Sigurnosne prijetnje i rizici računarstva u oblaku

Holovka, Kristina

Sveučilište u Zadru

Stručni prijediplomski studij
Informacijske tehnologije

Kristina Holovka

Sigurnosne prijetnje i rizici računarstva u oblaku

Završni rad

Zadar, 2024.

Sveučilište u Zadru

Stručni prijediplomski studij
Informacijske tehnologije

Sigurnosne prijetnje i rizici računarstva u oblaku

Završni rad

Student/ica:
Kristina Holovka

Mentor/ica:
prof.dr.sc. Dino Županović

Zadar, 2024.

Izjava o akademskoj čestitosti

Ja, **Kristina Holovka,** ovime izjavljujem da je moj **završni** rad pod naslovom **Sigurnosne prijetnje i rizici računarstva u oblaku** rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 23. rujna 2024.

SADRŽAJ

SAŽETAK

Računarstvo u oblaku u suvremenom digitalnom okruženju postalo je nezamjenjiv alat koji omogućuje fleksibilnost i skalabilnost u korištenju računalnih resursa. Međutim, uz sve prednosti, pojavljuju se i brojni sigurnosni izazovi poput neovlaštenog pristupa, krađe podataka i napada na infrastrukturu. Korištenje modela poput IaaS, PaaS i SaaS, kao i različitih oblika implementacije, zahtijeva od korisnika i pružatelja usluga aktivnu ulogu u održavanju sigurnosti. Primjena mehanizama zaštite poput enkripcije, autentifikacije te načela najmanjih privilegija, uz stalnu edukaciju i svijest o potencijalnim prijetnjama, ključna je za sigurno korištenje usluga u oblaku. Zaključno, učinkovita zaštita podataka u oblaku zahtijeva cjelovite i proaktivne sigurnosne strategije koje uključuju kontinuiranu procjenu i praćenje rizika. Kroz stalno praćenje prijetnji, prilagođavanje sigurnosnih mjera te usklađivanje sa sigurnosnim standardima, korisnici i organizacije mogu postići visoku razinu zaštite podataka. Na taj način, prednosti računalstva u oblaku mogu se iskoristiti u potpunosti, osiguravajući pouzdano okruženje za pohranu i obradu podataka.

Ključne riječi: računarstvo u oblaku, sigurnost, prijetnje, zaštita podataka, sigurnosni mehanizmi

POPIS KORIŠTENIH KRATICA

IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
AWS	Amazon Web Services
IBM	International Business Machines
GUI	Graphical User Interface
GCP	Google Cloud Platform
VM	Virtual Machine
IAM	Identity and Access Management
IoT	Internet of Things
ERP	Enterprise Resource Planning
CMS	Content Management System
HRM	Human Resource Management
CRM	Customer Relationship Management
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
CIA	Confidentiality, Integrity, and Availability
DDoS	Distributed Denial of Service
SSRF	Server-Side Request Forgery

TLS	Transport Layer Security
RaaS	Ransomware as a Service
APT	Advanced Persistent Threat
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SLA	Service Level Agreement
ISO	International Organization for Standardization
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
CCM	Cloud Controls Matrix
STAR	Security, Trust & Assurance Registry
CSA	Cloud Security Alliance
ISMS	Information Security Management System
CCSP	Certified Cloud Security Professional
FTE	Full-Time Employee
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RBAC	Role-Based Access Control
FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology

IDE	Integrated Development Environment
SSL	Secure Sockets Layer
POLP	Principle of Least Privilege
SQL	Structured Query Language
OWASP	Open Web Application Security Project
IT	Information Technology
CSP	Cloud Service Provider
S3	Amazon Simple Storage Service
RFI	Remote File Inclusion
DevOps	Development and Operations
XSS	Cross-Site Scripting
USB	Universal Serial Bus
API	Application Programming Interface
ISC²	International Information System Security Certification Consortium

1. UVOD

U današnjem digitalnom svijetu, računarstvo u oblaku postalo je nezamjenjiv alat za organizacije i pojedince koji traže fleksibilnost, skalabilnost i učinkovitost u upravljanju podacima i poslovnim procesima. Koristeći različite oblike računalnih resursa, poput virtualnih poslužitelja, pohrane podataka i softverskih aplikacija, oblak omogućava korisnicima pristup tim resursima putem interneta bez potrebe za održavanjem vlastite infrastrukture. Zbog sve većeg broja korisnika i količine podataka koji se pohranjuju i obrađuju u oblaku, raste i broj sigurnosnih prijetnji koje mogu ugroziti povjerljivost, integritet i dostupnost podataka.

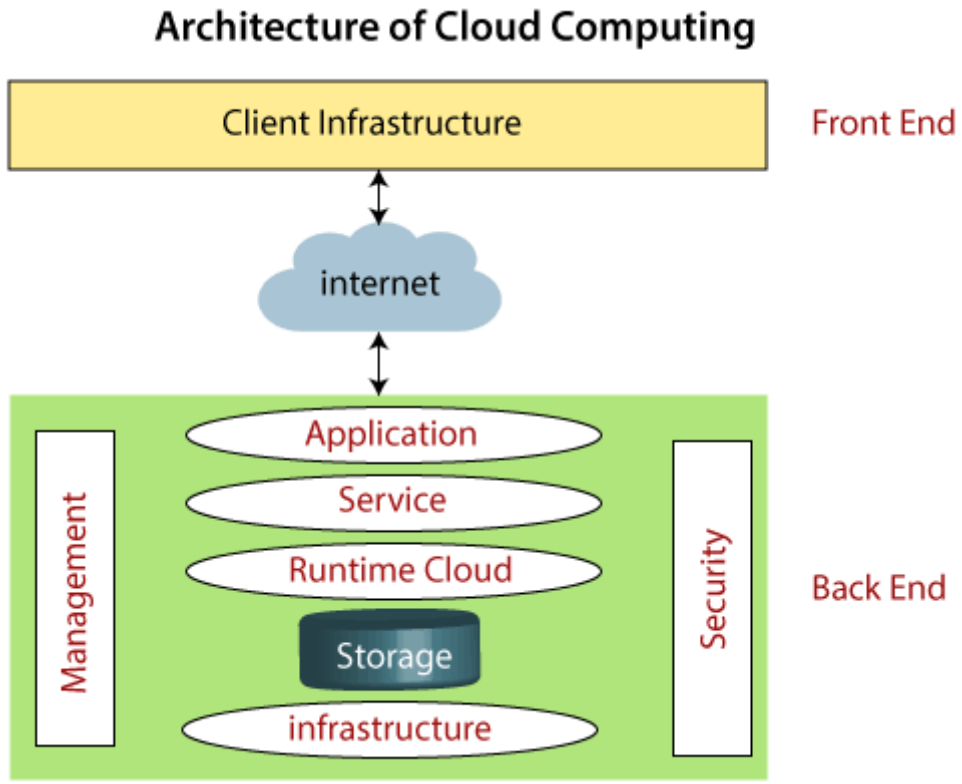
Napadi poput neovlaštenog pristupa, krađe podataka i napada na infrastrukturu postali su uobičajeni rizici s kojima se korisnici oblaka suočavaju. Sve složeniji i sofisticiraniji oblici napada, kao što su DDoS napadi, zlonamjerni softver, phishing kampanje i napadi na virtualne strojeve, predstavljaju značajan izazov u osiguravanju sigurnosti podataka u oblaku. U isto vrijeme, brzi napredak tehnologije dovodi do potrebe za implementacijom naprednih sigurnosnih mehanizama kako bi se zaštitili podaci i resursi u oblaku.

Cilj ovog rada je pružiti sveobuhvatan pregled računarstva u oblaku, s posebnim naglaskom na sigurnosne prijetnje, rizike i mehanizme zaštite. Posebna pažnja posvećena je ulozi korisnika i pružatelja usluga u održavanju sigurnosti te važnosti usklađenosti sa sigurnosnim standardima. Kroz istraživanje sigurnosnih izazova, dostupnih zaštitnih mjera i najboljih praksi, rad pokazuje kako korisnici i organizacije mogu učinkovito primijeniti sigurnosne mjere i sigurno koristiti računalstvo u oblaku.

2. RAČUNARSTVO U OBLAKU

Računarstvo u oblaku omogućuje pristup računalnim resursima kao što su fizički ili virtualni poslužitelji, pohrana podataka, umrežavanje, alati za razvoj aplikacija, softver, analitički alati s umjetnom inteligencijom i druge funkcionalnosti putem interneta, uz model plaćanja prema stvarnom korištenju [1].

Osnovna ideja iza računarstva u oblaku je da korisnici mogu pristupiti ovim resursima s bilo kojeg mjesta i u bilo koje vrijeme, uz fleksibilnost u prilagodbi kapaciteta prema potrebama trenutnog poslovanja. To donosi brojne prednosti, uključujući smanjenje troškova infrastrukture jer organizacije plaćaju samo za resurse koje stvarno koriste, što može smanjiti kapitalna ulaganja i operativne troškove.



Slika 1 Arhitektura računarstva u oblaku, Izvor: https://www.javatpoint.com/cloud-computing-architecture

Arhitektura računalstva u oblaku obuhvaća različite komponente koje zajedno omogućuju učinkovitu isporuku i upravljanje računalnim resursima putem interneta. Ova arhitektura se sastoji od dva glavna dijela: prednjeg dijela (*front-end*) i stražnjeg dijela (*back-end*).

Prednji dio obuhvaća korisničko sučelje i aplikacije koje korisnici koriste za interakciju s oblakom. To uključuje web preglednike, klijentske uređaje i aplikacije koje omogućuju pristup raznim uslugama oblaka. Klijenti koriste ove aplikacije za pristup informacijama, pohranu podataka, upravljanje aplikacijama i druge funkcionalnosti koje nudi oblak. Stražnji dio arhitekture oblaka uključuje različite komponente i usluge koje pružatelji oblaka koriste za upravljanje resursima. Ovaj dio obuhvaća poslužitelje, pohranu podataka, baze podataka, virtualizacijske tehnologije i mrežne infrastrukture [2].

Mrežna infrastruktura omogućuje siguran prijenos podataka između klijentskih uređaja i oblaka. Modeli usluga u računarstvu u oblaku uključuju IaaS (infrastruktura kao usluga), PaaS (platforma kao usluga) i SaaS (softver kao usluga). IaaS omogućuje korisnicima virtualizirane računalne resurse, dok PaaS pruža platforme za razvoj i implementaciju aplikacija bez potrebe za održavanjem infrastrukture. SaaS nudi softverske aplikacije koje su dostupne putem interneta, s dobavljačima koji upravljaju infrastrukturom i aplikacijama. Važno je napomenuti i različite modele implementacije oblaka. Javni oblak pruža usluge više korisnicima putem interneta, dok privatni oblak nudi infrastrukturu koja je posebno posvećena jednoj organizaciji, pružajući veću sigurnost i kontrolu nad podacima. Hibridni oblak kombinira ove pristupe, omogućujući organizacijama da iskoriste prednosti oba modela prema specifičnim potrebama i sigurnosnim zahtjevima [1].

Uz brz razvoj tehnologije i rastuću potražnju za skalabilnošću i sigurnošću, računarstvo u oblaku nastavlja revolucionirati način na koji organizacije koriste IT resurse. Pružajući ekonomske, sigurnosne i operativne prednosti, oblak postaje sveprisutno rješenje u modernom poslovanju, potičući inovacije i optimizaciju procesa širom svijeta.

2.1. POVIJEST I RAZVOJ RAČUNARSTVA U OBLAKU

Koncept računarstva u oblaku datira iz 1960-ih kada je John McCarthy predložio ideju da bi se računalstvo moglo organizirati kao javna usluga. Ova vizija sugerirala je da bi korisnici mogli pristupati računalnim resursima na način sličan korištenju javnih komunalnih usluga. Douglas Parkhill je 1966. u svojoj knjizi "*The Challenge of the Computer Utility*" prvi istraživao karakteristike oblaka, predviđajući njegov potencijal u pružanju računalnih usluga kao javnog resursa [3].

Termin "oblak" u kontekstu računarstva pojavio se iz mrežnih dijagrama u kojima je internet bio predstavljen kao oblačić, simbolizirajući slojeve infrastrukture koje korisnici ne trebaju razumjeti [4]. Ovo apstraktno predstavljanje omogućilo je jasniju vizualizaciju ideje skrivenih infrastrukturalnih slojeva koji omogućuju pristup računalnim resursima putem interneta.

Razvoj računarstva u oblaku bio je potaknut brzim napretkom tehnologije, povećanom potražnjom za računalnim resursima te potrebom za fleksibilnijim i ekonomičnijim modelima korištenja IT resursa. Osnovna ideja iza računarstva u oblaku je pružanje resursa na zahtjev, omogućujući korisnicima pristup s bilo kojeg mjesta i u bilo koje vrijeme. Ova fleksibilnost omogućava organizacijama prilagodbu kapaciteta prema trenutnim poslovnim potrebama, čime se optimiziraju resursi i smanjuju nepotrebni troškovi.

Prvi praktični koraci ka modernom računarstvu u oblaku dogodili su se 2006. godine, kada je Amazon pokrenuo Amazon Web Services (AWS). Istovremeno, Google i IBM započeli su vlastite projekte istraživanja u oblaku, čime su postavili temelje za današnji razvoj industrije. Glavni pružatelji IT usluga poput Amazona, Googlea i Microsofta igrali su ključnu ulogu u popularizaciji računarstva u oblaku putem svojih platformi kao što su Amazon Web Services (AWS), Google Cloud Platform (GCP) i Microsoft Azure. Ove platforme nude širok izbor usluga u oblaku uključujući pohranu podataka, računalne resurse, mrežne usluge i aplikacije kao uslugu (SaaS) [3].

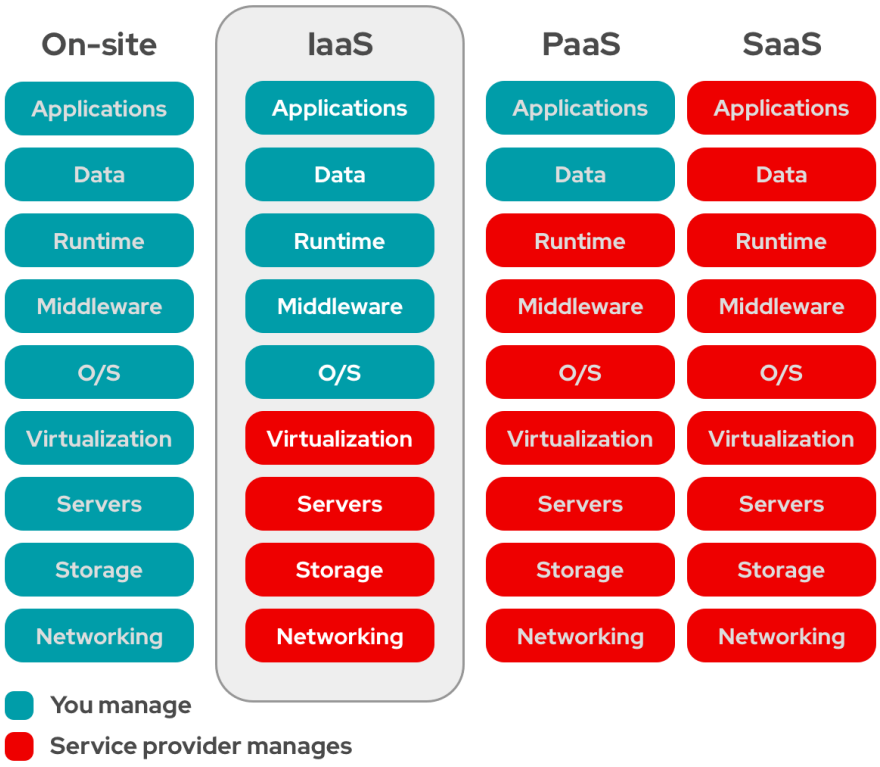
Razvoj računarstva u oblaku može se pratiti kroz nekoliko ključnih faza. U ranim fazama, od 1960-ih do 1990-ih, postavljeni su temelji tehnologije i razvijeni ključni koncepti. Prijelomni trenutak dogodio se 2006. godine s lansiranjem AWS-a, a ubrzo nakon toga Google i IBM započeli su vlastite projekte istraživanja u oblaku. Tijekom 2010-ih, standardizacija i popularizacija računarstva u oblaku postale su ključne teme, s prvim Međunarodnim kongresom o računarstvu u oblaku održanim 2010. godine [5].

Računarstvo u oblaku nije samo transformiralo način na koji organizacije upravljaju IT resursima, već je omogućilo inovacije u raznim industrijama. Od zdravstvenog sektora do obrazovanja, prednosti fleksibilnosti, skalabilnosti i ekonomičnosti dovele su do povećane produktivnosti i poboljšanih usluga. U proteklim godinama, računarstvo u oblaku doživjelo je značajan rast i širenje upotrebe u različitim sektorima, uključujući poslovne, akademske i osobne svrhe. Napredak u sigurnosnim tehnologijama i prilagodljivost platformi u oblaku

kontinuirano unaprjeđuje performanse, sigurnost i dostupnost usluga. Budućnost računarstva u oblaku obećava još veće integracije s tehnologijama poput umjetne inteligencije i Internet of Things (IoT), što će dodatno proširiti mogućnosti i primjene ove revolucionarne tehnologije.

2.2. MODELI USLUGA RAČUNARSTVA U OBLAKU

Kroz računarstvo u oblaku, organizacije mogu brzo prilagoditi svoje IT resurse trenutnim potrebama, skalirati ih prema zahtjevima tržišta i smanjiti operativne troškove. Osim toga, računarstvo u oblaku omogućava bržu implementaciju inovacija, povećava agilnost i omogućava globalnu dostupnost usluga. No, kako bi se u potpunosti razumjele prednosti i izazovi računarstva u oblaku, važno je detaljno istražiti različite modele usluga koje nudi: *infrastructure as a service* (IaaS), *platform as a service* (PaaS) i *software as a service* (SaaS).



Slika 2 Usporedba modela On-site, IaaS, PaaS i SaaS u upravljanju IT infrastrukturom, Izvor: https://www.redhat.com/en/topics/cloud-computing/what-is-iaas

IaaS omogućuje korisnicima pristup temeljnim računalnim, mrežnim i skladišnim resursima. Ova vrsta usluge pruža fleksibilnost korisnicima da izgrade prilagođene usluge i aplikacije koristeći resurse koje pružatelji usluga u oblaku stavljaju na raspolaganje. Pružatelj usluga u oblaku kontrolira fizičke resurse, dok korisnici kontroliraju sve ostalo, poput operativnih

sustava i razvojnih alata [6]. Na primjer, Amazon Web Services (AWS) je jedan od najpoznatijih pružatelja IaaS usluga, omogućujući korisnicima pristup virtualnim serverima, pohrani i mrežnim resursima na zahtjev.

PaaS pruža naprednije okruženje u kojem se aplikacije mogu razvijati ili implementirati. Korisnici koriste pruženu platformu, kao što su naprimjer programski jezik Java i Oracle baze podataka, bez brige o temeljitim detaljima poput softverskih i hardverskih zavisnosti i konfiguracija. PaaS usluge omogućuju brži razvoj aplikacija jer se korisnici mogu fokusirati na programiranje bez pretjerane brige o infrastrukturi. Primjeri PaaS usluga uključuju Google App Engine i Microsoft Azure, koji nude alate i okruženja za razvoj, testiranje i implementaciju aplikacija [6].

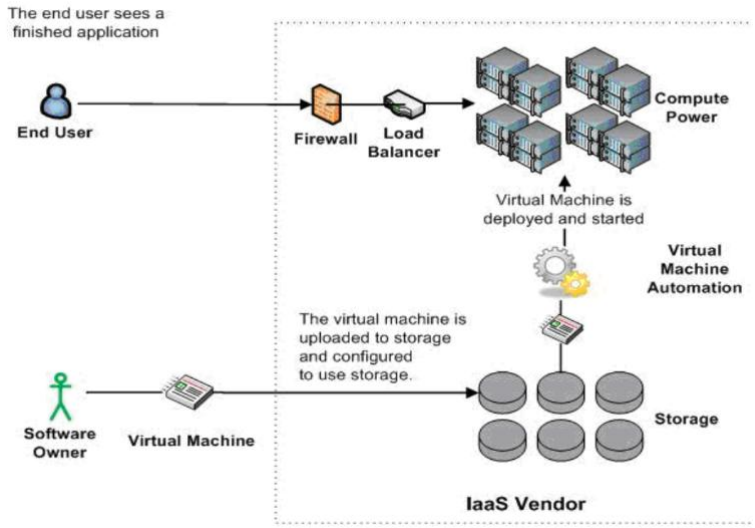
SaaS pruža najviši stupanj usluge, gdje korisnici koriste aplikacije koje su već dostupne i održavane od strane pružatelja usluga u oblaku. Većina besplatnih usluga u oblaku, kao što su web-bazirani email i aplikacije za obradu teksta, mogu se svrstati u ovu kategoriju usluga. Ovaj model praktično eliminira potrebu za održavanjem softvera za krajnje korisnike i pojednostavljuje postupke testiranja i implementacije za razvojne programere. Primjeri SaaS usluga uključuju Google Apps, Microsoft Office 365 i Salesforce, gdje korisnici mogu koristiti aplikacije direktno putem web preglednika bez potrebe za instalacijom softvera [6].

Računarstvo u oblaku je revolucija koja predstavlja paradigmu prijelaza s tradicionalnih načina upravljanja IT resursima na fleksibilnije, skalabilnije i ekonomski isplativije modele. Kroz IaaS, PaaS i SaaS, organizacije sada mogu birati razinu kontrole i odgovornosti koje najbolje odgovaraju njihovim potrebama, omogućujući im da se fokusiraju na svoje ključne kompetencije dok koriste napredne tehnologije bez velikih početnih ulaganja. Ovaj model ne samo da omogućuje bržu inovaciju nego i olakšava pristup naprednim tehnologijama malim i srednjim poduzećima koja ranije nisu imala tu priliku.

2.2.1. IAAS

Infrastructure as a Service (IaaS) predstavlja oblik računarstva u oblaku gdje se hardver (serveri, skladištenje i mreža) i pridruženi softver (operativni sustavi, virtualizacijska tehnologija, datotečni sustavi) isporučuju kao usluga. Ova evolucija tradicionalnog hostinga ne zahtijeva dugoročne ugovore i omogućuje korisnicima da si po potrebi osiguravaju resurse. Za razliku od

PaaS usluga, pružatelj IaaS usluga upravlja samo osnovnom infrastrukturom, dok korisnici sami postavljaju i održavaju softverske servise, kao što bi to činili u vlastitim podatkovnim centrima [7].



Slika 3 Infrastructure as a service, Izvor: Sushil Bhardwaj, Leena Jain, Sandeep Jain; Cloud computing: A study of infrastructure as a service (IAAS),« International Journal of Engineering and Information Technology , svez. 2, br. 1, pp. 60-63, 2010.

IaaS se često oslanja na tehnologije virtualizacije, automatizacije i orkestracije kako bi korisnicima pružio fleksibilno i skalabilno okruženje. Virtualne mašine omogućuju kreiranje izoliranih radnih okruženja unutar fizičkih servera, dok automatizacija pojednostavljuje proces implementacije i skaliranja resursa. Orkestracija omogućava koordinaciju automatiziranih zadataka, čime se osigurava učinkovito upravljanje velikim brojem resursa [8].

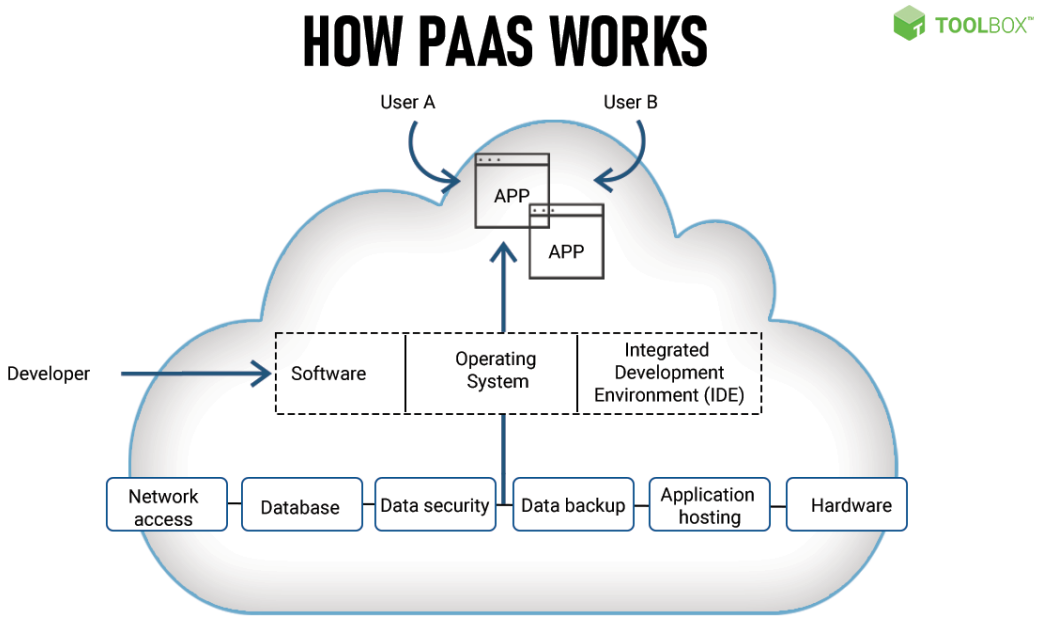
Neki pružatelji IaaS usluga također podržavaju kontejnerizaciju, gdje su aplikacije i sve njihove zavisnosti pakirane u kontejnere koji se mogu jednostavno premještati između različitih okruženja. Kontejneri ne uključuju vlastiti operativni sustav, što ih čini lakšima i bržima za implementaciju u usporedbi s virtualnim mašinama. Jedan od glavnih izazova s IaaS modelom su sigurnosni rizici povezani s dijeljenjem infrastrukture među više korisnika (*multi-tenancy*). Korisnici moraju pažljivo birati pouzdane i provjerene pružatelje usluga kako bi osigurali da su njihovi podaci sigurni i da su dostupni u svakom trenutku [8].

Računarstvo u oblaku, s naglaskom na IaaS, predstavlja temeljnu promjenu u načinu na koji organizacije upravljaju svojim IT resursima. Umjesto da ulažu velike kapitalne izdatke u vlastitu infrastrukturu, tvrtke sada mogu preusmjeriti svoje resurse prema inovacijama i rastu.

IaaS model pruža nevjerojatnu fleksibilnost i skalabilnost, omogućujući organizacijama da se brzo prilagode promjenama na tržištu i tako povećaju svoju agilnost i konkurentnost. Automatizacija i orkestracija unutar IaaS okruženja omogućuju učinkovito upravljanje resursima, dok kontejnerizacija dodatno pojednostavljuje implementaciju aplikacija. Unatoč sigurnosnim izazovima, pažljiv odabir pouzdanih pružatelja usluga može osigurati zaštitu podataka i kontinuitet poslovanja. Ovaj pristup demokratizira pristup naprednim tehnologijama, omogućujući manjim poduzećima da iskoriste resurse koji su prethodno bili dostupni samo velikim korporacijama, čime se stvara ravnopravnije poslovno okruženje i potiče inovacija na svim razinama.

2.2.2. PAAS

Platform as a Service (PaaS) predstavlja model računarstva u oblaku koji korisnicima omogućuje razvoj, testiranje i implementaciju aplikacija bez potrebe za upravljanjem osnovnom infrastrukturom. PaaS pruža sve potrebne alate i okruženja za razvoj softvera, uključujući operativne sustave, razvojne alate, baze podataka i web poslužitelje. Korisnici mogu koristiti te resurse kako bi brzo i učinkovito razvijali aplikacije, dok pružatelj usluga upravlja infrastrukturom, sigurnošću i operativnim sustavima. PaaS rješenja obično se sastoje od tri glavna dijela: infrastrukture oblaka koja uključuje virtualne strojeve, operativne sustave, pohranu, mrežu i vatrozidove; softvera za izgradnju, implementaciju i upravljanje aplikacijama; te grafičkog korisničkog sučelja (GUI) gdje razvojni ili DevOps timovi mogu raditi tijekom cijelog životnog ciklusa aplikacije. PaaS pružatelji upravljaju većinom *cloud computing* usluga, kao što su serveri, *runtime* okruženja i virtualizacija, dok korisnici zadržavaju upravljanje aplikacijama i podacima [9].



Slika 4. Kako PAAS funkcionira?, Izvor: https://www.spiceworks.com/tech/cloud/articles/what-is-platform-as-a-service/

Kao što je prikazano na slici 4, PaaS funkcionira tako da osnovne komponente poput mrežnog pristupa, baza podataka, sigurnosti podataka, backup sustava, hostinga aplikacija i hardvera čine temeljnu infrastrukturu koja podržava PaaS. Na sljedećoj razini nalazi se sloj softvera koji uključuje operativne sustave i integrirano razvojno okruženje (IDE). Ovaj sloj pruža sve potrebne alate i okruženje za izgradnju aplikacija. Razvojni inženjeri koriste ove alate za pisanje, testiranje i implementaciju svojih aplikacija. Naposljetku se nalaze krajnji korisnici aplikacija koji pristupaju aplikacijama razvijenim i implementiranim pomoću PaaS platforme. PaaS pružatelj upravlja svim infrastrukturnim komponentama i osigurava da aplikacije budu dostupne i sigurne, omogućujući programerima da se fokusiraju isključivo na razvoj softvera bez brige o održavanju i upravljanju infrastrukturom.

PaaS se koristi za različite scenarije, uključujući razvoj i implementaciju aplikacija, analitiku podataka, te automatizaciju poslovnih procesa. Na primjer, alati za analitiku i poslovnu inteligenciju dostupni kroz PaaS omogućuju organizacijama analizu podataka, otkrivanje uvida i predviđanje ishoda radi donošenja boljih poslovnih odluka. PaaS također omogućuje organizacijama dodavanje novih razvojnih mogućnosti bez potrebe za dodatnim osobljem, jer pružatelji usluga često nude unaprijed kodirane komponente i alate za razvoj [10].

Jedna od glavnih prednosti PaaS-a je smanjenje vremena potrebnog za izlazak na tržište. Budući da nema potrebe za kupovinom i instalacijom hardvera i softvera potrebnih za izgradnju i

održavanje platforme za razvoj aplikacija, razvojni timovi mogu odmah početi s radom koristeći PaaS resurse. To omogućava bržu izradu i implementaciju aplikacija.

2.2.3. SAAS

Software as a Service (SaaS) je oblik računarstva u oblaku koji omogućava korisnicima pristup aplikacijama putem internetskog preglednika, eliminirajući potrebu za instalacijom i održavanjem softvera na vlastitim uređajima. SaaS aplikacije se hostiraju na udaljenim serverima pružatelja usluga, koji također upravlja infrastrukturom, sigurnošću, održavanjem i ažuriranjima. Ovaj model smanjuje početne troškove za korisnike i olakšava pristup softveru bez potrebe za značajnim ulaganjima u hardver i IT infrastrukturu. SaaS aplikacije obično koriste *multi-tenant* arhitekturu, gdje više korisnika dijeli istu instancu aplikacije dok su njihovi podaci odvojeni. Ovaj model omogućuje pružateljima usluga da lako ažuriraju softver i implementiraju nove značajke bez prekida rada za korisnike. Korisnici pristupaju aplikacijama putem web preglednika, što omogućuje mobilnost i dostupnost aplikacija s bilo koje lokacije [11].

Slika 5 Vrste SaaS-a, Izvor: https://www.spiceworks.com/tech/cloud/articles/what-is-software-as-a-service/

Kao što je prikazano na slici 5, postoji više vrsta SaaS aplikacija koje se koriste za različite poslovne svrhe. Svaka vrsta SaaS-a odgovara specifičnim potrebama organizacija, omogućujući im da optimiziraju svoje poslovne procese i poboljšaju efikasnost. Prva vrsta

SaaS-a su aplikacije za planiranje resursa poduzeća (ERP). Zatim, tu su aplikacije za planiranje i fakturiranje, aplikacije za vođenje projekata, računovodstvo i knjigovodstvo, upravljanje sadržajem (CMS), maloprodaju i e-trgovinu. U području komunikacija, SaaS aplikacije olakšavaju poslovnu komunikaciju. Aplikacije za upravljanje ljudskim resursima (HRM) omogućuju bolju organizaciju i upravljanje zaposlenicima. Naposljetku, aplikacije za upravljanje odnosima s klijentima (CRM) pomažu tvrtkama u praćenju i optimizaciji interakcija s kupcima. Ova raznolikost SaaS aplikacija pokazuje koliko je široka njihova primjena i koliko mogu pomoći organizacijama da unaprijede svoje poslovanje na različitim razinama.

Primjeri poznatijih SaaS aplikacija uključuju alate za suradnju poput Google Docs i Microsoft Office 365, sustave za upravljanje odnosima s klijentima (CRM) poput Salesforce-a, te razne poslovne aplikacije za ljudske resurse, e-trgovinu i razvojne okoline. SaaS model je često temeljen na pretplatničkom modelu, gdje korisnici plaćaju mjesečnu ili godišnju naknadu za pristup softveru, što olakšava upravljanje troškovima i prilagođavanje potrebama korisnika [11].

SaaS predstavlja evoluciju u načinu na koji organizacije pristupaju i koriste softverske aplikacije. Ovaj model transformira tradicionalne metode kupnje, instalacije i održavanja softvera, omogućujući korisnicima pristup najnovijim tehnologijama uz minimalne troškove. SaaS demokratizira pristup naprednim softverskim alatima, omogućujući manjim organizacijama da koriste iste resurse kao i veće korporacije, čime se potiče inovacija i konkurentnost u globalnom poslovnom okruženju.

2.3. MODELI IMPLEMENTACIJE RAČUNARSTVA U OBLAKU

Računarstvo u oblaku može se implementirati na nekoliko različitih načina, pri čemu svaki nudi jedinstvene prednosti i odgovara specifičnim potrebama organizacija. Glavni modeli implementacije računarstva u oblaku su javni oblak, privatni oblak i hibridni oblak.

Javni oblak je model gdje se usluge poput infrastrukture, platformi i aplikacija pružaju putem interneta od strane trećih pružatelja usluga. Ove usluge su dostupne svima koji ih žele koristiti ili kupiti. Pružatelji javnih oblaka upravljaju i održavaju infrastrukturu i usluge, omogućujući korisnicima skaliranje resursa prema potrebi. Ovaj model je posebno isplativ jer korisnici plaćaju samo za ono što koriste, bez potrebe za značajnim kapitalnim ulaganjima u hardver i

softver. Međutim, izazovi u pogledu sigurnosti podataka i privatnosti prisutni su jer se resursi dijele među više korisnika [12].

Privatni oblak je oblačna infrastruktura namijenjena jednoj organizaciji. Može biti smještena na lokaciji same organizacije ili kod trećeg pružatelja usluga. Ovaj model nudi višu razinu kontrole i sigurnosti, što ga čini pogodnim za organizacije s visokim zahtjevima za regulativom i osjetljivim podacima. Privatni oblak omogućava fleksibilnost u prilagodbi infrastrukture i usluga specifičnim potrebama organizacije. Također omogućava bolju kontrolu nad podacima, sigurnosnim politikama i usklađenošću s regulatornim standardima. Međutim, troškovi postavljanja i održavanja privatnog oblaka mogu biti značajni [12].

Hibridni oblak kombinira javne i privatne oblake, omogućujući dijeljenje podataka i aplikacija između njih. Ovaj model omogućava organizacijama da iskoriste skalabilnost i isplativost javnih oblaka, dok zadržavaju sigurnost i kontrolu privatnih oblaka. Hibridna rješenja dizajnirana su kako bi pružila veću fleksibilnost omogućujući premještanje radnih opterećenja između privatnih i javnih oblaka prema potrebama i troškovima. Na primjer, organizacije mogu zadržati osjetljive operacije u privatnom oblaku, dok koriste javni oblak za manje osjetljive operacije, čime se postiže ravnoteža između učinkovitosti i sigurnosti [12].

Svaki model implementacije računarstva u oblaku nudi različite prednosti i izazove. Izbor modela ovisi o raznim faktorima, uključujući troškove, sigurnost, zahtjeve usklađenosti i specifične potrebe organizacije. Javni oblaci pružaju isplativost i skalabilnost, privatni oblaci nude poboljšanu sigurnost i kontrolu, dok hibridni oblaci kombiniraju najbolje od oba svijeta, pružajući fleksibilnost i optimiziranu upotrebu resursa. Razumijevanjem i odabirom odgovarajućeg modela implementacije, organizacije mogu učinkovito iskoristiti računarstvo u oblaku za podršku i poboljšanje svojih poslovnih ciljeva.

3. SIGURNOSNE PRIJETNJE U RAČUNARSTVU U OBLAKU

Računarstvo u oblaku nudi brojne prednosti, ali također donosi brojne specifične sigurnosne prijetnje sa kojima organizacije moraju pažljivo upravljati. Ove prijetnje mogu imati ozbiljne posljedice po povjerljivost, integritet i dostupnost podataka.

Među ključnim prijetnjama su napadi na infrastrukturu oblaka, uključujući virtualne mašine i mrežne komponente. Napadači često ciljaju na slabosti u virtualizacijskom sloju kako bi kompromitirali izolaciju između različitih korisničkih okruženja, što može dovesti do pristupa povjerljivim podacima i aplikacijama. Mrežna sigurnost također predstavlja izazov, s napadima koji mogu presresti ili preusmjeriti osjetljive podatke, naglašavajući potrebu za snažnim šifriranjem i autentifikacijskim mehanizmima [13].

Autorizacija i upravljanje identitetima i pristupom (IAM) su ključni aspekti zaštite podataka u oblaku. Prijetnja može nastati iz neadekvatno postavljenih dozvola ili neovlaštenog pristupa, što može dovesti do ozbiljnih sigurnosnih incidenata. Višefaktorska autentifikacija (MFA) i stroga pravila pristupa su osnovni alati za smanjenje rizika povezanih s neovlaštenim pristupom. Također, prijenos i pohrana podataka predstavljaju značajan rizik, posebno ako se ne koriste odgovarajuće enkripcijske metode. Nedostatak ili loša implementacija enkripcije može rezultirati krađom ili kompromitacijom podataka. Pravilno upravljanje enkripcijskim ključevima je od presudne važnosti za osiguranje sigurnosti podataka [13].

Dodatne prijetnje uključuju rizike povezane s višekorisničkim okruženjima *(multi-tenancy*), gdje različiti korisnici dijele iste fizičke resurse. Ovo može dovesti do neovlaštenog pristupa podacima zbog slabosti u izolaciji između korisničkih okruženja [14].

Sigurnosni problemi u oblaku također uključuju prijetnje poput *phishinga* i socijalnog inženjeringa, koje su u porastu. Prema izvještaju „*HP Wolf Security Threat Insights Report*“, broj napada putem *phishinga* povećao se za 27% u posljednjih godinu dana, što naglašava potrebu za jačanjem svijesti i obrazovanja korisnika [15].

Sigurnosne prijetnje u računarstvu u oblaku ističu složenost balansiranja između inovacije i sigurnosti. Dok tehnologija može značajno unaprijediti efikasnost i dostupnost, ona također uvodi nove slojeve rizika i nesigurnosti. Ova dinamika zahtijeva stalno prilagođavanje i učenje, gdje je ključna ljudska komponenta u osiguravanju pravovremenih i odgovarajućih reakcija na

nove prijetnje. U konačnici, sigurnost nije samo tehničko pitanje, već i etičko, zahtijevajući duboko promišljanje o povjerenju, odgovornosti i zaštiti privatnosti u današnjem digitalnom svijetu.

3.1. NEOVLAŠTENI PRISTUP I KRAĐA PODATAKA

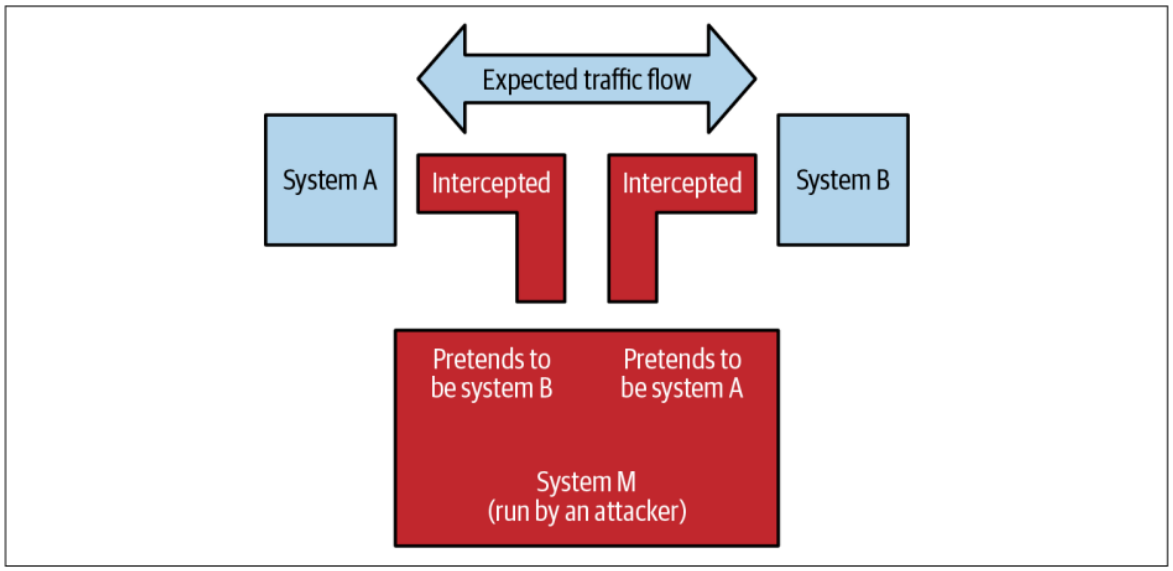
Neovlašteni pristup i krađa podataka predstavljaju jedne od najozbiljnijih prijetnji s kojima se suočava računarstvo u oblaku. Ove prijetnje mogu imati dalekosežne posljedice po povjerljivost, integritet i dostupnost podataka. Napadači često koriste različite metode kako bi dobili neovlašteni pristup sustavima u oblaku, uključujući socijalni inženjering, slabe lozinke, te ranjivosti u aplikacijama i infrastrukturi.

Jedna od glavnih metoda napada je korištenje socijalnog inženjeringa. Napadači koriste taktike kao što su *phishing* napadi kako bi prevarili korisnike da otkriju svoje vjerodajnice ili da kliknu na zlonamjerne linkove. Ovi napadi često ciljaju zaposlenike u organizacijama, koristeći lažne e-mailove ili poruke koje izgledaju kao legitimne komunikacije. Primjerice, HP Wolf Security izvještava da su napadi pomoću lažnih faktura i dalje česti, gdje napadači šalju e-mailove s lažnim fakturama kako bi naveli korisnike da preuzmu zlonamjerni softver [15].

Osim socijalnog inženjeringa, slabe lozinke predstavljaju značajan rizik. Mnoge organizacije i dalje koriste jednostavne ili ponovljene lozinke, što olakšava napadačima da provale u sustave. Implementacija višefaktorske autentifikacije (MFA) može značajno smanjiti ovaj rizik, omogućujući dodatni sloj sigurnosti koji otežava neovlašteni pristup čak i ako su vjerodajnice kompromitirane [13].

Ranjivosti u aplikacijama i infrastrukturi također su česta meta napada. Napadači iskorištavaju poznate ranjivosti u softveru kako bi dobili pristup sustavima i podacima. Redovito ažuriranje i zakrpe softvera ključni su za smanjenje ovih rizika. Na primjer, napadi na virtualne mašine (VM) poput "*VM escape*" napada omogućuju napadačima da izađu iz izolacije virtualne mašine i pristupe resursima domaćina, što može rezultirati kompromitacijom povjerljivih podataka i aplikacija [13].

Prijenos podataka između korisnika i oblaka također je kritična točka. Ako se podaci ne šifriraju tijekom prijenosa, postoji rizik da ih napadači presretnu. Enkripcija podataka u prijenosu i pohrani ključno je za zaštitu osjetljivih informacija od krađe [16].



Slika 6 Man-in-the-middle-attack, Izvor: O'Reilly, Chris Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly Media , 2023.

Na slici 6 prikazano je kako napadač može presresti promet između dva sustava koristeći metodu „*man-in-the-middle*“ (MITM). Ovaj napad je posebno problematičan u okruženju oblaka, gdje je komunikacija između različitih servisa i aplikacija česta. Bez adekvatne provjere certifikata i šifriranja, TLS enkripcija može biti nedovoljna za zaštitu podataka od ovakvih napada. Implementacija enkripcijskih ključeva i upravljanje certifikatima također su ključni za prevenciju MITM napada. Korištenje alata kao što su AWS Instance Identity Documents i HashiCorp Vault može pomoći u automatskoj generaciji ključeva i certifikata, čime se smanjuje rizik od kompromitacije [13].

Primjer konkretnih incidenata neovlaštenih pristupa i krađa podataka uključuje napad na kompaniju Equifax iz 2017. godine, gdje su napadači iskoristili ranjivost u aplikacijskom softveru kako bi pristupili osobnim podacima više od 147 milijuna ljudi. Ovaj incident naglašava važnost redovitog ažuriranja softvera i primjene sigurnosnih zakrpa kako bi se spriječili slični napadi [17].

Neovlašteni pristup i krađa podataka u računarstvu u oblaku predstavljaju izazov koji zahtijeva sveobuhvatan pristup sigurnosti. Iako tehnologija može pružiti sofisticirane alate za zaštitu, ljudski faktor često ostaje najslabija karika. Stoga, osim tehnoloških rješenja, ključna je kontinuirana edukacija i svijest korisnika o prijetnjama.

3.2. NAPADI NA INFRASTRUKTURU

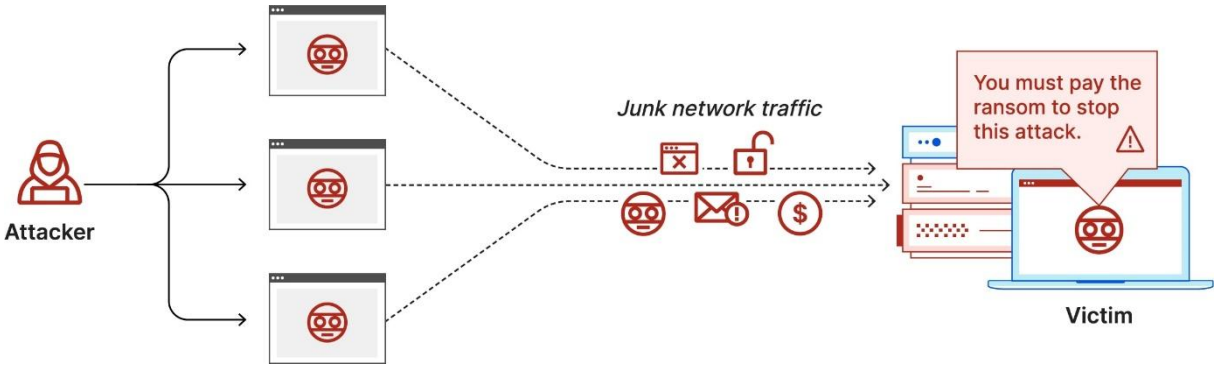
Infrastruktura oblaka predstavlja složeni ekosistem koji može biti meta različitih vrsta napada kao što su DDoS napadi, zlonamjerni softver, napadi pomoću botnet mreža, kao i ciljani napadi na specifične komponente oblaka. Napadi imaju za cilj preopterećenje ili kompromitaciju infrastrukture kako bi se narušila njena dostupnost, integritet ili povjerljivost podataka.

Prijetnje vezane za računalstvo u oblaku mogu se klasificirati prema CIA trijadi: povjerljivost (*Confidentiality*), integritet (*Integrity*) i dostupnost (*Availability*). Prijetnje povjerljivosti uključuju interne prijetnje podacima korisnika, rizik od vanjskih napada i sigurnosne probleme vezane uz podatke. Jedan od ključnih rizika je curenje podataka, koje može imati ozbiljne posljedice za financije tvrtke, povjerenje korisnika i gubitak kupaca. Prijetnje integritetu uključuju rizike vezane uz razdvajanje podataka, slabe kontrole pristupa korisnicima i rizike vezane uz kvalitetu podataka. Slabo upravljanje pristupom može otvoriti vrata napadačima da unište ili manipuliraju podacima, što može imati značajne posljedice na operacije i sigurnost organizacije. Prijetnje dostupnosti uključuju nedostupnost veza, stvarne smetnje resursa i neučinkovite postupke oporavka. Nedostupnost usluga može uzrokovati velike prekide u poslovanju i ugroziti korisničke podatke [16].

Napadi na komponente oblaka mogu se podijeliti u nekoliko kategorija: mrežni napadi, napadi na virtualne strojeve, napadi na pohranu podataka i napadi na aplikacije. Mrežni napadi uključuju napade poput skeniranja portova, botneta i napada lažnog predstavljanja (*spoofing*). Skeniranje portova koristi se za prikupljanje informacija o mrežnoj infrastrukturi kako bi se omogućili daljnji napadi. Botnete napadači koriste za izvođenje raznih zlonamjernih aktivnosti, dok napadi lažnog predstavljanja uključuju prevaru u kojoj napadač lažno predstavlja podatke u ime drugog korisnika. Napadi na virtualne strojeve uključuju bočne kanale (*side-channel attacks*) i zlonamjerni kod koji se umeće u slike virtualnih strojeva. Ovi napadi iskorištavaju specifične ranjivosti u virtualnim okruženjima kako bi kompromitirali sigurnost sustava. Napadi na pohranu podataka uključuju krađu podataka, duplikaciju podataka i uklanjanje podataka. Napadači mogu pristupiti osjetljivim podacima pohranjenim na uređajima i iskoristiti te podatke za daljnje napade. Napadi na aplikacije uključuju ubacivanje *malwarea,* kriptografske napade i napade na web usluge. Ovi napadi mogu rezultirati curenjem podataka, kompromitacijom aplikacija i gubitkom povjerljivosti i integriteta podataka [16].

Botneti su mreže zaraženih uređaja koje se koriste za izvođenje raznih zlonamjernih aktivnosti, uključujući DDoS napade, slanje spama i krađu podataka. Botneti postaju sve sofisticiraniji i otporniji, a njihov broj i upotreba su u porastu. Oni omogućuju napadačima daljinsku kontrolu nad velikim brojem uređaja, što povećava učinkovitost napada [18].

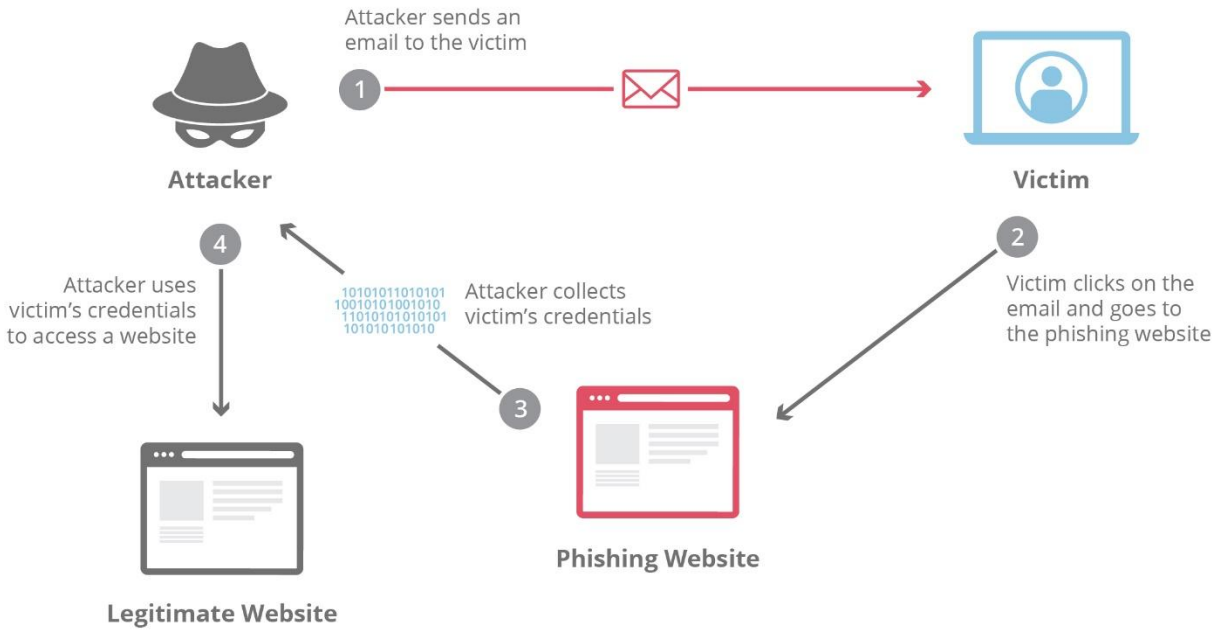
DDoS napadi predstavljaju jedan od najčešćih napada na infrastrukturu oblaka. Ovi napadi uključuju slanje velikog broja zahtjeva prema ciljnom sustavu kako bi se iscrpili resursi i onemogućilo legitimnim korisnicima pristup usluzi. DDoS napadi mogu biti izvedeni na različitim slojevima mreže, uključujući aplikacijski sloj, mrežni sloj ili transportni sloj [13].



Slika 7 DDoS dijagram napada, Izvor: https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/

Slika 7 prikazuje dijagram DDoS (*Distributed Denial of Service*) napada. Na slici možemo vidjeti napadača koji koristi više zaraženih uređaja (botova) za slanje velikog broja zahtjeva prema ciljanom serveru. Botovi generiraju *junk network traffic*, što preopterećuje ciljani server i uzrokuje njegovu nedostupnost. Napad rezultira porukom na uređaju žrtve koja zahtjeva otkupninu kako bi se zaustavio napad. Ovaj dijagram jasno ilustrira kako DDoS napad može iscrpiti resurse servera i onemogućiti pristup legitimnim korisnicima.

Zlonamjerni softver, ili *malware*, može biti u obliku virusa, trojanaca, crva ili *ransomware*a. Ovi programi mogu biti ubačeni u sustav putem *phishing* napada, kompromitiranih aplikacija ili drugih ranjivosti. Kada se jednom nađu unutar infrastrukture oblaka, mogu se koristiti za krađu podataka, ometanje operacija ili čak za preuzimanje kontrole nad cijelim sustavom. Napadi na aplikacijske slojeve uključuju napade poput SQL injekcija, *Cross-Site Scripting*-a (XSS), i *Remote File Inclusion*-a (RFI). Ovi napadi iskorištavaju ranjivosti u aplikacijama koje se izvršavaju na infrastrukturi oblaka kako bi stekli neovlašteni pristup podacima ili kontrolu nad aplikacijama. Na primjer, SQL injekcija omogućava napadaču da izvrši neovlaštene SQL naredbe u bazi podataka aplikacije, što može dovesti do krađe ili brisanja podataka [13].



Slika 8 Phishing dijagram napada, Izvor: https://www.cloudflare.com/learning/access-management/phishing-attack/

Na slici 8 prikazan je dijagram *phishing* napada. Na slici možemo vidjeti kako napadač šalje email žrtvi. Žrtva klikne na email i odlazi na *phishing* web stranicu, gdje napadač prikuplja vjerodajnice žrtve. Zatim napadač koristi prikupljene vjerodajnice za pristup legitimnoj web stranici. Ovaj dijagram jasno ilustrira korake *phishing* napada, od inicijalne poruke emailom do krajnjeg cilja, krađe vjerodajnica i neovlaštenog pristupa.

Upravljanje identitetima i pristupom (IAM) su ključni za sigurnost infrastrukture oblaka. Napadi na IAM mogu uključivati krađu identiteta, zloupotrebu lozinki, te napade na multi-faktorsku autentifikaciju. Napadači često koriste tehnike poput *phishinga* za krađu vjerodajnica, ili iskorištavaju slabe lozinke za dobivanje pristupa sustavima. Kada jednom steknu pristup, napadači mogu iskoristiti svoje privilegije i pristupiti osjetljivim dijelovima infrastrukture [13].

Ransomware-as-a-Service (RaaS) model omogućuje kriminalcima bez tehničkog znanja da koriste *ransomware* alate koje pružaju drugi cyber kriminalci. Ovaj model doprinosi povećanju broja *ransomware* napada, jer omogućuje lakšu distribuciju i upotrebu *ransomwarea*. RaaS operacije su sve sofisticiranije i ciljaju specifične organizacije, što povećava njihovu učinkovitost. *Advanced Persistent Threats* (APT) predstavljaju dugotrajne, sofisticirane napade koje izvode organizirane cyber kriminalne grupe ili državne organizacije. Ovi napadi su često usmjereni na specifične ciljeve i uključuju različite tehnike kako bi se osigurala dugotrajna prisutnost u sustavu. Primjer takvih grupa su Turla, StrongPity i OceanLotus, koje koriste

napredne tehnike za izbjegavanje otkrivanja i postizanje svojih ciljeva. Napadi putem uklonjivih medija, poput USB *stickova*, često se koriste za inicijalni pristup mreži. Maliciozni softver može biti repliciran putem ovih medija i zatim se širiti unutar mreže. Ovi napadi su posebno opasni jer ne ovise o mrežnom pristupu i mogu se širiti čak i u izoliranim sustavima [18].

S razvojem oblaka dolazi i povećana izloženost različitim sigurnosnim prijetnjama. Raznovrsni napadi, od DDoS napada do sofisticiranih *phishing* kampanja, pokazuju da je sigurnost oblaka dinamično polje. Iako se stalno razvijaju nove tehnologije i protokoli za zaštitu, jasno je da će potreba za naprednijim sigurnosnim rješenjima i dalje rasti. Ključno je ne samo ulagati u tehnološka rješenja već i u edukaciju korisnika kako bi se stvorila svijest o sigurnosnim prijetnjama. Samo kombinacijom ovih pristupa možemo se nadati da ćemo ostati korak ispred napadača i osigurati sigurno digitalno okruženje.

3.3. RANJIVOSTI SERVISA U OBLAKU

Servisi u oblaku pružaju mnoge prednosti, uključujući skalabilnost, fleksibilnost i ekonomičnost, no sa sobom donose i određene sigurnosne izazove. Ranjivosti servisa u oblaku mogu biti izuzetno štetne, ne samo zbog potencijalnog gubitka podataka, već i zbog mogućnosti ozbiljnih poremećaja u poslovanju. Kako se sve više organizacija oslanja na oblak kao rješenje za pohranu i obradu podataka, postaje ključno razumjeti i adresirati sigurnosne rizike povezane s ovim tehnologijama.

Ranjivosti u servisima koji se koriste u oblaku mogu imati dalekosežne posljedice na sigurnost podataka i operativnu stabilnost organizacija. Jedna od najznačajnijih ranjivosti je pogrešna konfiguracija oblaka, koja nastaje kada resursi ili servisi u oblaku nisu pravilno konfigurirani u skladu s najboljim sigurnosnim praksama ili regulacijama [19]. Na primjer, ako je spremnik za pohranu podataka slučajno postavljen kao javan, neovlaštene osobe mogu dobiti pristup osjetljivim informacijama. Takve pogrešne konfiguracije mogu dovesti do ozbiljnih kršenja regulacija o zaštiti podataka, što može rezultirati financijskim gubicima, pravnim obvezama i gubitkom reputacije za korisnike i pružatelje usluga oblaka.

Druga značajna ranjivost je curenje podataka, koje se događa kada se podaci nenamjerno ili namjerno prenesu sa sigurnog izvora na neovlaštenu destinaciju. To se može dogoditi putem

nešifriranih komunikacijskih linija, nesigurnih API-ja ili kompromitiranih vjerodajnica. Curenje podataka može rezultirati financijskim gubicima, pravnim problemima i štetom po reputaciju, a također može uništiti konkurentsku prednost tvrtke otkrivanjem povjerljivih informacija konkurentima. Ranjivosti dijeljenih tehnologija također predstavljaju značajan rizik. Budući da cloud servisi često dijele infrastrukturu, platforme i softver među brojnim korisnicima, svaka ranjivost u dijeljenoj tehnologiji može ugroziti sve korisnike. Da bi se smanjili ovi rizici, pružatelji usluga oblaka i njihovi korisnici moraju pravovremeno primjenjivati sigurnosne zakrpe, osigurati izolaciju resursa i stalno pratiti sustave [19].

Svaka ranjivost u oblaku predstavlja potencijalni ulaz za *cyber* napadače, što naglašava potrebu za stalnim unapređivanjem sigurnosnih mjera. Ulaganje u napredne tehnologije, kontinuirano praćenje sustava i edukacija korisnika ključni su elementi u borbi protiv sigurnosnih prijetnji. Samo proaktivnim pristupom možemo osigurati da oblaci ostanu sigurni i pouzdani temelji za poslovanje i inovacije.

4. RIZICI I UPRAVLJANJE RIZICIMA U RAČUNARSTVU U OBLAKU

Računarstvo u oblaku donosi mnoge prednosti, ali i značajne rizike koji zahtijevaju pažljivo upravljanje. Kako sve više organizacija migrira svoje poslovne procese i podatke u oblak, postaje ključno identificirati i analizirati rizike povezane s ovom tehnologijom. Sigurnosni rizici uključuju prijetnje poput zlonamjernih napada, curenja podataka i neovlaštenog pristupa. Upravljanje ovim rizicima zahtijeva implementaciju naprednih sigurnosnih mjera, redovite sigurnosne revizije i edukaciju korisnika o najboljim praksama u zaštiti podataka. Pravna i regulatorna pitanja također igraju značajnu ulogu, jer organizacije moraju osigurati usklađenost s relevantnim zakonima i propisima koji se odnose na zaštitu podataka i privatnost.

Gubitak podataka i oporavak od katastrofa predstavljaju još jedan važan aspekt upravljanja rizicima u oblaku. Organizacije moraju razviti robusne strategije za sigurnosne kopije podataka i planove za oporavak kako bi osigurale kontinuitet poslovanja u slučaju nepredviđenih događaja. Planiranje odgovora na incidente također je ključno, jer omogućuje brzu i učinkovitu reakciju na sigurnosne incidente, minimizirajući potencijalnu štetu. Rizici privatnosti korisnika posebno su važni u kontekstu oblaka, jer oblak često uključuje pohranu i obradu osjetljivih osobnih podataka. Organizacije moraju osigurati da njihovi sustavi i procesi štite privatnost korisnika kroz implementaciju snažnih kontrola pristupa, enkripciju podataka i redovitih sigurnosnih provjera. Konačno, različiti modeli implementacije oblaka – javni, privatni i hibridni – nose sa sobom specifične rizike koje je potrebno pažljivo procijeniti i upravljati [20].

Upravljanje rizicima u oblaku podrazumijeva pažljivo razmatranje svih mogućih problema i prijetnji koje dolaze s korištenjem ove tehnologije. Iako oblak donosi mnoge prednosti poput uštede vremena i novca, također otkriva nove ranjivosti koje mogu uzrokovati velike probleme. Kombinirajući tehničke mjere s odgovornim pristupom, bitno je osigurati da oblak bude siguran i pouzdan za sve korisnike u budućnosti.

4.1. PRAVNA I REGULATORNA PITANJA

Korištenje računarstva u oblaku donosi brojne prednosti, ali i izazove u pogledu pravnih i regulatornih aspekata. Pravna i regulatorna pitanja igraju ključnu ulogu u osiguravanju da podaci i usluge u oblaku budu sigurni i u skladu s važećim zakonima. Usklađenost s propisima

često zahtijeva prilagodbu poslovnih procesa i implementaciju specifičnih sigurnosnih mjera kako bi se zadovoljili standardi zaštite podataka i privatnosti.

Mnoge organizacije koriste oblak za pohranu i obradu osjetljivih podataka, uključujući osobne podatke korisnika i povjerljive poslovne informacije. Stoga je neophodno da te organizacije budu svjesne pravnih zahtjeva koji se primjenjuju na obradu i pohranu tih podataka, kako na nacionalnoj, tako i na međunarodnoj razini. Jedan od ključnih izazova pri korištenju oblaka je rješavanje problema odgovornosti i povjerenja između korisnika i pružatelja usluga oblaka. Pružatelji usluga često odbijaju preuzimanje odgovornosti za sigurnost podataka, prebacujući taj teret na korisnike, što stvara rizik za korisnike koji nemaju uvijek potpuni uvid u sigurnosne mjere koje se provode. Ovaj problem dodatno komplicira činjenica da se sigurnost ne može apsolutno garantirati, te je teško usporediti sigurnosne mjere različitih sustava. Pravni okvir za zaštitu podataka u oblaku također uključuje specifične zakone i regulative koje se razlikuju od zemlje do zemlje. Primjerice, Europska unija ima stroge direktive o zaštiti podataka koje ograničavaju prijenos podataka izvan Unije u zemlje koje nemaju adekvatne zaštite. Ovo ograničava sposobnost američkih pružatelja usluga oblaka da izgrade prekogranične mreže i iskoriste ekonomije razmjera koje oblak nudi. Slične zabrane i ograničenja postoje u mnogim drugim zemljama koje žele osigurati da podaci njihovih građana budu pohranjeni i obrađeni unutar nacionalnih granica [21].

Jedan od ključnih izazova je sigurnost podataka i sustava unutar oblaka. Pružatelji usluga u oblaku moraju osigurati da korisnicima pruže istu razinu sigurnosti i kontrole kao i onu koju bi imali da upravljaju vlastitim sustavima. To uključuje dokazivanje usklađenosti sa sporazumima o razini usluge (SLA) i mogućnost dokaza te usklađenosti revizorima [22].

Pravni i regulatorni problemi također su važni, jer fizička lokacija podatkovnih centara može utjecati na primjenjive zakone. Na primjer, određene kriptografske metode možda nisu dopuštene u nekim zemljama, a nacionalni zakoni mogu zahtijevati da se osjetljivi podaci, poput zdravstvenih zapisa pacijenata, pohranjuju unutar nacionalnih granica [23].

Korištenje oblaka u modernom poslovanju predstavlja dinamičan sukob između tehnoloških inovacija i pravnih ograničenja. Dok oblak nudi nebrojene mogućnosti za poboljšanje efikasnosti i smanjenje troškova, pravni i regulatorni okviri često nisu u koraku s brzim

razvojem tehnologije. Sigurnosni rizici ne smiju biti prepreka napretku, već poticaj za kontinuirano poboljšanje i inovacije u sigurnosnim praksama.

4.2. GUBITAK PODATAKA I OPORAVAK OD KATASTROFA

Kada govorimo o zaštiti podataka i oporavku od katastrofa, ključno je razumjeti kontekst u kojem organizacije danas posluju. U digitalnom dobu, podaci su postali jedan od najvrjednijih resursa, a gubitak podataka može imati katastrofalne posljedice po poslovanje. Stoga, zaštita podataka i osiguranje njihovog brzog oporavka nakon katastrofe predstavlja ključni dio strategije upravljanja rizicima svake organizacije. Takve strategije ne samo da pomažu u minimiziranju prekida u poslovanju, već i u očuvanju povjerenja klijenata, zaštiti reputacije i osiguravanju kontinuiteta poslovanja.

Slika 9 Dijagram plana za oporavak od katastrofa, Izvor: https://www.veritis.com/blog/how-to-plan-an-effective-cloud-disaster-recovery-strategy/

Slika 9 prikazuje dijagram koji opisuje plan za oporavak od katastrofa u oblaku, sastavljen od sedam ključnih koraka. Proces započinje razumijevanjem infrastrukture i procjenom rizika, što je temeljni korak za izradu učinkovitog plana. Nakon što se utvrdi postojeća IT infrastruktura i

identificiraju potencijalni rizici, slijedi provođenje poslovne analize utjecaja (*Business Impact Analysis*). Ova analiza pomaže u određivanju koji su poslovni procesi najvažniji za kontinuitet poslovanja i koji zahtijevaju najvišu razinu zaštite u slučaju katastrofe. Nakon provođenja analize, prelazi se na izradu plana oporavka od katastrofa *(Disaster Recovery Plan*), koji se temelji na definiranim ciljevima vremena oporavka (RTO - *Recovery Time Objective*) i ciljevima točke oporavka (RPO - *Recovery Point Objective*). S ovim informacijama na raspolaganju, važno je odabrati odgovarajućeg pružatelja usluga u oblaku, koji će podržati strategiju oporavka od katastrofa. Izgradnja infrastrukture za oporavak od katastrofa u oblaku je sljedeći korak, a to uključuje implementaciju potrebnih tehnoloških rješenja unutar oblaka koja će omogućiti brz i učinkovit oporavak. Jednako važan je i proces dokumentiranja plana oporavka, koji osigurava da su svi sudionici upoznati s postupcima i odgovornostima unutar plana. Na kraju, plan treba često testirati kako bi se osiguralo da funkcionira ispravno u stvarnim uvjetima i da je spreman za primjenu u slučaju katastrofe.

Prilikom razmatranja strategija za smanjenje rizika od gubitka podataka, ključno je razumjeti prirodu rizika. Rizik je prisutan u svakom trenutku i može se manifestirati na različite načine, bilo da se radi o tehničkim kvarovima, cyber napadima ili prirodnim katastrofama. Upravo zbog ove nepredvidljivosti, organizacije trebaju biti spremne za brzu reakciju i oporavak u slučaju katastrofe. Rizik se može smanjiti kroz pažljivo planiranje i implementaciju zaštitnih mjera, kao što su redovite sigurnosne kopije podataka (*backup*), korištenje enkripcije, i osiguranje protiv cyber napada. Kada dođe do katastrofe, brzina i učinkovitost oporavka postaju ključni faktori u osiguravanju kontinuiteta poslovanja. Plan oporavka od katastrofe treba uključivati detaljan pristup zaštiti i obnovi ključnih poslovnih funkcija. To može uključivati prebacivanje rada na alternativne lokacije, korištenje rezervnih sustava ili čak prelazak na digitalne platforme za rad na daljinu. Poseban naglasak treba staviti na osposobljavanje zaposlenika da brzo i učinkovito reagiraju u kriznim situacijama [24].

Pitanje zaštite podataka u oblaku dodatno je kompliciranо zbog različitih modela usluga (IaaS, PaaS, SaaS) koje pružaju različite razine kontrole i odgovornosti za sigurnost. Na primjer, u SaaS modelu, veći dio odgovornosti za sigurnost leži na pružatelju usluge, dok u IaaS modelu korisnik mora osigurati većinu sigurnosnih mjera, uključujući zaštitu operativnih sustava, aplikacija i podataka. Jedan od ključnih dijelova plana odgovora na incidente jest uspostava učinkovitih mehanizama za obavještavanje i reagiranje. U slučaju sigurnosnog incidenta,

pružatelji usluga u oblaku trebaju odmah obavijestiti svoje korisnike kako bi oni mogli procijeniti potencijalnu štetu. Ovaj proces uključuje aktivaciju hitnog plana koji može obuhvaćati prilagodbu vatrozida na razini aplikacija, analizu zapisa s alata za praćenje aplikacija, pokretanje procedura za oporavak od katastrofa te vraćanje podataka iz postojećih sigurnosnih kopija [25].

Gubitak podataka i oporavak od katastrofa ističu važnost spremnosti i otpornosti u suvremenom poslovanju. Unatoč tehnološkom napretku, organizacije ostaju osjetljive na nepredvidive događaje, a pravi izazov leži u njihovoj sposobnosti da brzo i učinkovito odgovore. Ovi procesi nisu samo tehnička nužnost, već i ključni element za očuvanje povjerenja i stabilnosti u digitalnom svijetu koji se stalno mijenja.

4.3. PLAN ODGOVORA NA INCIDENTE

Kao što je prethodno opisano, ključna komponenta uspješnog oporavka leži u dobro pripremljenim planovima koji osiguravaju kontinuitet poslovanja čak i u najtežim situacijama. Međutim, jednako je važno imati razrađen plan odgovora na incidente koji se fokusira na trenutnu reakciju i suzbijanje sigurnosnih prijetnji u oblaku. Dok se oporavak od katastrofa bavi dugoročnim vraćanjem poslovanja u normalu, plan odgovora na incidente bavi se hitnim odgovorom i minimiziranjem štete u trenutku nastanka incidenta.

Plan odgovora na incidente u oblaku mora biti precizno definiran i uključivati sve ključne korake za prepoznavanje, procjenu, suzbijanje i oporavak od sigurnosnih prijetnji. Prvi korak u ovom procesu je prepoznavanje incidenta, koje zahtijeva stalni nadzor i prikupljanje informacija putem raznih sigurnosnih alata i tehnologija. To omogućuje brzo otkrivanje potencijalnih prijetnji prije nego što se one razviju u ozbiljnije probleme [26].

Jednom kada je incident identificiran, važno je odmah procijeniti njegov opseg i potencijalni utjecaj na poslovanje. Ova procjena pomaže u određivanju prioriteta i resursa koji će biti potrebni za učinkovito suzbijanje prijetnje. Uključivanje timova iz različitih sektora organizacije ključno je za koordiniranu reakciju koja će minimizirati štetu i osigurati brzu stabilizaciju situacije. Sljedeća faza je suzbijanje incidenta, gdje se primjenjuju različite metode kako bi se smanjila njegova štetnost. Ovo može uključivati izolaciju zaraženih sustava, blokiranje neovlaštenih pristupa ili privremeno isključivanje određenih usluga kako bi se

spriječilo daljnje širenje štete. Nakon što je incident suzbijen, fokus se prebacuje na oporavak, gdje se poduzimaju koraci za vraćanje sustava u normalno stanje. To može uključivati ponovno uspostavljanje sigurnosnih kopija, popravak zaraženih sustava ili obnovu izgubljenih podataka [27].

Konačni korak u planu odgovora na incidente je vođenje detaljne post-incident analize, gdje se procjenjuje učinkovitost reakcije i identificiraju mogućnosti za poboljšanje. Ovaj korak je ključan za kontinuirano unaprjeđivanje sigurnosne strategije i pripremu za buduće incidente. Dokumentacija i izvještavanje nakon incidenta također igraju važnu ulogu u ovom procesu, jer omogućuju organizaciji da uči iz iskustva i unaprijedi svoje odgovore na slične prijetnje u budućnosti [26].

Odgovor na sigurnosne incidente nije samo tehnički izazov, već i test zrelosti i otpornosti organizacije. U svijetu koji se neprestano mijenja, gdje prijetnje evoluiraju brže nego ikad prije, sposobnost prilagodbe i brzog odgovora postala je ključna za opstanak i uspjeh. Planiranje i priprema za incidente pokazuje koliko je organizacija svjesna svoje odgovornosti prema sigurnosti podataka i povjerenju svojih korisnika.

4.4. RAZLIKA U RIZICIMA MODELA IMPLEMENTACIJA

Postoje tri glavne vrste oblaka koje organizacije koriste: javni, privatni i hibridni oblak. Svaki od tih modela nudi različite prednosti, ali i nosi određene sigurnosne izazove. Razlike među njima odnose se na način na koji se podaci pohranjuju, kontroliraju i dijele, što direktno utječe na razinu sigurnosti i upravljanja rizicima. Ovisno o potrebama i prirodi podataka koje organizacija koristi, svaki model može pružiti različitu razinu sigurnosti i fleksibilnosti.

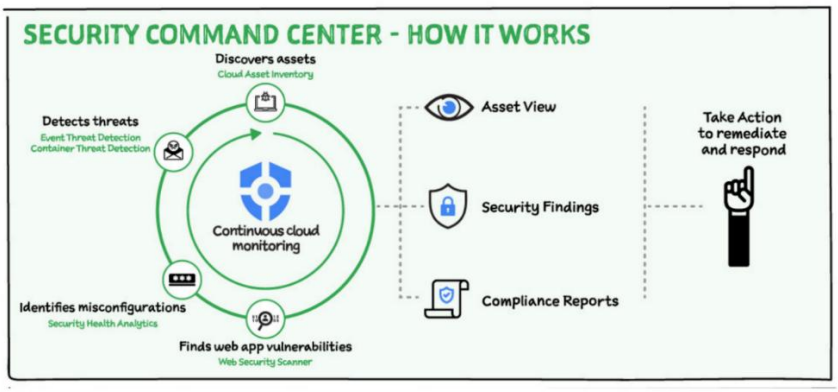
Javni oblak, gdje više korisnika dijeli iste resurse, često pruža skalabilnost i niže troškove, ali dolazi s većim rizikom od sigurnosnih propusta, budući da se podaci pohranjuju na zajedničkim platformama, što može izložiti podatke potencijalnim napadima ili greškama pružatelja usluga. Rizici uključuju i manjak kontrole nad podacima, što može otežati poštivanje određenih regulatornih standarda i privatnosti. Privatni oblak, s druge strane, osigurava mnogo veću razinu kontrole i sigurnosti jer je namijenjen samo jednoj organizaciji. No, ovaj model nosi veće troškove implementacije i održavanja. Privatni oblaci omogućuju potpunu prilagodbu sigurnosnih mjera, što ih čini pogodnim za tvrtke koje upravljaju osjetljivim podacima ili

moraju poštovati iznimno stroge regulatorne zahtjeve. Međutim, visoki troškovi održavanja infrastrukture mogu biti izazov za manje organizacije. Hibridni oblak nudi balans između ova dva modela, kombinirajući sigurnost privatnog oblaka s fleksibilnošću i skalabilnošću javnog oblaka. Organizacije mogu pohraniti osjetljive podatke u privatni oblak, dok manje osjetljive operacije mogu obavljati putem javnog oblaka. Ipak, ovaj model dolazi s većim tehničkim izazovima jer zahtijeva učinkovito upravljanje podacima i prijenos između dva oblaka, što može povećati rizik od pogrešnih konfiguracija ili potencijalnih sigurnosnih ranjivosti [28].

Razlike u rizicima između modela implementacije ne odnose se samo na tehnologiju već i na strategiju upravljanja podacima. Dok javni oblak nudi jednostavnost i pristupačnost, privatni oblak predstavlja fokus na kontrolu i sigurnost. Hibridni oblak simbolizira kompromis između slobode i sigurnosti, omogućujući organizacijama da odlučuju koje dijelove svojih operacija žele izložiti riziku, a koje žele čuvati pod najstrožim uvjetima.

4.5. KONTINUIRANI NADZOR I PROCJENA RIZIKA

U IT okruženjima, a osobito u oblaku, kontinuirani nadzor i procjena rizika ključni su za održavanje sigurnosti i integriteta sustava. S obzirom na dinamičnost i složenost oblačnih okruženja, organizacije su suočene s potrebom za stalnim praćenjem potencijalnih prijetnji i ranjivosti, koje se mogu pojaviti u bilo kojem trenutku. Kontinuirani nadzor omogućuje organizacijama da pravovremeno detektiraju i odgovore na sigurnosne incidente, dok procjena rizika pomaže u identifikaciji rizika prije nego što oni postanu ozbiljna prijetnja.



Slika 10 Procesi za kontinuirani nadzor sigurnosti u oblaku, Izvor: https://cloud.google.com/blog/topics/developers-practitioners/security-monitoring-google-cloud

Kao što je prikazano na slici 10, sigurnosni centar predstavlja primjer sveobuhvatnog pristupa upravljanju sigurnošću u oblaku, kako to implementiraju vodeći pružatelji usluga oblaka. Unutar ovog sustava, svi ključni sigurnosni procesi odvijaju se istovremeno, osiguravajući stalni nadzor i zaštitu. Kontinuirani nadzor oblaka obuhvaća niz aktivnosti, uključujući otkrivanje resursa u oblaku, detekciju prijetnji, identifikaciju nepravilnih konfiguracija, te pronalaženje ranjivosti u web aplikacijama. Sustav neprekidno prati sve resurse povezane s oblakom i odmah reagira na prijetnje, bilo da se radi o zlonamjernim aktivnostima u događajima ili kontejnerskim okruženjima. Svi ovi podaci prikupljaju se i analiziraju u realnom vremenu, što omogućuje izradu sigurnosnih izvješća te izvještaja o usklađenosti, pružajući detaljan pregled stanja sigurnosti u oblaku. Na temelju ovih informacija, organizacija može odmah poduzeti potrebne mjere za otklanjanje problema i dati odgovor na potencijalne sigurnosne incidente. Kontinuirani nadzor i procjena rizika u oblaku funkcioniraju u sinergiji, gdje nadzor prikuplja ključne podatke o stanju sustava, dok procjena rizika analizira te podatke kako bi identificirala i prioritizirala prijetnje te omogućila donošenje odluka koje štite sustav.

Metode i alati za kontinuirani nadzor često se oslanjaju na napredne tehnologije poput umjetne inteligencije i strojnih algoritama, koji su sposobni prepoznati obrasce ponašanja koji odstupaju od normalnog i automatski pokrenuti odgovarajuće sigurnosne mjere. Na primjer, sustavi za detekciju proboja (IDS) i sustavi za prevenciju proboja (IPS) ključni su u zaštiti od vanjskih prijetnji, dok alati za nadzor aplikacija pomažu u otkrivanju unutarnjih prijetnji, poput zlonamjernih aktivnosti korisnika ili grešaka u kodiranju. Nakon identifikacije rizika, sljedeći korak je procjena vjerojatnosti i potencijalnog utjecaja tih prijetnji na sustav. Ova procjena omogućuje prioritizaciju prijetnji i fokusiranje resursa na najkritičnija područja. Procjena rizika također uključuje procjenu ranjivosti sustava, što podrazumijeva analizu sigurnosnih mjera koje su već implementirane i njihovu učinkovitost u zaštiti od identificiranih prijetnji [13].

Kontinuirani nadzor i procjena rizika u oblaku su ključni za osiguravanje stabilnosti i sigurnosti u digitalnom okruženju. U vrijeme kada su prijetnje sve sofisticiranije, ove prakse omogućuju organizacijama da budu korak ispred potencijalnih problema.

5. SIGURNOSNI MEHANIZMI, PRAKSE I PRINCIPI

Sigurnosni mehanizmi, najbolje prakse i osnovni principi zaštite u oblaku osiguravaju da podaci i usluge ostanu zaštićeni od prijetnji, dok se istovremeno zadovoljavaju zahtjevi za pouzdanost, povjerljivost i dostupnost. Da bi se osigurala kvalitetna zaštita podataka u oblaku, potrebno je primijeniti razne sigurnosne mjere i pridržavati se smjernica koje su razvile vodeće organizacije u industriji.

Uspostava učinkovitih sigurnosnih mehanizama u oblaku zahtijeva razumijevanje osnovnih principa zaštite, kao što su povjerljivost, integritet i dostupnost podataka, što čini takozvanu CIA trijadu. Ovi principi postavljaju temelj za izgradnju robusnih sigurnosnih arhitektura u oblaku. Uz to, od suštinske je važnosti primjena najboljih praksi koje su razvijene kroz iskustva i preporuke stručnih tijela poput Cloud Security Alliance-a (CSA). CSA nudi smjernice za implementaciju sigurnosnih mjera koje omogućuju organizacijama da sigurno upravljaju svojim podacima i aplikacijama u oblaku [29].

Jedan od bitnih elemenata sigurnosti u oblaku je pentesting ili penetracijsko testiranje, koje pomaže u identifikaciji sigurnosnih slabosti u sustavu prije nego što ih zlonamjerni akteri mogu iskoristiti. Autentifikacija i autorizacija igraju ključnu ulogu u kontroli pristupa podacima, dok enkripcija osigurava da podaci ostanu zaštićeni čak i ako dođe do neovlaštenog pristupa. Načelo najmanjih privilegija, ograničava pristup korisnicima samo za one resurse koji su im nužni za obavljanje zadataka, te je također ključno za minimiziranje rizika [30].

U konačnici, sigurnost u oblaku nije statičan cilj, već dinamičan proces koji zahtijeva stalnu prilagodbu. Kako tehnologija i prijetnje evoluiraju, tako i sigurnosne prakse moraju biti fleksibilne i sposobne da odgovore na nove izazove. Budućnost sigurnosti u oblaku ovisi o našoj sposobnosti da razumijemo i primijenimo ove principe, ne samo kao tehničke zahtjeve, već kao temeljne vrijednosti u izgradnji povjerenja u digitalnom okruženju.

5.1. CSA – CLOUD SECURITY ALLIANCE

Cloud Security Alliance (CSA) je vodeća organizacija koja postavlja smjernice, najbolje prakse i standarde za sigurnost u računarstvu u oblaku. Osnovana je s ciljem da pomogne organizacijama u prepoznavanju i ublažavanju sigurnosnih prijetnji specifičnih za oblak.

Njihove smjernice i okvirni standardi prepoznati su globalno i često se koriste kao osnova za implementaciju sigurnosnih mjera u oblaku.

Jedna od ključnih inicijativa koju je pokrenula CSA je *Cloud Controls Matrix* (CCM), koji pruža sveobuhvatan okvir sigurnosnih kontrola posebno dizajniranih za cloud okruženje. CCM pokriva razne aspekte računarstva u oblaku, uključujući upravljanje rizicima, sigurnost podataka, upravljanje identitetima i enkripciju. Ovaj alat pomaže organizacijama da procjene svoje sigurnosne potrebe i osiguraju usklađenost s međunarodnim standardima kao što su ISO 27001, HIPAA i drugi. CSA također predvodi inicijative koje se bave specifičnim aspektima sigurnosti u oblaku, poput STAR (*Security, Trust & Assurance Regist*ry) certifikacije, koji omogućuje pružateljima cloud usluga da transparentno prikažu svoje sigurnosne kontrole i prakse. Ovaj registar pomaže korisnicima da donesu informirane odluke prilikom odabira cloud usluga, osiguravajući da su njihovi podaci zaštićeni u skladu s najvišim sigurnosnim standardima [31].

CSA nudi i certificiranje poput *Certified Cloud Security Professional* (CCSP), koje je prepoznato kao vodeći certifikat u industriji za profesionalce koji žele produbiti svoje znanje o sigurnosti u oblaku. Ovi certifikati pokrivaju širok spektar tema, uključujući upravljanje rizicima, pravne aspekte računarstva u oblaku, kao i tehničke aspekte zaštite podataka i infrastrukture. Certifikacija CCSP, razvijena u suradnji s (ISC)², osmišljena je kako bi pomogla stručnjacima da steknu duboko razumijevanje sigurnosnih izazova i primjene sigurnosnih praksi u oblaku [30].

U širem kontekstu, Cloud Security Alliance igra ključnu ulogu u oblikovanju sigurnosnih standarda u oblaku. Kroz svoje inicijative i smjernice, CSA ne samo da pomaže organizacijama da implementiraju najbolje prakse, već i promovira kontinuirano unapređenje sigurnosnih mjera kako bi one bile u skladu s tehnološkim razvojem i promjenjivim prijetnjama. Njihov rad utječe na sve sektore koji koriste cloud tehnologiju, pružajući temelj za pouzdan i siguran razvoj digitalne infrastrukture.

5.2. CIA TRIJADA

CIA trijada (*Confidentiality, Integrity, Availability*) predstavlja osnovni koncept u informacijskim sigurnosnim strategijama, te se koristi kao temelj za osiguranje podataka i

sustava u različitim IT okruženjima, uključujući računarstvo u oblaku. Ova trijada obuhvaća tri ključna elementa koji su kritični za zaštitu podataka: povjerljivost, integritet i dostupnost.

Povjerljivost (*Confidentiality*) se odnosi na sprječavanje neovlaštenog pristupa informacijama. U računarstvu u oblaku, povjerljivost se postiže kroz različite metode kao što su enkripcija podataka, kontrola pristupa, i autentifikacija korisnika. Ove mjere osiguravaju da samo ovlašteni korisnici imaju pristup osjetljivim podacima, čime se štiti privatnost i osjetljive informacije organizacija i pojedinaca. Integritet (*Integrity*) se odnosi na točnost i pouzdanost podataka, osiguravajući da se podaci ne mogu mijenjati ili brisati bez autorizacije. U kontekstu oblaka, integritet podataka osigurava se kroz tehnologije koje omogućavaju detekciju i sprječavanje neovlaštenih promjena, kao što su digitalni potpisi i hash funkcije. Cilj je osigurati da su podaci koji se pohranjuju, prenose ili obrađuju točni i konzistentni, što je ključno za povjerenje u informacijske sustave. Dostupnost (*Availability*) osigurava da su podaci i resursi dostupni ovlaštenim korisnicima u svakom trenutku kada su im potrebni. To se postiže kroz implementaciju redundancije, sigurnosnih kopija i robusnih planova oporavka od katastrofa. U oblaku, dostupnost je kritična jer se podaci i aplikacije često koriste u realnom vremenu, a korisnici očekuju neprekidan pristup bez obzira na tehničke ili vanjske probleme. Održavanje visoke razine dostupnosti ključno je za kontinuitet poslovanja i zadovoljstvo korisnika [32].

Razumijevanje i implementacija CIA trijade omogućava organizacijama da izgrade robusne sigurnosne strategije koje ne samo da štite podatke, već i osiguravaju povjerenje korisnika u njihove usluge.

5.3. PENTESTING

Pentesting ili penetracijsko testiranje je ključna sigurnosna praksa koja se koristi za identifikaciju ranjivosti u računalnim sustavima, aplikacijama i mrežama. Ova metoda simulira napade koje bi mogli izvršiti zlonamjerni hakeri, ali ih provode etički hakeri, poznati kao "*penetration testers*" ili "pentesteri". Cilj pentestinga nije samo otkriti slabosti, već i demonstrirati kako bi te slabosti mogle biti iskorištene te pružiti preporuke za njihovo otklanjanje [33].

Slika 11 Proces penetration testinga, Izvor: https://plextrac.com/blog/hack-the-10-steps-of-the-pentesting-routine/

Na slici 11 vidimo ciklički proces penetracijskog testiranja koji se sastoji od deset faza. Prva faza je postavljanje, gdje se definira okruženje i ciljevi testiranja. Zatim slijedi otkrivanje, gdje pentesteri prikupljaju informacije o ciljnim sustavima, i enumeracija, koja omogućava detaljniju analizu mrežnih resursa i korisničkih računa. Nakon toga dolazi faza detekcije, gdje se identificiraju potencijalne ranjivosti. Sljedeća faza je eksploatacija, u kojoj pentesteri pokušavaju iskoristiti pronađene ranjivosti. Post-eksploatacija omogućava procjenu koliko daleko napadač može napredovati u sustavu. U fazi izvještavanja, svi nalazi se dokumentiraju i predstavljaju ključnim dionicima u fazi iščitavanja rezultata. Nakon toga, dolazi se do ispravka, gdje se poduzimaju potrebne mjere za otklanjanje ranjivosti, a cijeli proces završava sa završnim testiranjem, kojim se provjerava učinkovitost provedenih korektivnih akcija.

Pentesting se može provoditi na različitim razinama, od jednostavnih skeniranja sigurnosnih propusta do složenih, ciljanih napada koji oponašaju stvarne prijetnje. Postoje dvije glavne vrste pentestinga: crna kutija (*black box*), gdje pentester nema prethodne informacije o sustavu koji se testira, i bijela kutija (*white box*), gdje pentester ima potpuni uvid u sustav i njegovu arhitekturu. Obje metode imaju svoje prednosti, a često se koriste u kombinaciji kako bi se postigla sveobuhvatna sigurnosna provjera [33].

Pentesting organizacijama omogućava da na vrijeme identificiraju i otklone potencijalne prijetnje. U svijetu gdje su cyber napadi u stalnom razvoju, pentesting postaje nezamjenjiv dio suvremenih sigurnosnih strategija, pomažući organizacijama da zaštite svoje resurse i održe povjerenje korisnika.

5.4. AUTENTIFIKACIJA I AUTORIZACIJA

Autentifikacija i autorizacija predstavljaju dva ključna sigurnosna mehanizma koji su esencijalni za zaštitu podataka u oblaku. Autentifikacija se odnosi na proces potvrđivanja identiteta korisnika koji pokušava pristupiti određenom resursu, dok se autorizacija odnosi na određivanje razine pristupa koju taj korisnik ima nakon što je njegov identitet potvrđen. Ovi mehanizmi zajedno osiguravaju da samo ovlašteni korisnici mogu pristupiti osjetljivim podacima i sustavima, čime se smanjuje rizik od neovlaštenog pristupa i potencijalnih sigurnosnih incidenata. U oblaku, autentifikacija često koristi višefaktorski pristup, uključujući nešto što korisnik zna (lozinku), nešto što korisnik ima (autentifikacijski token), ili nešto što korisnik jest (biometrijski podaci). Ovaj višeslojni pristup smanjuje rizik od neovlaštenog pristupa, čak i ako su vjerodajnice korisnika kompromitirane. Na primjer, nakon unosa lozinke, korisnik može biti zatražen da unese jednokratni kod poslan na njegov mobilni uređaj, čime se dodatno osigurava da je prava osoba na pravom računu [13].

Autorizacija, s druge strane, koristi se za kontrolu pristupa resursima unutar oblaka, često kroz sustave kao što je *role-based access control* (RBAC). RBAC omogućava organizacijama da definiraju uloge i povezuju ih s određenim pravima pristupa, čime se osigurava da korisnici imaju pristup samo onim podacima i resursima koji su im potrebni za obavljanje njihovih zadataka. Na ovaj način se minimizira rizik od neovlaštenog pristupa osjetljivim informacijama unutar organizacije [34].

U konačnici, učinkovita implementacija autentifikacije i autorizacije ključna je za zaštitu podataka u oblaku. Ove sigurnosne mjere omogućavaju organizacijama da osiguraju povjerljivost, integritet i dostupnost svojih resursa, istovremeno održavajući usklađenost s regulativama i standardima sigurnosti.

5.5. ENKRIPCIJA PODATAKA

Enkripcija podataka ključni je alat za zaštitu informacija u oblaku. Kako se sve više osjetljivih podataka prenosi i pohranjuje u cloud okruženjima, enkripcija osigurava da ti podaci ostanu sigurni čak i u slučaju neovlaštenog pristupa.

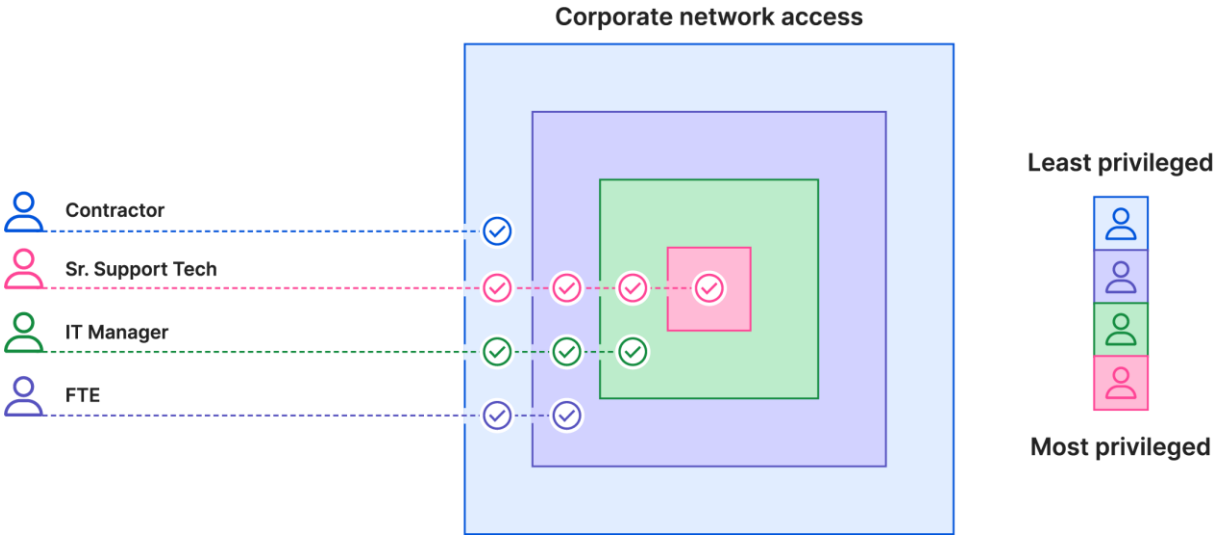
Enkripcija pretvara običan tekst u nečitljiv kodirani tekst pomoću kriptografskih algoritama, čime se osigurava da podaci mogu biti pročitani samo od strane onih koji posjeduju odgovarajući ključ za dekripciju. Jedna od ključnih preporuka NIST-a za enkripciju podataka u mirovanju (*data at rest*) je korištenje *Advanced Encryption Standard* (AES) algoritma za enkripciju podataka. AES, koji je definiran kao *Federal Information Processing Standard* (FIPS) 197, nudi visoku razinu sigurnosti i koristi se za zaštitu osjetljivih informacija u mnogim industrijama. AES-256, koji koristi 256-bitne ključeve, posebno se preporučuje za zaštitu visoko osjetljivih podataka zbog svoje otpornosti na kriptografske napade. Enkripcija podataka u prijenosu (*data in transit*) osigurava se primjenom kriptografskih protokola poput *Transport Layer Security* (TLS). TLS je dizajniran da osigura privatnost i integritet podataka između aplikacija putem mreže, štiteći podatke od presretanja i manipulacije tijekom prijenosa. Prema NIST-u, implementacija TLS-a je kritična za osiguravanje sigurnog prijenosa podataka, posebno u cloud okruženjima gdje podaci često prolaze kroz neovlaštene mrežne segmente. NIST također naglašava važnost pravilnog upravljanja kriptografskim ključevima, jer sigurnost enkripcije izravno ovisi o zaštiti tih ključeva. Preporuča se korištenje sigurnih metoda za generiranje, distribuciju, pohranu i rotaciju kriptografskih ključeva, kako bi se osigurala trajna zaštita kriptiranih podataka [35].

Enkripcija također igra ključnu ulogu u osiguravanju usklađenosti s globalnim regulativama i standardima zaštite podataka, kao što su GDPR u Europi ili HIPAA u SAD-u. Ovi propisi često zahtijevaju enkripciju osjetljivih podataka kao mjeru za zaštitu privatnosti i sigurnosti korisnika [36].

U konačnici, enkripcija podataka, kako u prijenosu tako i u mirovanju, predstavlja ključni aspekt sigurnosti u oblaku, omogućavajući organizacijama da zaštite svoje informacije od neovlaštenog pristupa i zadrže usklađenost s regulatornim zahtjevima.

5.6. NAČELO NAJMANJIH PRIVILEGIJA

Načelo najmanjih privilegija (*Principle of Least Privilege*) jedan je od najvažnijih sigurnosnih principa u upravljanju pristupom unutar računalnih sustava, uključujući i oblake. Ovo načelo nalaže da korisnici i aplikacije trebaju imati samo one privilegije koje su apsolutno potrebne za obavljanje njihovih zadataka, i ništa više od toga. Ograničavanjem pristupa minimizira se rizik od neovlaštenih aktivnosti, čime se značajno smanjuje površina napada unutar sustava.



Slika 12 Prikaz načela najmanjih privilegija u kontekstu korporativnog pristupa mreži, Izvor: https://www.cloudflare.com/learning/access-management/principle-of-least-privilege/

Na slici 12 vidimo prikaz načela najmanjih privilegija u kontekstu korporativnog pristupa mreži. Slika prikazuje različite razine pristupa koje imaju različiti korisnici unutar organizacije, organizirane u slojevima koji predstavljaju razine pristupa mrežnim resursima. Korisnici su podijeljeni u četiri kategorije: Contractor (Vanjski suradnik), Sr. Support Tech (Senior tehničar za podršku), IT Manager (IT Menadžer) i FTE (Prosječni zaposlenik s punim radnim vremenom). Svaka od ovih uloga ima različitu razinu pristupa unutar korporativne mreže. Vanjski suradnik ima najnižu razinu pristupa i može pristupiti samo vanjskim slojevima mreže. FTE ima nešto širi pristup, koji obuhvaća dodatne resurse unutar mreže. IT Manager ima još veći pristup mrežnim resursima, dok Sr. Support Tech ima najvišu razinu pristupa, koja mu omogućava pristup i najosjetljivijim dijelovima mreže. Ovaj prikaz ilustrira kako načelo najmanjih privilegija ograničava pristup prema potrebama korisnika, osiguravajući da svaka uloga unutar organizacije ima samo one ovlasti koje su potrebne za obavljanje njenih zadataka. Na taj način se smanjuje rizik od neovlaštenog pristupa i potencijalnih sigurnosnih propusta.

U kombinaciji sa Zero Trust modelom, načelo najmanjih privilegija dodatno pojačava sigurnost oblaka. Zero Trust pristup naglašava da nijedan entitet ne bi trebao automatski dobiti povjerenje bez obzira na to nalazi li se unutar ili izvan organizacijske mreže. U ovom kontekstu, POLP se koristi za ograničavanje pristupa svakom dijelu sustava samo na osnovu dokaza o potrebnoj funkcionalnosti. Svaki pristup mora biti verificiran i opravdan, što smanjuje rizik od internih prijetnji i neovlaštenih upada. Zero Trust i POLP zajedno stvaraju višeslojni sigurnosni model

koji smanjuje potencijalne vektore napada i osigurava integritet i sigurnost podataka unutar oblaka [13].

Načelo najmanjih privilegija pomaže organizacijama da unaprijede svoju sigurnost, smanje ranjivosti i zaštite svoje podatke i resurse u dinamičnom okruženju oblaka. Primjenom ovog načela, pristup se strogo ograničava na ono što je neophodno, čime se značajno smanjuje mogućnost zloupotrebe ovlasti.

5.7. OWASP TOP 10

OWASP Top 10 predstavlja listu najvećih sigurnosnih rizika za web aplikacije u današnjem digitalnom svijetu. Ova lista se ažurira svakih 3 do 4 godine, a najnovija verzija, objavljena 2021. godine, reflektira promjene u prijetnjama i tehnološkim trendovima. OWASP Top 10 nije samo tehnički vodič, već je i upozorenje za developere i organizacije da obrate pažnju na sigurnosne propuste koji mogu ozbiljno ugroziti njihove aplikacije. Namijenjena je kao podsjetnik da je sigurnost temeljni dio razvoja web aplikacija i digitalne infrastrukture te da zahtijeva stalno ulaganje napora i resursa.

OWASP TOP 10 Lista sigurnosnih rizika:

1. Zloupotreba kontrole pristupa (*Broken Access Control*): Kada aplikacija neadekvatno implementira kontrole pristupa, napadači mogu dobiti neovlašteni pristup resursima ili podacima. Najčešći propusti uključuju neograničene privilegije i zaobilaženje autentifikacijskih mehanizama.
2. Kriptografski propusti (*Cryptographic Failures*): Ovaj rizik se javlja kada aplikacija neadekvatno štiti osjetljive podatke, bilo tijekom prijenosa ili pohrane. Primjeri uključuju slabe ili zastarjele enkripcijske algoritme, kao i neprimjenjivanje enkripcije na osjetljive informacije.
3. Umetanje koda (*Injection*): Zlonamjerni kod može biti ubačen u aplikaciju kroz nesigurne unose podataka. To uključuje *SQL injection, NoSQL injection* i druge vrste napada koji iskorištavaju ranjivosti u procesima validacije unosa, omogućavajući napadačima izvršavanje neovlaštenih komandi ili pristup povjerljivim podacima.
4. Nesigurno dizajniranje (*Insecure Design*): Ovo se odnosi na manjak sigurnosnih mjera već na razini dizajna aplikacije. Aplikacije dizajnirane bez razmatranja sigurnosnih

aspekata često su lak plijen napadača, jer ranjivosti mogu biti ukorijenjene duboko u osnovnoj arhitekturi.

5. Sigurnosni propusti u komponentama trećih strana (*Vulnerable and Outdated Components*): Korištenje zastarjelih ili ranjivih biblioteka i softverskih komponenti može ugroziti sigurnost cijele aplikacije. Često se koriste nesvjesno ili se ne ažuriraju na vrijeme, ostavljajući prostor za napade.
6. Pogrešna konfiguracija sigurnosti (*Security Misconfiguration*): Propusti u konfiguraciji sigurnosnih postavki, kao što su neispravni sigurnosni certifikati, nepotpuna ažuriranja softvera ili korištenje zadatih lozinki, mogu omogućiti napadačima da iskoriste te ranjivosti.
7. Propusti u identifikaciji i autentifikaciji (*Identification and Authentication Failures*): Slabi sustavi za autentifikaciju i loša zaštita korisničkih podataka mogu omogućiti napadačima da preuzmu kontrolu nad korisničkim računima ili se lažno predstavljaju kao drugi korisnici.
8. Nepouzdana integracija podataka (*Software and Data Integrity Failures*): Aplikacije koje ne primjenjuju adekvatne mjere zaštite integriteta podataka mogu postati meta napada gdje se manipulira softverskim kodom ili podacima kako bi se omogućile zlonamjerne aktivnosti.
9. Nedostatak praćenja i zapisivanja sigurnosnih događaja (*Security Logging and Monitoring Failures*): Ako aplikacija ne bilježi sigurnosne događaje ili nema adekvatno praćenje aktivnosti, napadi mogu ostati neotkriveni, omogućujući napadačima kontinuirani pristup bez ometanja.
10. Nesigurni zahtjevi prema serverima (*Server-Side Request Forgery – SSRF*): Ovaj napad omogućava napadačima da pošalju lažne zahtjeve poslužitelju, često zaobilaženjem sigurnosnih mjera i pristupom osjetljivim informacijama [37].

Zaključno, OWASP Top 10 nije samo popis tehničkih ranjivosti, već ključni alat za podizanje svijesti o sigurnosnim prijetnjama. Njegova važnost ne leži samo u tehničkom kontekstu, već i u upravljanju rizicima na razini cijele organizacije. Korištenjem ove liste, ne samo developeri, već i menadžeri, timovi za sigurnost i svi uključeni u životni ciklus razvoja softvera mogu razumjeti gdje su najkritičnije ranjivosti i kako ih rješiti. OWASP Top 10 pomaže organizacijama u usvajanju boljih sigurnosnih praksi, što ne samo da smanjuje izloženost prijetnjama, već jača povjerenje korisnika i štiti ugled tvrtki.

6. ULOGA KORISNIKA I PRUŽATELJA USLUGA U OBLAKU

Računarstvo u oblaku revolucioniralo je način na koji organizacije koriste i upravljaju IT resursima. Umjesto održavanja lokalnih podatkovnih centara, mnoge tvrtke sada ovise o pružateljima usluga u oblaku (CSP) za pohranu podataka, izračune i pristup aplikacijama. Međutim, s prijelazom na oblak dolazi i novi koncept odgovornosti: model podijeljene odgovornosti (*shared responsibility model*). Ovaj model definira kojim sigurnosnim aspektima upravlja pružatelj usluge, a kojim korisnik. Kako bi se osigurala potpuna zaštita podataka i sustava, oba sudionika moraju jasno razumjeti svoje uloge i obveze te uskladiti svoje sigurnosne prakse.

U SaaS modelu pružatelj usluge brine o sigurnosti same aplikacije, kao i o njenoj infrastrukturi, dok korisnik preuzima odgovornost za sigurnost podataka. Nasuprot tome, u IaaS modelu pružatelj usluga osigurava sigurnost svih infrastrukturnih komponenti, dok je korisnik odgovoran za sigurnost bilo koje aplikacije instalirane na infrastrukturi. PaaS model predstavlja sredinu između ova dva pristupa, gdje pružatelj usluge upravlja platformom, a korisnik je odgovoran za sigurnost aplikacija koje razvija na toj platformi [38].

Iako je podjela jasna na papiru, mnoge organizacije se bore s razumijevanjem točne raspodjele odgovornosti. Posljedica toga često su loše konfiguracije usluga u oblaku, poput primjerice nesigurnih postavki u AWS S3 bucketima, koje mogu dovesti do ozbiljnih sigurnosnih incidenata. Kako bi se smanjio rizik, ključno je uvesti snažne mjere za upravljanje identitetom i pristupima te koristiti rješenja za upravljanje sigurnosnim stanjem oblaka, koja automatiziraju praćenje i ispravke potencijalnih ranjivosti [13].

Model podijeljene odgovornosti osnova je sigurnosnog okvira za oblak, ali njegova učinkovitost ovisi o razumijevanju i suradnji između korisnika i pružatelja usluga. Dok pružatelji osiguravaju sigurnost infrastrukture i platformi, korisnici moraju aktivno upravljati svojim podacima, konfiguracijama i pristupima. U tom kontekstu, educiranje korisnika kako bi ispravno razumjeli svoje sigurnosne obveze i korištenje naprednih alata za praćenje sigurnosnog stanja postaje ključni element uspješne primjene sigurnosnih praksi u oblaku.

6.1. SURADNJA I UGOVORI U O RAZINI USLUGE (SLA)

U modernom poslovanju, gdje su aplikacije i podaci sve češće premješteni u oblak, postavlja se pitanje kako osigurati stabilnost i kvalitetu usluga na koje se korisnici oslanjaju. S obzirom na to da tvrtke često ovise o pružateljima usluga u oblaku za ključne operacije, nužno je uspostaviti jasne smjernice koje definiraju što korisnici mogu očekivati, a što pružatelji moraju isporučiti. U ovom kontekstu dolazi do izražaja važnost ugovora o razini usluge (SLA), koji djeluje kao most između korisničkih potreba i tehničkih mogućnosti pružatelja.

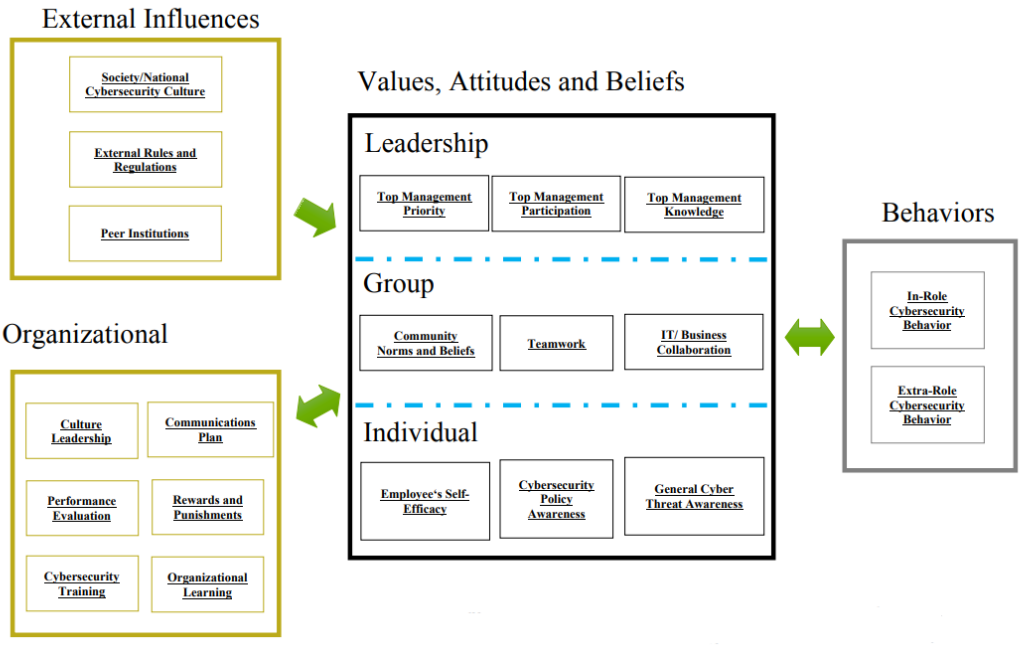
SLA (*Service level agreements*), ugovori o razini usluge predstavljaju ključan dio suradnje između korisnika i pružatelja usluga u oblaku, osiguravajući jasno definirane standarde i odgovornosti za obje strane. SLA-ovi su posebno važni jer omogućuju korisnicima da unaprijed razumiju kakvu razinu usluge mogu očekivati, uključujući dostupnost, sigurnost i vrijeme odaziva na probleme. Za pružatelje usluga, SLA-ovi pomažu u održavanju visokih standarda kvalitete i odgovornosti, stvarajući transparentan odnos temeljen na mjerljivim kriterijima. Primjerice, u SLA-ovima za cloud usluge, kao što su AWS ili druge vodeće platforme, često se navodi jamstvo visoke dostupnosti, primjerice 99.99% dostupnosti tijekom određenog vremenskog razdoblja. Osim dostupnosti, SLA-ovi definiraju mjere za rješavanje eventualnih problema, kao što su vrijeme odgovora na zahtjeve korisnika i planovi za oporavak u slučaju prekida usluge. U slučaju nepoštivanja dogovorenih standarda, korisnici mogu ostvariti prava na određene oblike naknade, poput servisnih kredita, koji se obračunavaju u skladu s prekršenim razinama usluge. Još jedan važan element SLA-a je osiguranje sigurnosnih mjera, gdje pružatelji usluga moraju jamčiti primjenu protokola poput enkripcije podataka, redovitih sigurnosnih ažuriranja i zaštite privatnosti podataka. Ovaj dio SLA-a često uključuje i planove za oporavak podataka i detalje o sigurnosnim postupcima u slučaju incidenta [39].

Zaključno, SLA omogućava korisnicima i pružateljima usluga da uspostave stabilan temelj za dugoročnu suradnju, postavljajući jasna pravila i odgovornosti za obje strane. Kroz precizno definirane uvjete usluge, kao što su dostupnost, performanse, sigurnost i vrijeme reakcije, SLA pomaže u izgradnji povjerenja između svih strana. Korisnici tako stječu sigurnost da će njihovi ključni poslovni procesi biti podržani stabilnim i pouzdanim uslugama na koje se mogu osloniti, dok pružatelji usluga mogu učinkovitije planirati resurse i održavati visoke standarde kvalitete.

6.2. EDUKACIJA I SVIJEST KORISNIKA

U današnjem digitalnom okruženju, edukacija korisnika o sigurnosnim prijetnjama postaje ključna komponenta svakog uspješnog sigurnosnog sustava. *Cyber* prijetnje su u stalnom porastu, a ljudske greške, poput slabe lozinke ili nepažnje pri otvaranju *phishing* e-mailova, često predstavljaju najslabiju kariku u obrani. Upravo zbog toga organizacije moraju ulagati u kontinuiranu edukaciju zaposlenika, čime ih osposobljavaju da prepoznaju prijetnje i reagiraju na odgovarajući način.

Edukacija korisnika mora pokriti nekoliko ključnih sigurnosnih aspekata kako bi organizacija bila cyber-otporna. Lozinke i pristupni podaci predstavljaju prvi sloj obrane, stoga je važno naučiti korisnike kako stvarati jake lozinke i redovito ih mijenjati. Sigurnost komunikacijskih kanala, posebno zaštita e-mailova od *phishing* napada, također je ključna jer mnogi napadi započinju kroz nepažnju korisnika. Prevencija *malwarea* zahtijeva svijest o instaliranju neovlaštenih aplikacija, dok je edukacija o mobilnim uređajima i prijenosnim medijima važna kako bi se spriječilo neovlašteno prodiranje u sustav putem uređaja koji korisnici koriste [40].



Slika 13 Model za izgradnju kulture kibernetičke sigurnosti, Izvor: https://cams.mit.edu/wp-content/uploads/Building-a-Culture-of-Cybersecurity.pdf

Na slici 13 prikazan je složen odnos između različitih čimbenika koji zajedno stvaraju kulturu kibernetičke sigurnosti unutar organizacije. U sredini slike nalaze se tri razine odgovornosti

koje utječu na stavove i ponašanje u vezi s kibernetičkom sigurnošću: liderstvo, grupe i pojedinci. Na razini liderstva, ključni su prioriteti menadžmenta, njihovo sudjelovanje u sigurnosnim procesima te razina znanja koju posjeduju o *cyber* prijetnjama. Upravo je ova razina odgovorna za kreiranje općeg smjera i strateških odluka vezanih uz sigurnost. Ako vrh menadžmenta ne postavi sigurnost kao prioritet, teško je očekivati da će ostali dijelovi organizacije ozbiljno pristupiti tom pitanju. Grupna razina odnosi se na zajedničke norme i vjerovanja unutar organizacijskih timova, gdje timski rad i suradnja između IT odjela i drugih poslovnih jedinica igraju ključnu ulogu. Ovo područje sugerira da uspješna cyber sigurnost ovisi o koordinaciji između različitih sektora unutar organizacije. Na razini pojedinca, naglasak je stavljen na osobnu svijest zaposlenika o prijetnjama, njihovo samopouzdanje u primjeni sigurnosnih politika i opća svjesnost o cyber prijetnjama. Ovdje je ključna uloga edukacije i treninga koji pomažu pojedincima da postanu proaktivni sudionici u zaštiti organizacije.

Navedeni interni čimbenici (liderstvo, grupa i pojedinac) ne djeluju izolirano, već su pod utjecajem vanjskih čimbenika kao što su društvena kultura cyber sigurnosti, vanjske regulative i prakse drugih institucija. Ovi vanjski utjecaji postavljaju šire okvire unutar kojih organizacija mora razvijati svoje sigurnosne prakse. Na kraju, dolazimo do ponašanja koja proizlaze iz svega navedenog. Ponašanja se dijele na "*In-role*", što predstavlja formalne sigurnosne zadatke koje zaposlenici moraju obavljati, i "*Extra-role*", gdje pojedinci poduzimaju dodatne mjere sigurnosti izvan svojih osnovnih obaveza. Ova ponašanja zajedno jačaju otpornost organizacije na kibernetičke prijetnje.

Cjelokupni model prikazan na slici naglašava važnost integracije vanjskih utjecaja, organizacijskih politika i individualne svijesti u izgradnji snažne sigurnosne kulture, koja na kraju dovodi do ponašanja koja pomažu u zaštiti organizacije od prijetnji. Edukacija korisnika nije samo tehnički zadatak, već proces oblikovanja svjesnog i odgovornog ponašanja unutar digitalnog svijeta. Kada svaki pojedinac postane svjestan svoje uloge u zaštiti informacija, organizacija postaje snažnija u borbi protiv nepredvidivih kibernetičkih prijetnji. Sigurnost je zajednička odgovornost, a bez stalnog ulaganja u znanje, ni najbolji tehnološki alati neće biti dovoljni.

6.3. SIGURNOSNE POLITIKE

Korištenje oblaka postalo je nezaobilazno za organizacije svih veličina. No, s povećanjem migracije podataka i poslovnih operacija u oblak, sigurnosni izazovi su postali složeniji. Sigurnosne politike predstavljaju ključan mehanizam za zaštitu podataka i upravljanje sigurnosnim rizicima u cloud okruženju. Ove politike jasno definiraju pravila o pristupu podacima, njihovoj zaštiti, te načinima na koje se mogu spriječiti neovlašteni upadi ili gubici podataka. Pravilno definirane sigurnosne politike ne samo da pomažu u prevenciji sigurnosnih incidenata, već osiguravaju i usklađenost s regulatornim okvirima, čime jačaju povjerenje korisnika i partnera.

Sigurnosne politike za oblak moraju pokriti različite aspekte kako bi se osigurala potpuna zaštita podataka i usklađenost s regulatornim zahtjevima. Prema Aqua Security, postoji devet ključnih komponenti koje treba obuhvatiti prilikom definiranja sigurnosne politike u oblaku. Prva je upravljanje i usklađenost, koja uključuje definiranje uloga i odgovornosti unutar organizacije, kao i osiguranje usklađenosti s industrijskim standardima i regulatornim propisima. Druga komponenta je procjena i upravljanje rizicima, koja osigurava da organizacija redovito procjenjuje potencijalne prijetnje i ranjivosti te prema tome prilagođava svoje sigurnosne mjere. Treća komponenta odnosi se na sigurnosnu arhitekturu, gdje se opisuje struktura sigurnosnih mjera unutar cloud okruženja, uključujući mrežnu segmentaciju, vatrozide i enkripciju. Četvrta komponenta, upravljanje pristupom i identitetima, odnosi se na implementaciju strogih kontrola pristupa kako bi se spriječio neovlašteni pristup podacima, uz korištenje višefaktorske autentifikacije i upravljanja privilegijama. Šifriranje podataka kao peta komponenta odnosi se na zaštitu podataka u mirovanju i u prijenosu, osiguravajući da čak i u slučaju incidenta, podaci ostanu zaštićeni. Šesta komponenta odnosi se na odgovor na incidente i upravljanje njima, gdje se definiraju jasni postupci za rukovanje sigurnosnim incidentima, uključujući identificiranje, odgovaranje i sanaciju prijetnji. Revizija i praćenje čine sedmu komponentu, osiguravajući da se sve aktivnosti unutar cloud okruženja redovito prate i pregledavaju kako bi se otkrile nepravilnosti i zadržala usklađenost s politikama. Osma komponenta, upravljanje sigurnosnim kontrolama, osigurava implementaciju tehničkih mjera kao što su enkripcija, pristupne liste i mrežna segmentacija. Konačno, deveta komponenta obuhvaća neprestano unapređivanje i prilagodbu sigurnosnih politika prema novim prijetnjama i tehnološkim promjenama, čime organizacija osigurava otpornost svojih cloud operacija na

nove sigurnosne izazove. Time se stvara okvir koji omogućuje organizacijama da stalno poboljšavaju svoje sigurnosne prakse i smanje rizik od sigurnosnih incidenata [41].

Sigurnosne politike nisu samo skup tehničkih pravila već i izraz odgovornosti koju svaka organizacija ima prema svojim podacima, korisnicima i poslovnim partnerima. Kroz jasno definiranje i dosljedno provođenje ovih politika, organizacije stvaraju okruženje u kojem je sigurnost podataka temeljna vrijednost. Sigurnost ne smije biti opcija, već nužnost, koja osigurava dugoročnu stabilnost poslovanja i povjerenje klijenata.

6.4. SIGURNOSNE CERTIFIKACIJE

Današnje kompanije koje koriste infrastrukturu u oblaku suočavaju se s potrebom usklađivanja s nizom sigurnosnih regulativa i standarda. To nije samo zakonska obaveza, već i ključan faktor u izgradnji povjerenja klijenata i partnera. Kako bi zaštitili osjetljive podatke i osigurali stabilno poslovanje, organizacije moraju implementirati najbolje sigurnosne prakse i proći relevantne certifikacije. Usklađenost sa sigurnosnim zahtjevima postala je preduvjet za dugoročnu suradnju, jer korisnici očekuju visoku razinu sigurnosti i transparentnosti.

Sigurnosne certifikacije pružaju ključne okvire za osiguranje pouzdanosti i sigurnosti u oblaku. Jedan od najvažnijih standarda je ISO 27001, koji je dio šire ISO 27000 obitelji standarda i pruža smjernice za uspostavljanje sustava upravljanja informacijskom sigurnošću (ISMS). Ovaj standard pomaže organizacijama da identificiraju sigurnosne rizike i uvedu odgovarajuće kontrole kako bi zaštitili podatke. ISO 27017 i ISO 27018 nadopunjuju ISO 27001 s posebnim fokusom na sigurnost u oblaku, osiguravajući da su podaci pohranjeni u oblaku zaštićeni prema najvišim standardima. Na primjer, ISO 27018 se posebno bavi zaštitom osobnih podataka u oblaku, osiguravajući privatnost i sigurnost podataka korisnika, što je od vitalne važnosti za usklađenost s regulativama poput GDPR-a. GDPR je europska regulativa koja postavlja stroge zahtjeve za zaštitu osobnih podataka. U skladu s GDPR-om, tvrtke moraju osigurati da osobni podaci građana Europske unije budu pravilno zaštićeni, što uključuje transparentno upravljanje podacima, pravo korisnika na brisanje podataka, i obvezu obavještavanja o povredama sigurnosti. Sigurnosne certifikacije također zahtijevaju redovite revizije kako bi se osiguralo da pružatelji usluga u oblaku kontinuirano održavaju najviše standarde sigurnosti. Ove revizije osiguravaju da pružatelji odgovaraju na nove prijetnje i prilagođavaju svoje mjere kako bi zadržali status certifikacije [42].

Sigurnosne certifikacije nisu „samo“ formalne akreditacije, već predstavljaju ključan dokaz odgovornosti i predanosti pružatelja usluga visokim sigurnosnim standardima. One odražavaju kontinuiranu usklađenost s najboljim praksama u industriji, te služe kao jamstvo korisnicima i poslovnim partnerima da se njihove podatke i sustave štiti na najvišoj razini. Kroz proces certificiranja i redovite revizije, pružatelji usluga omogućuju sigurnije i pouzdanije digitalno okruženje za sve sudionike.

7. ZAKLJUČAK

U ovom radu objašnjena je rastuća važnost i složenost računarstva u oblaku, s posebnim naglaskom na sigurnosne prijetnje, rizike i mehanizme zaštite. Računarstvo u oblaku postalo je nezaobilazno u suvremenom poslovanju i privatnom životu, pružajući brojne prednosti kao što su fleksibilnost, skalabilnost i ekonomičnost. Međutim, uz ove prednosti, dolazi i niz sigurnosnih izazova koji ugrožavaju povjerljivost, integritet i dostupnost podataka.

Kroz proučavanje sigurnosnih prijetnji, poput neovlaštenog pristupa, napada na infrastrukturu i ranjivosti servisa, jasno je da oblak nije imun na sigurnosne rizike. Sve sofisticiraniji napadi i evolucija prijetnji ukazuju na potrebu za naprednijim i proaktivnim sigurnosnim mjerama. Uvođenje mehanizama zaštite, poput enkripcije podataka, autentifikacije, pentestinga te primjene principa poput načela najmanjih privilegija, pokazalo se ključnim za zaštitu resursa u oblaku.

Ova saznanja naglašavaju i važnost podijeljene odgovornosti između korisnika i pružatelja usluga oblaka, kao i potrebu za usklađivanjem sa sigurnosnim standardima i certifikacijama. Iako tehnologija pruža moćne alate za sigurnost, ljudska komponenta ostaje jednako važna. Kontinuirana edukacija korisnika i svijest o prijetnjama neophodni su za učinkovitu zaštitu u oblaku.

S obzirom na stalnu evoluciju prijetnji, organizacije moraju primijeniti sveobuhvatan pristup sigurnosti koji kombinira tehnološka rješenja, obuku i svijest o sigurnosti. Samo takvim cjelovitim pristupom mogu se učinkovito zaštititi od rastućih prijetnji te iskoristiti prednosti računarstva u oblaku na siguran i odgovoran način.

8. LITERATURA

[1] S. Susnjara i I. Smalley, »What is cloud computing?: IBM,« IBM, 14. 2. 2024.. [Mrežno]. Available: https://www.ibm.com/topics/cloud-computing. [Pristupljeno 2. 7. 2024.].

[2] Javatpoint, »Cloud computing architecture: Javatpoint,« Javatpoint, [Mrežno]. Available: https://www.javatpoint.com/cloud-computing-architecture. [Pristupljeno 3. 7. 2024.].

[3] Swati I. Bairagi, Ankur O. Bang , »Cloud Computing: History, Architecture, Security,« *International Journal of Advent Research in Computer and Electronics (IJARCE)* , p. 7, 2015.

[4] P. A. A. H. A. A.-A. ,. P. D. S. J. Fursan Thabita, »Exploration of Security Challenges in Cloud Computing: Issues,,« *Journal of Information and Computational Science,* svez. 10, br. 12, p. 23, 2020.

[5] V. V. Arutyunov, »Cloud Computing: Its History of Development, Modern State,,« svez. 39, br. 3, pp. 173-178, 2012.

[6] T. Kajiyama, Cloud computing security: How risks and threats are affecting cloud adoption decisions, San Diego: San Diego State University, 2012.

[7] L. J. S. J. Sushil Bhardwaj, »Cloud computing: A study of infrastructure as a service (IAAS),« *International Journal of Engineering and Information Technology* , svez. 2, br. 1, pp. 60-63, 2010.

[8] Redhat, »Redhat: Topics - Understanding cloud computing: What is IAAS?,« Redhat, 22. 6. 2022.. [Mrežno]. Available: https://www.redhat.com/en/topics/cloud-computing/what-is-iaas#kinds-of-%E2%80%9Cas-a-service%E2%80%9D-offerings. [Pristupljeno 7. 7. 2024.].

[9] IBM, »IBM Topics - What is Paas (Platform-as-a-Service)?,« IBM, [Mrežno]. Available: https://www.ibm.com/topics/paas. [Pristupljeno 9. 7. 2024.].

[10] Google, »Learn: What is Platform as a service(PaaS)?,« Google, [Mrežno]. Available: https://cloud.google.com/learn/what-is-paas?hl=en. [Pristupljeno 9. 7. 2024.].

[11] IBM, »IBM Topics: Understanding cloud computing: What is Saas?,« IBM, 3. 25. 2022.. [Mrežno]. Available: https://www.redhat.com/en/topics/cloud-computing/what-is-saas. [Pristupljeno 9. 7. 2024.].

[12] V. P. T. a. D. P. Aithal, »Cloud computing security issues - challenges and opportunities,« *International Journal of Management, Technology and Social sciences,* svez. 1, br. 1, pp. 33-42, 2017..

[13] O'Reilly, Chris Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly Media , 2023.

[14] T. I. a. D. Manivannan, »A Classification and Characterization of Security Threats in Cloud Computing,« *College of Communication and Information, University of Kentucky*, March 2016.

[15] H. W. Security, »Threat Insights Report,« HP, 2024.

[16] R. A. M. M. H. A. M. T. A. N. A. Umer Ahmed Butt, »Cloud Security Threats and Solutions: A Survey,« *Springer Science+Business Media, LLC, part of Springer Nature,* 28 August 2022.

[17] E. A. F. L. G. B. S. Maniah, »Survey on Threats and Risks in the Cloud Computing Environment,« *The Fifth Information Systems International Conference 2019* , 2019.

[18] Fortinet, »Global Threat Landscape Report - A Semiannual Report by FortiGuard Labs,« Fortinet, 2023.

[19] R. A. M. F. D. o. C. N. a. C. (. K. F. U. A. H. 3. S. A. Alanoud Alquwayzani, »Prominent Security Vulnerabilities in Cloud,« *(IJACSA) International Journal of Advanced Computer Science and Applications,* svez. 15, br. 2, 2024.

[20] M. I. F. A. K. Gururaj Ramachandra, »A Comprehensive Survey on Security in Cloud Computing,« *The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017),* 2017.

[21] D. M. W. Allan A. Friedman, »Privacy and Security in Cloud Computing,« *Center for Technology Innovation at Brookings,* October 2010.

[22] A. A.-Y. Nabeel Khan, »Identifying Cloud Security Threats to Strengthen Cloud Computing,« *The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies* , 2016.

[23] S. Khan, »Cloud Computing: Issues and risks of Embracing the Cloud in a Business Environment,« *International Journal of Education and Management Engineering* , pp. 44-56, 8 7 2019.

[24] D. N. R. Moşteanu, »MANAGEMENT OF DISASTER AND BUSINESS CONTINUITY IN A DIGITAL WORLD,« *International Journal of Management* , pp. 169-177, 4 4 2020.

[25] Y. D. T. Z. J. F. Jianhua Che, »Study on the security models and strategies of cloud computing,« *2011 International Conference on Power Electronics and Engineering Application* , pp. 586-593, 2011.

[26] A. W. Services, »AWS Security Incident Response Guide, AWS Technical Guide,« Amazon Web Services, [Mrežno]. Available: https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/introduction.html. [Pristupljeno 10 8 2024].

[27] T. M. T. K. S. Paul Cichonski, »Computer Security Incident Handling Guide,« National Institute of Standards and Technology, 2012.

[28] DartPoints, »Public, Private, and Hybrid Cloud Computing – What You Need to Know: DartPoints,« DartPoints, [Mrežno]. Available: https://dartpoints.com/public-private-and-hybrid-cloud-computing-what-you-need-to-know/. [Pristupljeno 01. 09. 2024.].

[29] S. K. S. L. Tim Mather, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, Sebastopol: O'Reilly Media Inc., 2009.

[30] Exabeam, »Cloud Security: Exabeam,« Exabeam, [Mrežno]. Available: https://www.exabeam.com/explainers/cloud-security/cloud-security-principles-solutions-and-architectures/. [Pristupljeno 11. 8. 2024].

[31] J. A. F. G. A. L. D. M. G. P. M. R. Rich Mogull, Security Guidance For Critical Areas of Focus In Cloud Computing v4.0, Cloud Security Alliance, 2017.

[32] Fortinet, »Cia Triad: Fortinet,« Fortinet, [Mrežno]. Available: https://www.fortinet.com/resources/cyberglossary/cia-triad. [Pristupljeno 11. 8. 2024].

[33] Cloudflare, »What is penetration testing : Cloudflare,« Cloudflare, [Mrežno]. Available: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/. [Pristupljeno 11. 8. 2024].

[34] N. C. S. K. P. J. Vijaya Chandra, »Authentication and Authorization Mechanism for Cloud Security,« *International Journal of Engineering and Advanced Technology (IJEAT),* August 2019.

[35] NIST, »Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,« NIST, 2020.

[36] Crowdstrike, »What is Cloud Encryption? Crowdstrik,« Crowdstrike, [Mrežno]. Available: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-encryption/. [Pristupljeno 11. 8. 2024.].

[37] OWASP, »OWASP,« OWASP, 2021. [Mrežno]. Available: https://owasp.org/Top10/. [Pristupljeno 18. 09. 2024.].

[38] Crowdstrike, »Cloud Security - Shared Resposibility Model - Crowdstike,« Crowdstrike, 14. 11. 2022.. [Mrežno]. Available: 2024.. [Pristupljeno 18. 09. 2024.].

[39] A. W. Services, »What is Service Level Agreement: Amazon Web Services,« Amazon Web Services, [Mrežno]. Available: https://aws.amazon.com/what-is/service-level-agreement/. [Pristupljeno 19. 09. 2024.].

[40] Lumifi, »Why user education is important in cybersecurity resiliance: Lumifi,« Lumifi, 19. 12. 2020.. [Mrežno]. Available: https://www.lumificyber.com/blog/why-user-education-is-important-cybersecurity-resilience/. [Pristupljeno 19. 09. 2024.].

[41] Aqua, »9 Key Components of a Cloud Security Policy: Aqua,« Aqua, 23. 07. 2023.. [Mrežno]. Available: https://www.aquasec.com/cloud-native-academy/cspm/cloud-security-policy/. [Pristupljeno 19. 09. 2024.].

[42] Crowdstrike, »A Starter Guide to Cloud Compliance: Crowdstrike,« Crowdstrike, 10. 07. 2024.. [Mrežno]. Available: https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-compliance/. [Pristupljeno 19. 09. 2024.].

10. POPIS SLIKA

SECURITY THREATS AND RISKS OF CLOUD COMPUTING

SUMMARY

Cloud computing has become an indispensable tool in today's digital environment, offering flexibility and scalability in the use of computing resources. However, alongside its numerous advantages, various security challenges such as unauthorized access, data breaches, and attacks on infrastructure have emerged. Utilizing models like IaaS, PaaS, and SaaS, as well as different deployment types, requires active involvement from both users and service providers in maintaining security. The implementation of protection mechanisms such as encryption, authentication, and the principle of least privilege, along with continuous education and awareness of potential threats, is crucial for the secure use of cloud services. In conclusion, effective data protection in the cloud requires comprehensive and proactive security strategies that involve continuous risk assessment and monitoring. Through ongoing threat monitoring, adaptation of security measures, and alignment with security standards, users and organizations can achieve a high level of data protection. This enables the full utilization of cloud computing advantages, ensuring a reliable environment for data storage and processing.

Keywords: cloud computing, security, threats, data protection, security mechanisms