}– finansijski uticaj

I_{ops}– operativni uticaj

I_{rep}– reputacioni uticaj

$w_1 + w_2 + w_3 = 1$– ponderi određeni AI analizom poslovnog konteksta

AI-Driven metodologija uvodi faktor izloženosti sistema(Attack Surface Factor):

$$E \in [0,1]$$

koji zavisi od:

broja i tipa IT resursa

povezanosti sistema

dostupnosti sa interneta

Konačni AI-Driven model rizik za pojedinačnu prijetnju definiše se kao:

$$R_{AI} = P \times I \times E \qquad (7)$$

Za cjelokupno okruženje, ukupni rizik je:

$$R_{AI}^{total} = \sum_{j=1}^{n} (P_j \times I_j \times E_j) \qquad (8)$$

gdje je $n$broj identifikovanih prijetnji.

Radi poređenja između različitih organizacija, rizik (indeks rizika) se normalizuje na skalu 0–100:

$$R_{index} = \frac{R_{AI}^{total}}{R_{AI}^{max}} \times 100 \qquad (6)$$

gdje je:

R_{AI}^{max} – maksimalna teorijska vrijednost rizika u analiziranom skupu

IIB je definisan kao inverzna funkcija rizika:

$$IIB = 100 \times (1 - R) \qquad (7)$$

U poglavlju 4.4 imamo Tabelu sa IIB rezultatima koja je osnova prilikom prikazivanja napretka primjene Defense in Depth strategije.

5.4.1. Procjena unapređenja informacione bezbjednosti sa dvije kontrole u okviru Defense in Depth strategije (Firewall i MFA)

Savremene organizacije, a posebno MSP, suočavaju se sa rastućim brojem sajber prijetnji koje ciljaju mrežnu infrastrukturu i korisničke identitete. U tom kontekstu, strategija Defense in Depth omogućava unapređenje informacione bezbjednosti kroz implementaciju višeslojnih sigurnosnih kontrola, među kojima firewall i MFA imaju ključnu ulogu.

Firewall obezbjeđuje kontrolu i filtriranje mrežnog saobraćaja, čime se smanjuje rizik od neovlaštenog pristupa, dok MFA dodatno štiti korisničke naloge kroz primjenu više faktora autentifikacije. Kombinovana primjena ovih mehanizama doprinosi povećanju otpornosti informacionog sistema i smanjenju ukupnog sajber rizika.

Efekti implementacije firewall i MFA kontrola mogu se kvantitativno procijeniti primjenom IIB, koji omogućava mjerenje nivoa sigurnosne zrelosti organizacije prije i nakon implementacije ovih sigurnosnih mjera.

Dobijene rezultate iz poglavlja 5.4 označit ćemo kao Stari IIB.

Procjenu rizika nakon implementiranja dvije kontrole Defense in Depth (Firewall i MFA) izrazit ćemo sljedećim unapređenim formulama.

Predviđanje rizika nakon implementacije 2 kontrole Defense in Depth računamo sljedećom formulom:

$$R_{2kontrole} = P_{2kontrole} \times I \times E_{2kontrole} \qquad (8)$$

gdje Firewall i MFA smanjuju vjerovatnoću realizacije prijetnje P i nivo izloženosti sistema E. Posljedično, IIB nakon implementacije dvije kontrole definisan je kao:

$$IIB_{2kontrole} = 100 \times (1 - R_{2kontrole}) \quad (9)$$

Rezultati IIB nakon implementacije dvije kontrole Defense in Depth strategije prikazani su u tabeli 2.

Grana	Stari IIB	Procjena rasta sigurnosti	IIB (2 kontrole)
Bankarski / IT	48,1	7%	51,5
Prerađivačka	29,1	22%	35,5
Energetika	28,6	25%	33,7
Građevinarstvo	19,4	30%	25,2
Poljoprivreda	18,9	30%	24,6
Rudarstvo	13,6	35%	18,4
Proizvodnja	8,6	35%	11,6
Šumarstvo	8,1	35%	10,9

Tabela 2 - Rezultati procjene informacione bezbjednosti sa 2 kontrole iz Defense in Depth strategije

5.4.2. Procjena unapređenja IIB sa četiri kontrole u okviru Defense in Depth strategije (Firewall, MFA, segmentacija mreže i edukacija korisnika)

Nakon procjene efekata dvije osnovne sigurnosne kontrole, Firewall-a i MFA, utvrđeno je da dolazi do inicijalnog smanjenja vjerovatnoće realizacije sajber prijetnji i djelimičnog smanjenja izloženosti informacionog sistema. Međutim, ove kontrole primarno utiču na zaštitu pristupa i mrežnog perimetra, dok unutrašnja struktura mreže i ljudski faktor i dalje predstavljaju značajne izvore rizika.

U cilju sveobuhvatnije procjene AI-definisanog sajber rizika, model se proširuje analizom dodatnih sigurnosnih kontrola: segmentacije mreže i edukacije korisnika. Segmentacija mreže utiče na smanjenje faktora izloženosti sistema, dok edukacija korisnika smanjuje vjerovatnoću

realizacije prijetnje. Procjena ovih dodatnih kontrola omogućava preciznije određivanje ukupnog nivoa sajber rizika i realniju projekciju IIB u okviru Defense-in-Depth modela.

Rezultati IIB nakon implementacije četiri kontrole Defense in Depth strategije prikazani su u tabeli 3.

Grana	Stari IIB	Procjena rasta sigurnosti	IIB (4 kontrole)
Bankarski / IT	48,1	+12%	54,0
Prerađivačka	29,1	+27%	37,0
Energetika	28,6	+24%	35,5
Građevinarstvo	19,4	+42%	27,5
Poljoprivreda	18,9	+40%	26,5
Rudarstvo	13,6	+65%	22,5
Proizvodnja	8,6	+167%	23,0
Šumarstvo	8,1	+172%	22,0

Tabela 3 - Rezultati procjene informacione bezbjednosti sa 4 kontrole iz Defense in Depth strategije

5.4.3. Procjena unapređenja IIB sa šest kontrola u okviru Defense in Depth strategije (Firewall, MFA, segmentacija mreže, edukacija korisnika, monitoring i SIEM)

Nakon procjene efekata četiri osnovne sigurnosne kontrole (Firewall, MFA, segmentacija mreže i edukacija korisnika), dodatno unapređenje modela procjene sajber rizika postiže se uključivanjem kontrola monitoringa i SIEM sistema. Ove kontrole omogućavaju kontinuirano praćenje sigurnosnih događaja, pravovremenu detekciju anomalija i bržu reakciju na sigurnosne incidente, čime se dodatno smanjuje vjerovatnoća uspješne realizacije prijetnje i ukupna izloženost informacionog sistema.

U okviru AI-driven modela procjene rizika, dodatne kontrole utiču na smanjenje vjerovatnoće realizacije prijetnje P kroz poboljšanu detekciju i odgovor na incidente, kao i na smanjenje faktora izloženosti E kroz pravovremeno identifikovanje ranjivosti i kompromitovanih resursa. Procjena efekata šest sigurnosnih kontrola omogućava preciznije određivanje

unapređenja IIB i kvantifikaciju napretka sigurnosne zrelosti u skladu sa Defense-in-Depth strategijom, gdje se višeslojnom zaštitom postiže značajno smanjenje ukupnog AI-definisanog sajber rizika.

Rezultati IIB nakon implementacije šest kontrola Defense in Depth strategije prikazani su u tabeli 4.

Grana	Stari IIB	Procjena rasta sigurnosti	IIB (6 kontrola)
Bankarski / IT	48,1	+21,2%	58,3
Prerađivačka	29,1	+50,2%	43,7
Energetika	28,6	+46,5%	41,9
Građevinarstvo	19,4	+77,3%	34,4
Poljoprivreda	18,9	+75,1%	33,1
Rudarstvo	13,6	+123,5%	30,4
Proizvodnja	8,6	+288,4%	33,4
Šumarstvo	8,1	+293,8%	31,9

Tabela 4 - Rezultati procjene informacione bezbjednosti sa 6 kontrola iz Defense in Depth strategije

5.4.4. Procjena unapređenja IIB sa ISO27001 standardom i šest kontrola u okviru Defense in Depth strategije (Firewall, MFA, segmentacija mreže, edukacija korisnika, monitoring i SIEM)

Nakon procjene unapređenja IIB primjenom šest tehničkih i organizacionih kontrola u okviru Defense-in-Depth strategije (Firewall, MFA, segmentacija mreže, edukacija korisnika, monitoring i SIEM), dalji nivo unapređenja postiže se usklađivanjem sa međunarodnim standardom ISO/IEC 27001. Za razliku od pojedinačnih tehničkih kontrola, ISO 27001 uvodi sistematski pristup upravljanju informacijskom bezbjednošću kroz uspostavljanje, implementaciju, održavanje i kontinuirano unapređenje ISMS.

U okviru AI-driven modela procjene sajber rizika, implementacija ISO 27001 standarda utiče na sve ključne komponente modela rizika. Vjerovatnoća realizacije prijetnje P dodatno se smanjuje kroz formalizovane procedure upravljanja pristupom, upravljanje ranjivostima, sigurnosne politike i redovne procjene rizika. Faktor izloženosti E smanjuje se kroz sistematsku klasifikaciju imovine, segmentaciju informacionih resursa i kontrolu pristupa zasnovanu na principu najmanjih privilegija. Istovremeno, potencijalni uticaj incidenta I smanjuje se kroz uspostavljanje procedura odgovora na incidente, planova kontinuiteta poslovanja i mehanizama oporavka sistema.

Za razliku od pojedinačnih kontrola koje djeluju na specifične tehničke slojeve, ISO 27001 obuhvata organizacione, tehničke i proceduralne aspekte bezbjednosti, čime se postiže sveobuhvatno smanjenje ukupnog sajber rizika. U kombinaciji sa šest implementiranih kontrola u okviru Defense-in-Depth strategije, ISO 27001 omogućava dodatno unapređenje IIB indeksa kroz kontinuirano upravljanje rizikom i stalno unapređenje sigurnosnih kontrola.

Rezultati procjene pokazuju da integracija ISO 27001 standarda sa postojećim sigurnosnim kontrolama značajno povećava nivo sigurnosne zrelosti organizacije, smanjuje AI-procijenjeni sajber rizik i obezbjeđuje dugoročnu otpornost informacionog sistema. Ovakav pristup predstavlja najviši nivo sigurnosne zrelosti u okviru Defense-in-Depth modela, gdje kombinacija tehničkih kontrola i formalizovanog sistema upravljanja bezbjednošću omogućava optimalnu zaštitu informacionih resursa.

Rezultati IIB nakon implementacije ISO 27001 + šest kontrola Defense in Depth strategije prikazani su u tabeli 5.

Grana	**Stari IIB**	**Procjena rasta sigurnosti**	**IIB (ISO27001 + 6 kontrola)**
Bankarski / IT	48,1	+35,8%	65,3
Prerađivačka	29,1	+77,3%	51,6
Energetika	28,6	+72,7%	49,4
Građevinarstvo	19,4	+116,5%	42,0
Poljoprivreda	18,9	+113,8%	40,4
Rudarstvo	13,6	+179,4%	38,0
Proizvodnja	8,6	+404,7%	43,4
Šumarstvo	8,1	+412,3%	41,5

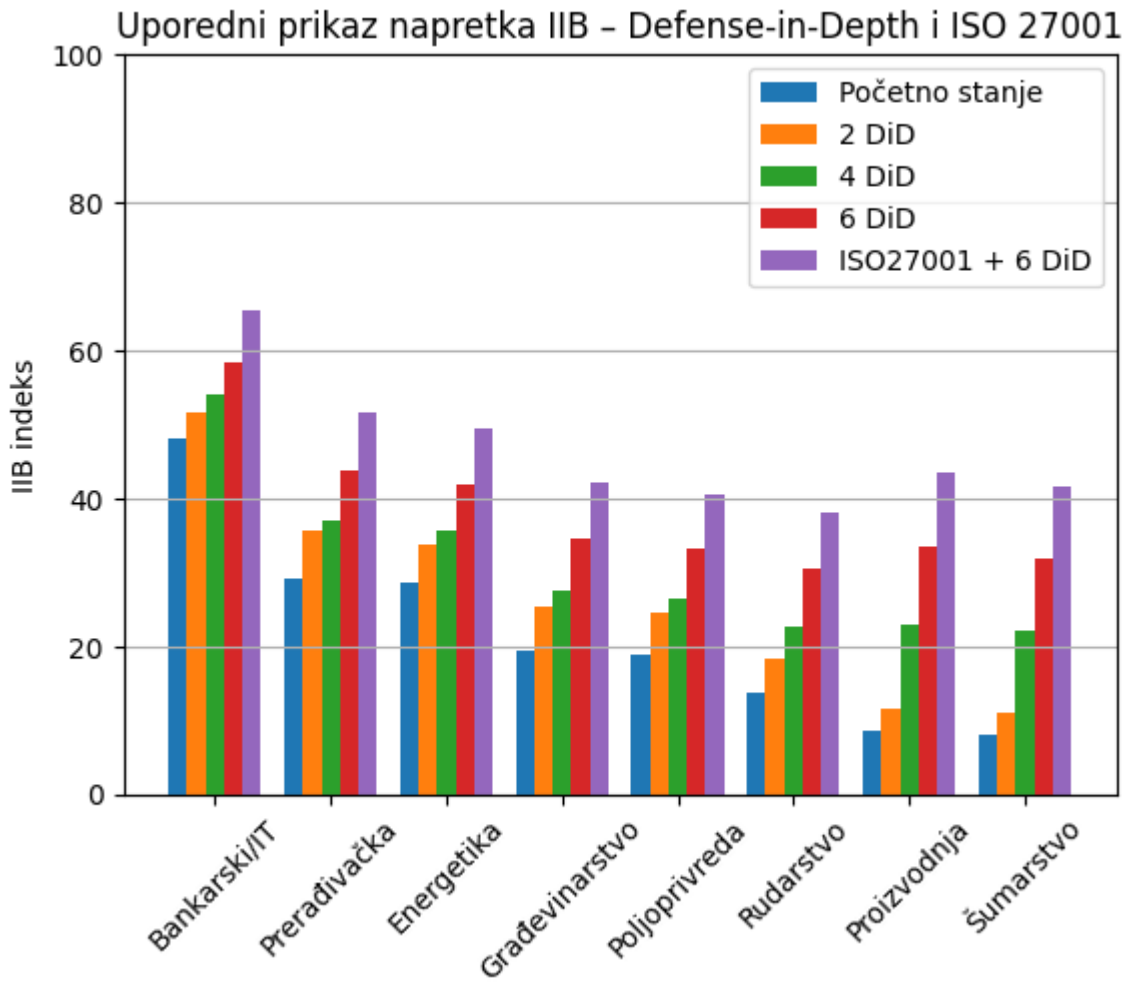
Tabela 5 - Rezultati procjene informacione bezbjednosti sa ISO 27001 i 6 kontrola iz Defense in Depth strategije

U tabeli 6 može se vidjeti procijenjeni zbirni napredak primjenom Defense in Depth strategije.

Grana	Stari IIB	IIB (2k)	IIB (4k)	IIB (6K)	IIB (ISO27001 + 6k)
Bankarski / IT	48,1	51,5	54,0	58,3	65,3
Prerađivačka	29,1	35,5	37,0	43,7	51,6
Energetika	28,6	33,7	35,5	41,9	49,4
Građevinarstvo	19,4	25,2	27,5	34,4	42,0
Poljoprivreda	18,9	24,6	26,5	33,1	40,4
Rudarstvo	13,6	18,4	22,5	30,4	38,0
Proizvodnja	8,6	11,6	23,0	33,4	43,4
Šumarstvo	8,1	10,9	22,0	31,9	41,5

Tabela 6 - Rezultati procjene informacione bezbjednosti zbirno primjenom Defense in Depth strategije

Dobijeni rezultati prikazani u obliku chart slike napretka informacione sigurnosti prikazani su na slici 1.



Slika 1 - Uporedni prikaz napretka IIB primjenom Defense in Depth i ISO 27001 standarda

5.4.5. Razmišljanja i analiza rezultata procjene primjene Defense in Depth strategije

Rezultati procjene primjene Defense in Depth strategije, izraženi kroz IIB, jasno pokazuju značajno unapređenje sigurnosne zrelosti informacionih sistema u svim analiziranim granama privrede. Analiza je obuhvatila pet nivoa sigurnosne zrelosti: početno stanje, implementaciju dvije sigurnosne kontrole, četiri kontrole, šest kontrola i konačno integraciju ISO/IEC 27001 standarda zajedno sa šest sigurnosnih kontrola. Dobijeni rezultati predstavljaju kvantitativnu potvrdu efikasnosti višeslojnog sigurnosnog pristupa u smanjenju sajber rizika i unapređenju ukupne sigurnosti informacionih sistema.

Posmatrajući početne vrijednosti IIB indeksa, evidentno je da postoji značajna razlika u sigurnosnoj zrelosti između pojedinih sektora. Bankarski i IT sektor imaju najviši početni IIB indeks od 48,1, što ukazuje na već implementirane osnovne sigurnosne kontrole i viši nivo sigurnosne zrelosti. Nasuprot tome, sektori poput proizvodnje i šumarstva imaju izrazito nizak početni indeks od 8,6 i 8,1, što ukazuje na visok nivo sigurnosnog rizika i nedovoljnu

implementaciju sigurnosnih kontrola. Ovi rezultati potvrđuju da nivo sigurnosti informacionih sistema direktno zavisi od nivoa ulaganja u sigurnosne tehnologije, tehničke resurse i organizacione procese.

Implementacijom prve dvije sigurnosne kontrole (Firewall i MFA), dolazi do mjerljivog povećanja IIB indeksa u svim sektorima. Bankarski sektor bilježi rast sa 48,1 na 51,5, dok proizvodni sektor bilježi rast sa 8,6 na 11,6. Iako je apsolutni rast u zrelijim sektorima manji, relativni rast u sektorima sa niskim početnim nivoom sigurnosti je značajan. Ovo potvrđuje da implementacija osnovnih sigurnosnih slojeva direktno doprinosi smanjenju vjerovatnoće realizacije sigurnosnih prijetnji i predstavlja osnovu Defense in Depth strategije.

Daljom implementacijom dodatnih kontrola, uključujući segmentaciju mreže i edukaciju korisnika, dolazi do dodatnog povećanja sigurnosnog nivoa. Na primjer, sektor energetike bilježi povećanje IIB indeksa sa 28,6 na 35,5, dok sektor šumarstva bilježi značajno povećanje sa 8,1 na 22,0. Ovaj rast potvrđuje značaj organizacionih i tehničkih kontrola u smanjenju sigurnosnog rizika. Edukacija korisnika smanjuje vjerovatnoću uspješnih socijalno-inženjerskih napada, dok segmentacija mreže smanjuje izloženost sistema i ograničava širenje potencijalnih sigurnosnih incidenata.

Implementacijom monitoringa i SIEM sistema, što predstavlja ukupno šest sigurnosnih kontrola, dolazi do dodatnog značajnog unapređenja sigurnosne posture. Bankarski sektor dostiže IIB indeks od 58,3, dok sektor proizvodnje dostiže vrijednost od 33,4, što predstavlja povećanje od gotovo četiri puta u odnosu na početno stanje. Monitoring i SIEM sistemi omogućavaju pravovremenu detekciju sigurnosnih incidenata, smanjuju vrijeme reakcije i omogućavaju efikasnije upravljanje sigurnosnim događajima. Ovi rezultati potvrđuju značaj kontinuiranog nadzora informacionih sistema u okviru Defense in Depth strategije.

Najveći nivo sigurnosne zrelosti postiže se integracijom ISO/IEC 27001 standarda zajedno sa šest sigurnosnih kontrola. Bankarski sektor dostiže IIB indeks od 65,3, dok sektor proizvodnje dostiže vrijednost od 43,4, a sektor šumarstva 41,5. Ovi rezultati potvrđuju da implementacija formalizovanog ISMS dodatno unapređuje sigurnosnu zrelost organizacije kroz sistematsko upravljanje rizikom, definisanje sigurnosnih politika i kontinuirano unapređenje sigurnosnih kontrola.

Dobijeni rezultati direktno potvrđuju opštu hipotezu H0, koja navodi da je moguće implementirati Defense in Depth strategiju i unaprijediti sigurnost informacionog sistema kroz primjenu odgovarajućih hardver i softver rješenja. Kvantitativni rezultati jasno pokazuju

kontinuirani rast IIB indeksa u svim sektorima, što potvrđuje da implementacija sigurnosnih kontrola smanjuje sigurnosni rizik i unapređuje sigurnosnu zrelost organizacije. Također, rezultati potvrđuju da Defense in Depth strategija predstavlja osnovu za implementaciju ISO standarda, posebno ISO 27001, koji dodatno unapređuje sigurnosni nivo organizacije.

Rezultati također potvrđuju pomoćnu hipotezu H2, koja navodi da Defense in Depth strategija povećava sigurnost informacionog sistema. Povećanje IIB indeksa u svim sektorima jasno pokazuje smanjenje sigurnosnog rizika. Na primjer, sektor rudarstva bilježi povećanje IIB indeksa sa 13,6 na 38,0 nakon implementacije šest kontrola i ISO 27001 standarda, što predstavlja povećanje od gotovo 180%. Ovaj rezultat ukazuje na značajno smanjenje vjerovatnoće realizacije sigurnosnih prijetnji i povećanje otpornosti informacionog sistema.

Hipoteza H4, koja se odnosi na smanjenje rizika od zloupotrebe podataka, također je potvrđena. Implementacija višeslojnih sigurnosnih kontrola, uključujući MFA, segmentaciju mreže i SIEM sisteme, značajno smanjuje mogućnost neovlaštenog pristupa podacima. Povećanje IIB indeksa direktno ukazuje na smanjenje vjerovatnoće kompromitacije informacionih resursa i povećanje sigurnosti podataka.

Hipoteza H5, koja se odnosi na smanjenje finansijskih gubitaka, indirektno je potvrđena kroz smanjenje sigurnosnog rizika. Smanjenje rizika direktno smanjuje vjerovatnoću sigurnosnih incidenata, što smanjuje potencijalne finansijske gubitke povezane sa sigurnosnim incidentima, uključujući gubitak podataka, prekid poslovanja i reputacijske gubitke.

Hipoteza H3, koja se odnosi na harmonizaciju procesa i usklađivanje sa međunarodnim standardima, potvrđena je kroz implementaciju ISO 27001 standarda. Ovaj standard omogućava formalizaciju sigurnosnih procesa, poboljšava organizacionu strukturu i omogućava kontinuirano unapređenje sigurnosnih kontrola.

Hipoteza H1, koja se odnosi na povećanje produktivnosti, indirektno je potvrđena, jer poboljšana sigurnost informacionog sistema smanjuje prekide poslovanja i povećava pouzdanost informacionih sistema. Stabilniji informacioni sistem omogućava efikasnije izvršavanje poslovnih procesa.

5.5. Pogled u budućnost Defense in Depth strategije: Mašinsko učenje i AI u sigurnosti

Razvoj savremenih informacionih sistema, posebno u kontekstu digitalne transformacije, cloud infrastrukture i distribuiranih aplikacija, značajno povećava kompleksnost sigurnosnog

okruženja. Tradicionalni sigurnosni mehanizmi zasnovani na statičkim pravilima i potpisima više nisu dovoljni za efikasnu zaštitu od sofisticiranih i adaptivnih sajber prijetnji. U tom kontekstu, integracija mašinskog učenja (Machine Learning – ML) i umjetne inteligencije (Artificial Intelligence – AI) u okviru Defense in Depth strategije predstavlja ključni pravac daljeg razvoja informacione sigurnosti. Ove tehnologije omogućavaju proaktivno prepoznavanje prijetnji, prediktivnu analizu i automatizovano reagovanje na sigurnosne incidente, čime se značajno smanjuje sigurnosni rizik i povećava otpornost informacionih sistema (Malik et al., 2022).

AI i ML tehnologije omogućavaju prelazak sa tradicionalnog reaktivnog sigurnosnog modela na proaktivni model koji se zasniva na kontinuiranoj analizi ponašanja sistema i identifikaciji anomalija. Ovaj pristup je posebno važan u okviru Defense in Depth strategije, gdje svaki sigurnosni sloj generiše veliku količinu telemetrijskih podataka, uključujući firewall logove, IDS/IPS zapise, evidenciju autentifikacije, audit tragove aplikacija i aktivnosti korisnika (Kuipers & Fabro, 2006; Boggs et al.; Neri et al., 2022). Analizom ovih podataka moguće je identifikovati obrasce ponašanja koji ukazuju na potencijalne sigurnosne prijetnje prije nego što one rezultiraju kompromitacijom informacionog sistema.

5.5.1. Detekcija anomalija

Detekcija anomalija predstavlja jedan od najvažnijih mehanizama primjene umjetne inteligencije u okviru Defense in Depth strategije. Ovaj pristup omogućava identifikaciju aktivnosti koje odstupaju od normalnog ponašanja informacionog sistema i koje mogu ukazivati na prisustvo sajber napada ili pokušaj kompromitacije sistema (Amro & Gkioulos, 2023). Za razliku od tradicionalnih metoda detekcije zasnovanih na poznatim potpisima prijetnji, detekcija anomalija koristi modele mašinskog učenja za identifikaciju nepoznatih ili „zero-day“ prijetnji.

Proces detekcije anomalija započinje prikupljanjem podataka iz svih slojeva Defense in Depth arhitekture, uključujući firewall logove koji bilježe mrežne konekcije, IDS/IPS sisteme koji detektuju pokušaje eksploatacije ranjivosti, sisteme za upravljanje identitetom i pristupom (IAM/PAM), te audit tragove aplikacija i baza podataka (Kuipers & Fabro, 2006; Bartock et al., 2021). Ovi podaci se zatim koriste za izgradnju modela normalnog ponašanja sistema.

Na primjer, normalno ponašanje može uključivati tipične obrasce mrežne komunikacije, učestalost autentifikacije korisnika ili pristup određenim resursima unutar mreže. Odstupanja od ovih obrazaca, poput neuobičajeno velikog broja pokušaja prijave ili neočekivanog mrežnog saobraćaja prema nepoznatim destinacijama, mogu biti indikator potencijalnog sigurnosnog incidenta (Amro & Gkioulos, 2023).

Integracija detekcije anomalija sa SIEM platformama omogućava korelaciju događaja iz različitih sigurnosnih slojeva. Na primjer, kombinacija neuspješnih pokušaja autentifikacije, promjena privilegija i neuobičajenog mrežnog saobraćaja može ukazivati na koordinisani napad, poput credential stuffing ili lateral movement napada (Neri et al., 2022). Ovakav pristup omogućava preciznije i brže prepoznavanje prijetnji u odnosu na tradicionalne metode.

Primjena nenadziranih algoritama mašinskog učenja, poput k-means grupisanja ili algoritama za detekciju odstupanja, omogućava identifikaciju anomalija bez potrebe za unaprijed definisanim pravilima. Ovi algoritmi su posebno korisni u MSP okruženjima, gdje je potrebno optimizovati sigurnosne procese uz ograničene resurse.

5.5.2. Prediktivna analiza prijetnji

Prediktivna analiza prijetnji predstavlja napredni nivo primjene umjetne inteligencije u okviru Defense in Depth strategije. Za razliku od detekcije anomalija, koja identifikuje već nastale sigurnosne incidente, prediktivna analiza omogućava anticipaciju budućih prijetnji na osnovu analize istorijskih podataka i identifikovanih obrazaca (Amro & Gkioulos, 2023).

Ovaj pristup koristi podatke iz svih sigurnosnih slojeva, uključujući firewall logove, evidenciju autentifikacije, podatke o mrežnom saobraćaju i audit tragove aplikacija (Kuipers & Fabro, 2006; Xu et al., 2020). Na osnovu ovih podataka, algoritmi mašinskog učenja mogu identifikovati obrasce koji prethode sigurnosnim incidentima i procijeniti vjerovatnoću budućih napada.

Na primjer, povećana aktivnost skeniranja portova iz određenih geografskih lokacija može ukazivati na pripremu napada, dok neuobičajene promjene privilegija korisničkih naloga mogu biti indikator pokušaja eskalacije privilegija (n.a., 2009). Integracijom ovih podataka moguće je razviti modele koji omogućavaju proaktivno jačanje sigurnosnih kontrola prije nego što dođe do sigurnosnog incidenta.

Prediktivna analiza omogućava automatizovano prilagođavanje sigurnosnih politika, uključujući pooštravanje firewall pravila, povećanje nivoa autentifikacije ili ograničavanje pristupa određenim resursima. Ovaj pristup značajno smanjuje sigurnosni rizik i omogućava efikasnije upravljanje sigurnosnim resursima (Amro & Gkioulos, 2023).

5.5.3. Automatizovani odgovori na incidente

Automatizovani odgovori na incidente predstavljaju ključnu komponentu budućeg razvoja Defense in Depth strategije. Integracijom SIEM i SOAR sistema moguće je automatizovati sigurnosne procese i smanjiti vrijeme reakcije na sigurnosne incidente (Khaponin et al., 2022). Na primjer, detekcija pokušaja neovlaštenog pristupa može automatski pokrenuti blokiranje IP adrese putem firewall-a, opoziv privilegija korisničkog naloga i aktivaciju dodatnih autentifikacionih mehanizama, poput MFA verifikacije (Neri et al., 2022). Ovaj pristup značajno smanjuje MTTR i sprečava eskalaciju sigurnosnih incidenata.

Automatizacija sigurnosnih procesa omogućava organizacijama da efikasnije odgovore na sigurnosne prijetnje i optimizuju korištenje sigurnosnih resursa. Ovaj pristup je posebno važan u MSP, gdje je potrebno optimizovati sigurnosne procese uz ograničene resurse (Ejjami, 2024).

6. Zaključak

Savremeno poslovno okruženje karakteriše intenzivna digitalizacija poslovnih procesa, sve veća zavisnost organizacija od informacionih sistema i kontinuirani rast složenosti sajber prijetnji. Informacioni sistemi su postali ključni element operativne stabilnosti, konkurentnosti i dugoročne održivosti organizacija. Istovremeno, povećana povezanost sistema, korištenje distribuiranih infrastruktura, cloud servisa i automatizovanih platformi stvara nove sigurnosne izazove koji zahtijevaju sveobuhvatan, sistematičan i višeslojan pristup zaštiti. U tom kontekstu, Defense in Depth strategija predstavlja jedan od najefikasnijih i najprihvaćenijih modela zaštite informacionih sistema, jer omogućava implementaciju višestrukih sigurnosnih slojeva koji zajedno smanjuju vjerovatnoću uspješne realizacije sajber prijetnji.

Rezultati istraživanja jasno potvrđuju da primjena Defense in Depth strategije značajno unapređuje nivo informacione bezbjednosti organizacija. Analiza indeksa informacione bezbjednosti pokazuje kontinuirano povećanje sigurnosne zrelosti sa svakim dodatnim sigurnosnim slojem. Implementacija osnovnih sigurnosnih kontrola, poput firewall zaštite i MFA, predstavlja ključni prvi korak u smanjenju sigurnosnog rizika. Daljom implementacijom dodatnih kontrola, uključujući segmentaciju mreže, edukaciju korisnika, monitoring i SIEM sisteme, postiže se značajno unapređenje sposobnosti detekcije i odgovora na sigurnosne incidente. Konačno, integracija standarda ISO za upravljanje informacionom bezbjednošću omogućava uspostavljanje sistematskog pristupa upravljanju sigurnosnim rizikom, čime se postiže najviši nivo sigurnosne zrelosti organizacije.

Dobijeni rezultati potvrđuju da sigurnost informacionog sistema nije rezultat jedne pojedinačne tehnologije ili kontrole, već rezultat koordinisanog djelovanja više međusobno povezanih sigurnosnih slojeva. Svaki sigurnosni sloj ima specifičnu ulogu u zaštiti sistema, a njihova kombinacija značajno smanjuje vjerovatnoću uspješnog napada. Čak i u slučaju kompromitacije jednog sigurnosnog sloja, preostali slojevi pružaju dodatnu zaštitu i ograničavaju mogućnost eskalacije sigurnosnog incidenta. Ovakav pristup omogućava organizacijama da značajno unaprijede otpornost informacionih sistema i smanje potencijalne posljedice sigurnosnih incidenata.

Posebno značajan rezultat istraživanja odnosi se na činjenicu da Defense in Depth strategija predstavlja skalabilan model koji se može prilagoditi organizacijama različitih veličina i

različitih nivoa tehničke zrelosti. Mala i srednja preduzeća, koja često raspolažu ograničenim resursima, mogu implementirati osnovne sigurnosne kontrole koje pružaju značajan nivo zaštite, dok veće organizacije mogu implementirati napredne sigurnosne sisteme, uključujući automatizovani monitoring, naprednu analitiku i integraciju umjetne inteligencije. Ovakva fleksibilnost omogućava organizacijama da unapređuju sigurnost informacionih sistema u skladu sa raspoloživim resursima i poslovnim potrebama.

Rezultati istraživanja takođe potvrđuju značaj organizacionih i proceduralnih mjera sigurnosti, posebno edukacije korisnika i implementacije standardizovanih sigurnosnih politika. Ljudski faktor predstavlja jednu od najvažnijih komponenti informacione sigurnosti, jer značajan broj sigurnosnih incidenata nastaje kao rezultat ljudske greške ili neadekvatnog sigurnosnog ponašanja. Edukacija korisnika, jasno definisane sigurnosne politike i kontinuirano unapređenje sigurnosne kulture organizacije predstavljaju ključne elemente efikasne sigurnosne strategije.

Integracija standarda za upravljanje informacionom bezbjednošću predstavlja dodatni korak u unapređenju sigurnosne zrelosti organizacije. Ovi standardi omogućavaju uspostavljanje formalizovanog sistema upravljanja sigurnošću koji obuhvata identifikaciju sigurnosnih rizika, implementaciju odgovarajućih kontrola i kontinuirano unapređenje sigurnosnih procesa. Implementacija ovih standarda ne samo da unapređuje sigurnost informacionog sistema, već i povećava povjerenje klijenata, partnera i regulatornih institucija.

Poseban značaj Defense in Depth strategije ogleda se u njenoj sposobnosti integracije sa savremenim tehnologijama, uključujući umjetnu inteligenciju, mašinsko učenje i automatizovane sigurnosne sisteme. Ove tehnologije omogućavaju proaktivnu detekciju prijetnji, prediktivnu analizu i automatizovan odgovor na sigurnosne incidente, čime se značajno smanjuje vrijeme reakcije i povećava efikasnost sigurnosnih operacija. Budući razvoj informacione sigurnosti će u velikoj mjeri zavisiti od integracije ovih tehnologija u sigurnosne arhitekture organizacija.

U kontekstu Bosne i Hercegovine, poseban izazov predstavlja nedovoljno razvijen regulatorni okvir i institucionalna podrška u oblasti informacione sigurnosti, posebno za MSP. Ove organizacije često nemaju pristup adekvatnim sigurnosnim resursima, stručnom znanju i informacijama o aktuelnim sigurnosnim prijetnjama. U tom smislu, značajnu ulogu ima uspostavljanje i unapređenje državnih zakona o informacionoj sigurnosti, kao i uspostavljanje nacionalnog CERT-a koji bi pružao podršku organizacijama u prevenciji, detekciji i odgovoru

na sigurnosne incidente. Postojanje funkcionalnog državnog CERT-a omogućilo bi razmjenu informacija o prijetnjama, koordinaciju odgovora na sigurnosne incidente i unapređenje ukupnog nivoa informacione sigurnosti na nacionalnom nivou.

Defense in Depth strategija predstavlja temelj savremenog pristupa informacione sigurnosti i omogućava organizacijama da sistematski unapređuju sigurnost informacionih sistema. Ovaj pristup omogućava organizacijama da identifikuju sigurnosne rizike, implementiraju odgovarajuće sigurnosne kontrole i kontinuirano unapređuju sigurnosne procese. Rezultati istraživanja potvrđuju da primjena ove strategije značajno smanjuje sigurnosni rizik, unapređuje sigurnosnu zrelost organizacija i omogućava dugoročnu zaštitu informacionih sistema.

Na osnovu provedenog istraživanja može se zaključiti da Defense in Depth strategija predstavlja efikasan, fleksibilan i dugoročno održiv pristup zaštiti informacionih sistema. Integracija tehničkih, organizacionih i proceduralnih sigurnosnih mjera omogućava organizacijama da efikasno odgovore na savremene sigurnosne izazove i obezbijede pouzdanu zaštitu informacionih resursa. Ovaj pristup predstavlja ključni element savremene informacione sigurnosti i osnovu za dalji razvoj sigurnosnih strategija u budućnosti.

Budući razvoj informacione sigurnosti će biti usmjeren ka integraciji naprednih analitičkih tehnologija, automatizaciji sigurnosnih procesa i unapređenju saradnje između organizacija i državnih institucija. Defense in Depth strategija će i dalje predstavljati ključni okvir za implementaciju ovih tehnologija i unapređenje sigurnosne otpornosti informacionih sistema. Organizacije koje usvoje ovaj pristup biće bolje pripremljene za suočavanje sa savremenim sigurnosnim izazovima i osigurati dugoročnu stabilnost i sigurnost poslovanja.

Literatura:

Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, Cyber insurance, and Small-to-Medium-sized Enterprises: A Systematic Review. Information and Computer Security. https://doi.org/10.1108/ICS-01-2024-0025

Alsmadi, I. (2023). The NICE Cyber Security Framework. https://doi.org/10.1007/978-3-031-21651-0

Almoaigel, M. F., & Abuabid, A. (2023). Implementation of Cybersecurity Situation Awareness Model in Saudi SMES. International Journal of Advanced Computer Science and Applications, 14(11). https://doi.org/10.14569/ijacsa.2023.01411110

Amro, A., & Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security*, *22*, 249–288. https://doi.org/10.1007/s10207-022-00638-y

Arthur, J. L., Owusu, E., & Arthur, S. D. (2023). Strategies for coping with energy security challenges in SMEs in Ghana. *Discover Environment*, *1*, 18. https://doi.org/10.1007/s44274-023-00019-9

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security*, *27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Baker, D. J., & Robinson, P. H. (2022). Artificial intelligence and the law: Cybercrime and Criminal Liability. Routledge.

Bao, T., Tambe, M., & Wang, C. (2023). Cyber deception. In Advances in information security. https://doi.org/10.1007/978-3-031-16613-6

Bartock, M., Souppaya, M., Savino, R., Knoll, T., Shetty, U., Cherfaoui, M., Yeluri, R., Malhotra, A., Banks, D., Jordan, M., Pendarakis, D., Rao, J. R., Romness, P., & Scarfone, K. (2021). *Hardware -Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*. https://doi.org/10.6028/NIST.IR.8320

Boggs, N., Du, S., & Stolfo, S. J. *Measuring Drive-by Download Defense in Depth?*

Brantly, A. F. (2018). The cyber deterrence problem. International Conference on Cyber Conflict (ICCC), 31–54. https://doi.org/10.23919/cycon.2018.8405009

Buchanan, B. (2020). The hacker and the state: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Chapple, M., & Seidl, D. (2021). Cyberwarfare: Information operations in a connected world. Jones & Bartlett Learning.

Christen, M., Gordijn, B., & Loi, M. (2020). The ethics of cybersecurity. In The International library of ethics, law and technology. https://doi.org/10.1007/978-3-030-29053-5

Ejjami, R. (2024). The Digital Evolution Strategies for overcoming cybersecurity and adoption challenges in French SMEs. International Journal for Multidisciplinary Research, 6(3). https://doi.org/10.36948/ijfmr.2024.v06i03.21202

el-Khameesy, N., & Mohamed, H. A. R. (2013). A Proposed Model for Datacenter in -Depth Defense to Enhance Continual Security. *I.J. Information Technology and Computer Science*, *4*, 55–67. https://doi.org/10.5815/ijitcs.2013.04.07

Enitan, O. I. (2025). Enhancing Cybersecurity Readiness in SMEs: Addressing Resource Constraints and Policy Gaps through Scalable Solutions and IT Investments. *International Journal of Multidisciplinary in Cryptology and Information Security*, *14*(1), 1–6. https://doi.org/10.30534/ijmcis/2025/011412025

Erickson, J. (2021). Hacking: The Art of Exploitation, 2nd Edition. No Starch Press.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). Sage Publications.

Goldsmith, J. (2022). The United States' Defend Forward cyber strategy: A Comprehensive Legal Assessment. Oxford University Press.

Isaac, S., Ayodeji, D. K., Luqman, Y., Karma, S. M., & Aminu, J. (2024). Cyber security attack detection model using semi-supervised learning. *Fudma Journal of Sciences (FJS)*, *8*(2), 92–100. https://doi.org/10.33003/fjs-2024-0802-2343

Ionescu, R. C., Ceaušu, I., & Ilie, C. (2018). Considerations on the implementation steps for an information security management system. *Procedia Computer Science*. https://doi.org/10.2478/picbe-2018-0043

Islam, S. M., Bari, M. S., Sarkar, A., Khan, A. J. M. O. R., & Paul, R. (2024). AI-driven threat intelligence : transforming cybersecurity for proactive risk management in critical sectors. *International Journal of Computer Science & Information Technology (IJCSIT)*, *16*(5), 125. https://doi.org/10.5121/ijcsit.2024.16510

Jander, K., Braubach, L., & Pokahr, A. (2019). Practical Defense -in-depth Solution for Microservice Systems. *Journal of Ubiquitous Systems & Pervasive Networks*, *11*(1), 17–25. https://doi.org/10.5383/JUSPN.11.01.003

Jevtic, N., & Alhudaidi, I. (2023). The Importance of Information Security for Organizations. *Serbian Journal of Engineering Management*, *8*(2), 48. https://doi.org/10.5937/SJEM2302048J

Johnson, K. (2025, February 18). *What is defense in depth?* TechTarget. https://www.techtarget.com/searchsecurity/definition/defense-in-depth

Judijanto, L., Hindarto, D., Wahjono, S. I., & Djunarto. (2023). Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. *International Journal Software Engineering and Computer Science (IJSECS)*, *3*(3), 386–396. https://doi.org/10.35870/ijsecs.v3i3.1816

Kamis, A. (2020). Cyber attack and threat protection. IX International Conference on Social and Technological Development Trebinje BIH, 2303-498X. https://doi.org/10.7251/ZRPIM2001365K

Kamis, A., & M Stamenković, N. (2023). *Defense-in-Depth of modern radio systems.* XII International Conference on Social and Technological Development Trebinje BIH. https://doi.org/10.7251/PIMZ2301348K

Kamis, A. , Zakic, A., Popovic, G. , Bogavac, M., Milic D., Ignjatovic B., Lakhmi C. J. (2026). " *Development of a cloud-based WebRTC VoIP application using the Docker platform for an educational environment,* International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 2334-8496

Kamis, A. , Zakic, A., Zakic, M. , Deretic, N., (2025). *"Eyes wide open" – one of the fundamentals of information security,* XIV International Conference on Social and Technological Development Trebinje BIH. https://doi.org/10.63395/STEDConf14022025935K187

Kashyap, A. K., & Chaudhary, M. (2023). Cyber Security Laws and Safety in E-Commerce in India. *2 (89)*, 207. https://doi.org/10.32631/pb.2023.2.19

Kello, L. (2022). Striking back: The End of Peace in Cyberspace - and How to Restore It. Yale University Press.

Khlaponin, Y. I., Kozubtsova, L. M., Kozubtsov, I. M., & Shtonda, R. M. (2022). Functions of the information protection system and cybersecurity of critical information infrastructure. 3 *(15)*. https://doi.org/10.28925/2663-4023.2022.15.1241341

Kosseff, J. (2019). Cybersecurity Law. John Wiley & Sons.

Krulík, O. (2018). *Milestones Related to the Development of Organizational Aspects of Cybersecurity and Protection against Cyber-Threats in the Czech Republic*. *17*(3), 115–130. https://doi.org/10.32565/aarms.2018.3.8

Kuipers, D., & Fabro, M. (2006). Control Systems Cyber Security: Defense in Depth Strategies. https://nsarchive.gwu.edu/sites/default/files/documents/3121326/Document-06.pdf

Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. Information Management & Computer Security, 21(5), 420–443. https://doi.org/10.1108/IMCS-04-2013-0027

N.A. (2009). Next Generation Nuclear Plant Defense-in-Depth Approach. *https://art.inl.gov/ART%20Document%20Library/Published%20Documents/Licensing%20Reports/Defense_In_Depth_Approach.pdf*.

(2009). https://art.inl.gov/ART%20Document%20Library/Published%20Documents/Licensing%20Reports/Defense_In_Depth_Approach.pdf

Neri, M., Niccolini, F., & Pugliese, R. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *Online Journal of Applied Knowledge Management*, *10*(2), 1.

Novianto, F. (2020). Evaluation of e-government information security using the defense in depth model. Cyber Security Dan Forensik Digital, 3(1), 14–19. https://doi.org/10.14421/csecurity.2020.3.1.1962

Nyamwesa, A. (2024). Cloud Computing Technology Adoption: Challenges for SMEs, A Case of Selected SMEs in Tanzania. *International Journal of Advanced Business Studies*, *3*(2). https://doi.org/10.59857/IJABS.3118

Malik, P., Nautiyal, L., & Ram, M. (2022*). Machine learning for Cyber security.* Walter de Gruyter GmbH & Co KG.

Maulding, C. (2026). *Defense in depth: A layered approach to cybersecurity.* SDM Magazine. https://www.sdmmag.com/articles/104936-defense-in-depth-a-layered-approach-to-cybersecurity

Peña-Montes De Oca, A. I., & Mondragón-Gutiérrez, E. (2023). Culture of data protection, service and quality is cybersecurity in SMEs. *ECORFAN Journal -Republic of Cameroon*, *9*(17), 22–28. https://doi.org/10.35429/EJRC.2023.17.9.22.28

Popovic G., Kamis A., Zakic A., Ignjatović B., Milic D., Sarcevic Dj.(2026), *Procjena sajber rizika vođena vještačkom inteligencijom u savremenim poslovnim informacionim sistemima*. 25th International Symposium INFOTEH-JAHORINA

Prasad, R., & Rohokale, V. (2019). Cyber security: the lifeline of information and communication technology. In Springer series in wireless technology. https://doi.org/10.1007/978-3-030-31703-4

Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Rébé, N. (2022). *Cyber laundering: International Policies and Practices*. World Scientific Publishing Europe Limited.

Riebe, T., Biselli, T., Kaufhold, M.-A., & Reuter, C. (2023). Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey. *Proceedings on Privacy Enhancing Technologies*, *2023*(1), 477–493. https://doi.org/10.56553/popets-2023-00281

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131

Safitri, R., & Darjat, D. (2024). Evaluation of the Impact of Risk management and Information Security on Cybersecurity Maturity of the Institute ABC Data Management Application. *West Science Information System and Technology*, *2*(01), 18–27. https://doi.org/10.58812/wsist.v2i01.802

Scholl, M., & Schuktomow, R. (2021). The Current State of "Information Security Awareness" in German SMEs. *International Journal of Emerging Technology and Advanced Engineering*, *11*(12), 151. https://doi.org/10.46338/ijetae1221_16

Sharkov, G. (2020). Assessing the Maturity of National Cybersecurity and Resilience. *Connections: The Quarterly Journal*, *19*(4), 5–24. https://doi.org/10.11610/Connections.19.4.01

Shekh, A.-A.-M. A. (2024). *Information Security Risk Management Framework*. https://doi.org/10.58830/ozgur.pub445

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, *25*(1), 235–246. https://doi.org/10.48009/1_iis_2024_120

Thach, N. N., Hanh, H. T., Gwoździewicz, S., Huy, D. T. N., Nga, L. T. V., Thuy, D. M., & Hong, P. V. (2020). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets - the case in Vietnam.

International Journal for Quality Res earch, *15*(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Wang, Z. (2023). Digital Transformation and Risk Management for SMEs: A Systematic Review on Available Evidence. У *Proceedings of the 2nd International Conference on Financial Technology and Business Analysis* (Том 65, стр. 209). https://doi.org/10.54254/2754-1169/65/20231639

Xu, H., Zhou, Y., Ming, J., & Lyu, M. (2020). Layered obfuscation: a taxonomy of software obfuscation techniques for layered security. *Cybersecurity*, *3*(9), 9. https://doi.org/10.1186/s42400-020-00049-3

Prilozi

Biografija autora

Alen Kamiš rođen je 8. aprila 1978. godine u Sarajevu, gdje je završio osnovno i srednje obrazovanje. Svoje visoko obrazovanje započeo je na Visokoj školi za uslužni biznis u Istočnom Sarajevu – Sokolac, gdje je stekao zvanje diplomirani menadžer poslovne informatike s prosječnom ocjenom 8,60. Dalje akademsko usavršavanje nastavio je na Univerzitetu za poslovni inženjering i menadžment PIM, na Fakultetu informacionih tehnologija, gdje je stekao zvanje diplomirani inženjer računarstva i informatike s prosječnom ocjenom 8,82, a potom završio i master studij s prosječnom ocjenom 9,50, čime je stekao zvanje master računarstva i informatike. S ciljem daljeg naučno-istraživačkog i stručnog razvoja, 2021. godine upisuje doktorske studije na Alfa BK Univerzitetu u Beogradu, na studijskom programu Informaciono-komunikacione tehnologije.

Tokom svoje profesionalne karijere, koja traje duže od dvije decenije, stekao je bogato iskustvo u oblasti informacionih tehnologija, sa posebnim fokusom na sajber sigurnost, sistemsku integraciju, virtualizaciju, mrežne tehnologije i upravljanje složenim IT infrastrukturama. Učestvovao je u projektovanju, implementaciji i održavanju naprednih informacionih sistema u složenim produkcionim okruženjima, primjenjujući savremene standarde, najbolje prakse i međunarodne sigurnosne okvire. Njegov stručni profil karakteriše kontinuirano profesionalno usavršavanje i aktivno praćenje savremenih tehnoloških trendova.

Posjeduje više od 50 međunarodno priznatih stručnih certifikata vodećih svjetskih tehnoloških kompanija, uključujući Microsoft, VMware, Kaspersky i Veeam. Među najznačajnijim certifikatima izdvajaju se Microsoft Certified Azure Solutions Architect Expert, Microsoft 365 Certified Teams Voice Engineer Expert, Microsoft 365 Certified Administrator Expert, Microsoft Certified Trainer, VMware Certified Professional Data Center Virtualization, Kaspersky Certified Trainer, kao i Veeam Certified Engineer. Ovi certifikati potvrđuju visok nivo stručnosti u oblasti cloud tehnologija, virtualizacije, sigurnosti informacionih sistema, zaštite podataka i upravljanja IT infrastrukturom.

Pored profesionalnog angažmana u industriji, aktivno učestvuje i u nastavnom procesu. Od 2019. godine angažovan je na Visokoj školi za uslužni biznis u Istočnom Sarajevu – Sokolac, gdje obavlja dužnost višeg asistenta i profesora iz prakse. U okviru nastavnih aktivnosti učestvuje u izvođenju nastave na predmetima Operativni sistemi i arhitektura, Računarske mreže, Web dizajn, Zaštita i sigurnost informacija i Elektronsko poslovanje, gdje studentima prenosi praktična znanja i iskustva stečena kroz dugogodišnji rad u realnim IT okruženjima.
Njegov profesionalni i akademski rad usmjeren je na unapređenje sigurnosti informacionih sistema, razvoj pouzdanih i skalabilnih IT infrastruktura, kao i primjenu savremenih tehnologija u poslovnom i akademskom okruženju. Kontinuiranim stručnim i naučnim usavršavanjem doprinosi razvoju oblasti informaciono-komunikacionih tehnologija i podizanju nivoa stručnosti u oblasti sajber sigurnosti i digitalne transformacije.

Bibliografija autora

Radovi u časopisima:

Kamis, A. , Zakic, A., Popovic, G. , Bogavac, M., Milic D., Ignjatovic B., Lakhmi C. J. (2026). " *Development of a cloud-based WebRTC VoIP application using the Docker platform for an educational environment,* International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 2334-8496 -**M22**

Kamis, A., Zakic, A., & Kukolj, S. (2023). *Elimination of interference with wireless mesh networks through binary symmetrical channels*. STED Journal - Journal of Social and Technological Development, 2637–2614. https://doi.org/10.7251/STED2302074K - **M23**

Kukolj, S., Deretic, N., & Kamis, A. (2023). *Research on the quality of work life and employee motivation in IT company*. SCIENCE International Journal, Skopje, North Macedonia, 2(3). https://doi.org/10.35120/sciencej0203157k -**M23**

Kukolj, S., Deretic, N., Kamis, A. (2025)., *Upotreba digitalnih tehnologija u promociji kulturnog turizma: značaj i uloga četbotova,* Međunarodna naučna konferencija „Turizam i kulturno nasleđe: tradicija, inovacije i globalni, Sremski Karlovci, Republika Srbija, https://doi.org/10.18485/akademac_nsk.2025.6.ch26 - **M33**

Zbornici međunarodnih naučnih skupova:

Popovic G., Kamis A., Zakic A., Ignjatović B., Milic D., Sarcevic Dj. (2026), *Procjena sajber rizika vođena vještačkom inteligencijom u savremenim poslovnim informacionim sistemima*. 25th International Symposium INFOTEH-JAHORINA – **M33**

Denic, N., Milosevic, M., Kamis,A., Mihajlovic, S., Milic, S. (2025). *New possibilities and paradigms of applying artificial intelligence in electronic business*. 7th International conference on applied engineering and natural sciences icaens 2025, Turkey - **M33**

Kamis, A. , Zakic, A., Zakic, M. , Deretic, N., (2025). *"Eyes wide open" – one of the fundamentals of information security,* XIV International Conference on Social and Technological Development Trebinje BIH, 2303-498X. -**M33**

Zakic, A., Zakic M., Trajkovic, S., Kamis, A. *Github copilot: budućnost veb razvoja,* IV Scientific Meeting "Balkan on Jahorina 2025" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667. –**M33**

Kamis, A., Zakic, A., Kukolj, S., Deretic, N., (2024)., W*avelet transformation with examples,* XIII International Conference on Social and Technological Development Trebinje BIH, 2303-498X. -**M33**

Kamis, A., & M Stamenković, N. (2023). *Defense-in-Depth of modern radio systems.* XII International Conference on Social and Technological Development Trebinje BIH, 2303-498X. -**M33**

Kamis, A., Kukolj, S., Penjisevic, A., & Sancanin, B. (2023). *Defense in Depth protection strategy against social engineering and phishing attacks*. II Scientific Meeting "Balkan on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667. –**M33**

Kamis, A. (2022). *Establishing secure communication using SSL VPN*. XI International Conference on Social and Technological Development Trebinje BIH, 2303-498X. –**M33**

Kamis, A. (2022*). Creating cloud based WEBRTC voice over IP applications for wired and wireless users*. XI International Conference on Social and Technological Development Trebinje BIH, 2303-498X. -**M33**

Zakic, M., Kamis, A., & Zakic A. (2022). *Status and perspectives of the development of electronic government in the countries of the Western Balkans*. I Scientific Meeting "Balkan

on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667. – **M33**

Trajkovic, S., Jaksic, K., Kamis, A., & Zakic, M. (2022). *Integration of electronic services during the Covid 19 pandemic*. I Scientific Meeting "Balkan on Jahorina 2023" Development Perspectives of the Western Balkans in the XXI Century East Sarajevo - Sokolac, 2831–0667. - **M33**

Kamis, A. (2020). *Methodological basis of designing, implementation and administration IoT*. IX International Conference on Social and Technological Development Trebinje BIH, 2303-498X. https://doi.org/10.7251/ZRPIM2001359K - **M33**

Kamis, A. (2020). Cyber attack and threat protection. IX International Conference on Social and Technological Development Trebinje BIH, 2303-498X. https://doi.org/10.7251/ZRPIM2001365K -**M33**