Sigurnosna pohrana podataka u oblaku

Bućaj, Emanuel

Sveučilište Sjever

Računarstvo i informatika

Zavrsni rad br. 8/RINF/2024

Sigurnosna pohrana podataka u oblaku

Student

Emanuel Bućaj, 033605104

Mentor

dr.sc. Dražen Lučić

Đurđevac, kolovoz 2024. godine

Sveučilište Sjever
Sveučilišni centar Koprivnica
Trg dr. Žarka Dolinara 1, HR-48000 Koprivnica

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL Računarstvo i informatika

STUDIJ stručni prijediplomski studij računarstva i informatike

PRISTUPNIK Emanuel Bučaj | MATIČNI BROJ 0336051504

DATUM 13.09.2024. | KOLEGIJ Računalstvo u oblaku

NASLOV RADA Sigurnosna pohrana podataka u oblaku

NASLOV RADA NA ENGL. JEZIKU Data Backup in Cloud

MENTOR dr.sc. Dražen Lučić | ZVANJE predavač

ČLANOVI POVJERENSTVA
1. dr.sc. Mario Weber
2. mag.el. Josip Jozić
3. dr.sc. Dražen Lučić
4. doc.dr.sc. Domagoj Frank
5.

Zadatak završnog rada

BROJ 8/RINF/2024

OPIS

U digitalnom dobu podaci su jedan od ključnih elemenata suvremenog poslovanja. S porastom količine podataka i potrebom za njihovom sigurnom pohranom i obradom, pohrana podataka u oblaku postala je neizostavna tehnologija za mnoge organizacije diljem svijeta. Ova tehnologija omogućuje korisnicima da pohranjuju, upravljaju i pristupaju podacima udaljenim pristupom, bez potrebe za cjelokupnom vlastitom infrastrukturom, što donosi brojne prednosti poput skalabilnosti, fleksibilnosti i globalne dostupnosti.

Uz sve prednosti, pohrana podataka u oblaku također donosi niz izazova, posebno u području sigurnosti podataka. Sigurnost ostaje primarni izazov, s potrebom za zaštitom osjetljivih podataka od neovlaštenog pristupa, gubitka ili krađe. Stoga je ključno razumjeti različite aspekte pohrane podataka u oblaku, uključujući vrste oblaka, tehnologije, prednosti i izazove, kako bi se osiguralo uspješno i sigurno korištenje ove tehnologije u suvremenom poslovnom okruženju.

U radu će biti dan pregled rješenja za sigurnosnu pohranu podataka, s naglaskom na ono u oblaku. Raščlamba jednog takvog rješenja daje pregled prednosti i nedostataka sigurnosne pohrane podataka u oblaku. Praktična primjena tog rješenja je prikazana na primjeru jedne institucije, pravnog tijela s javni ovlastima, u Republici Hrvatskoj, kojoj je sigurnosna pohrana podataka u oblaku jedan od zaloga brzog i uspješnog nastavka poslovanja u slučaju kibernetičkog incidenta ili katastrofe.

ZADATAK URUČEN 13.09.2024. | POTPIS MENTORA

SVEUČILIŠTE SJEVER

Sažetak

Sigurnosna pohrana podataka u oblaku postala je jedna od ključnih tema u informacijsko-komunikacijskoj tehnologiji zbog sve veće primjene rješenja u oblaku u poslovanju. Ovaj rad analizira ključne aspekte i trendove u sigurnosnoj pohrani podataka u oblaku, fokusirajući se na tehnologije, alate i metode koje osiguravaju zaštitu podataka u okviru rješenja u oblaku. U uvodnom dijelu rada objašnjeni su temeljni koncepti oblaka, uključujući različite modele usluga (IaaS, PaaS, SaaS) i vrste oblaka (javne, privatne i hibridne).

Nadalje, rad analizira sigurnosne prijetnje i rizike specifične za okvir rješenja u oblaku, uključujući vanjske napade, tehničke kvarove i unutarnje prijetnje. Razmatrani su izazovi u osiguravanju podataka, kao i metode za ublažavanje sigurnosti podataka, poput šifriranja, upravljanja identitetom i pristupom, te sigurnosnog kopiranja. Suvremeni alati i tehnologije, uključujući kvantnu kriptografiju, napredne metode šifriranja i integraciju umjetne inteligencije, detaljno su opisani kako bi se prikazali načini na koje organizacije mogu poboljšati sigurnost svojih podataka.

Posebna pažnja posvećena je budućim trendovima u sigurnosnoj pohrani podataka u oblaku. Razmatra se razvoj kvantne kriptografije koja pruža otpornost na kvantna računala, kao i napredne metode šifriranja koje omogućuju obradu podataka bez njihovog dešifriranja. Integracija umjetne inteligencije i strojnog učenja omogućava brže prepoznavanje prijetnji, automatizirano upravljanje sigurnosnim incidentima i prediktivnu analitiku. Također, rad se bavi razvojem sigurnosnih politika i regulativa koje zahtijevaju usklađenost s novim standardima i zakonodavnim okvirima.

Konačno, rad naglašava važnost holističkog pristupa sigurnosti u oblaku, uključujući kontinuiranu evaluaciju i prilagodbu sigurnosnih politika, proaktivno praćenje mrežnih aktivnosti i obuku zaposlenika. Organizacije koje prihvate ove mjere bit će bolje pripremljene za suočavanje s budućim sigurnosnim izazovima i osiguranje dugoročne zaštite svojih podataka.

Summary

Data security in cloud storage has become one of the key topics in information and communication technology due to the increasing use of cloud solutions in business operations. This paper analyzes the key aspects and trends in cloud data security, focusing on technologies, tools, and methods that ensure data protection within cloud solutions. The introductory section explains the fundamental concepts of the cloud, including different service models (IaaS, PaaS, SaaS) and cloud types (public, private, and hybrid).

Furthermore, the paper examines security threats and risks specific to cloud solutions, including external attacks, technical failures, and insider threats. Challenges in securing data are discussed, along with methods for mitigating security risks, such as encryption, identity and access management, and data backups. Modern tools and technologies, including quantum cryptography, advanced encryption methods, and the integration of artificial intelligence, are detailed to illustrate how organizations can enhance their data security.

Special attention is given to future trends in cloud data security. The paper considers the development of quantum cryptography, which offers resistance to quantum computers, as well as advanced encryption methods that allow data processing without decryption. The integration of artificial intelligence and machine learning enables faster threat detection, automated security incident management, and predictive analytics. Additionally, the paper addresses the development of security policies and regulations that require compliance with new standards and legislative frameworks.

Finally, the paper emphasizes the importance of a holistic approach to cloud security, including continuous evaluation and adaptation of security policies, proactive monitoring of network activities, and employee training. Organizations that adopt these measures will be better prepared to face future security challenges and ensure the long-term protection of their data.

Popis ključnih riječi

Sigurnosna pohrana podataka: Praksa zaštite podataka od neovlaštenog pristupa, gubitka ili kompromitacije, posebno u oblačnim okruženjima.

Računalstvo u oblaku: Distribuirana mreža poslužitelja koja pruža računalne resurse i usluge putem interneta.

Hibridni oblaci: Kombinacija privatnih i javnih oblaka koja omogućuje organizacijama da koriste oba modela prema svojim potrebama.

Multicloud: Pristup korištenju više različitih pružatelja oblačnih usluga za optimizaciju performansi, sigurnosti i troškova.

Šifriranje podataka: Proces pretvaranja podataka u nečitljiv oblik kako bi se zaštitila njihova povjerljivost tijekom pohrane ili prijenosa.

Rješenje za oporavak od katastrofe odnosi se na planirane i organizirane postupke koje organizacije implementiraju kako bi brzo obnovile svoje IT sustave, podatke i poslovne operacije nakon neočekivanih katastrofalnih događaja. Ova rješenja uključuju upotrebu sigurnosnih kopija, redundancije sistema, replikacije podataka, i drugih tehnologija kako bi se osigurala kontinuitet poslovanja i minimalizirali gubici.

Strojno učenje: Podskup umjetne inteligencije koji omogućuje računalima da poboljšaju svoje performanse analizom i učenjem iz podataka bez eksplicitnog programiranja.

Sigurnosne prijetnje: Potencijalne opasnosti koje mogu ugroziti povjerljivost, integritet ili dostupnost podataka, poput kibernetičkih napada virusa ili unutarnjih prijetnji.

Regulativa: Skup zakona i standarda koji reguliraju način na koji organizacije upravljaju i štite podatke, posebno u kontekstu privatnosti i sigurnosti

Backup (sigurnosna kopija) predstavlja postupak izrade duplikata podataka ili sistema kako bi se osigurala njihova dostupnost u slučaju gubitka, oštećenja, ili katastrofalnog događaja. Sigurnosne kopije su ključni element strategije oporavka od katastrofe, jer omogućuju povratak na prethodno stanje i zaštitu od trajnog gubitka podataka.

Keywords List

Data Security in Cloud Storage: The practice of protecting data from unauthorized access, loss, or compromise, particularly in cloud environments.

Cloud Computing: A distributed network of servers providing computing resources and services over the internet.

Hybrid Clouds: A combination of private and public clouds that allows organizations to use both models according to their needs.

Multicloud: An approach involving the use of multiple cloud service providers to optimize performance, security, and costs.

Data Encryption: The process of converting data into an unreadable format to protect its confidentiality during storage or transmission.

Disaster Recovery Solution: Planned and organized procedures implemented by organizations to quickly restore their IT systems, data, and business operations after unexpected catastrophic events. These solutions include the use of backups, system redundancy, data replication, and other technologies to ensure business continuity and minimize losses.

Machine Learning: A subset of artificial intelligence that enables computers to improve their performance by analyzing and learning from data without explicit programming.

Security Threats: Potential dangers that may compromise the confidentiality, integrity, or availability of data, such as cyber-attacks, viruses, or insider threats.

Regulation: A set of laws and standards that govern how organizations manage and protect data, particularly in the context of privacy and security.

Backup: The process of creating a duplicate of data or systems to ensure their availability in case of loss, damage, or a catastrophic event. Backups are a key element of a disaster recovery strategy, as they allow recovery to a previous state and protect against permanent data loss.

1. Sadržaj

Sažetak 1

Popis ključnih riječi 2

1.Tablica sadržaja 3

1.Uvod 5

2.Računalstvo u oblaku 7

2.1.Tipovi oblaka 8
2.2.Osnove usluge oblaka 8
2.3.Prednosti i izazovi korištenja oblaka 9

3.Sigurnosni segmenti pohrane podataka u oblaku 11

3.1.Prijetnje i rizici 11
3.2.Sigurnosne mjere 12
3.3.Tehnološka rješenja 13

4.Pravni okviri 15

4.1.Lokalni zakoni 17
4.2.Implementacija pravnih zahtjeva 19
4.3.Izazovi koji dolaze s lokalnim zakonima i implementacijom 20

5.Suvremeni alati i tehnologije za sigurnost podataka 21

5.1.Alati za šifriranje 21
5.2.Upravljanje identitetom 22
5.3.Alati za oporavak i kopiranje 23
5.4.Alati za praćenje 24
5.5.Alati za zaštitu DDos napada 25
5.6.Tehnologija za sigurnost privatnosti osobnih podataka 26

6.Razvoj novih tehnologija za zaštitu podataka 27

6.1.Umjetna inteligencija i strojno učenje 28
6.2.Razvoj sigurnosnih politika 29
6.3.Razvoj tehnologija za privatnost osobnih podataka 30

7.Konkretan primjer napada na sustav 31

7.1.Specifikacija zahtjeva 31
7.2.Mreža povezanosti 33
7.3.Popis poslužitelja koji se trebaju replicirati 34
7.4.Managed Hosted server – samouslužna infrakstruktura 35

8.Zaključak 36

9.Literatura 38

1. Uvod

U današnje digitalno doba, rapidni razvoj tehnologije i sveobuhvatna digitalizacija poslovanja dovele su do sve veće važnosti računalstva u oblaku (Cloud computing). Oblak je postao ključna komponenta moderne informacijske infrastrukture, omogućujući organizacijama svih veličina da optimiziraju svoje operacije, smanje troškove i povećaju fleksibilnost i skalabilnost svojih IT resursa. Međutim, s povećanjem korištenja oblaka, raste i potreba za osiguravanjem sigurnosti pohranjenih podataka.

Kao student zainteresiran za informacijske-komunikacijske tehnologije i njihovu primjenu u poslovnom okruženju, odlučio sam se istražiti temu sigurnosne pohrane podataka u oblaku. Svakodnevno smo svjedoci vijesti o kibernetičkim napadima, gubicima podataka i povredama privatnosti koje mogu imati katastrofalne posljedice za organizacije. Stoga, cilj ovog rada je istražiti koje sigurnosne mjere i prakse su najučinkovitije u zaštiti podataka u oblaku te kako organizacije mogu implementirati ove mjere kako bi osigurale integritet, povjerljivost i dostupnost svojih podataka.

Cilj ovog završnog rada je analizirati sigurnosne aspekte pohrane podataka u oblaku, identificirati glavne prijetnje i rizike, te istražiti najvažnije sigurnosne mjere i najbolje prakse koje se koriste za zaštitu podataka. Također, želi razumjeti pravne i regulatorne okvire koji definiraju obveze organizacija u vezi sa zaštitom podataka, te pregledati najnovije tehnologije i alate koji se koriste za osiguranje sigurnosti podataka.

U prvom dijelu rada obrađeni su osnovni pojmovi i koncepti vezani za računalstvo u oblaku, uključujući različite tipove oblaka kao što su javni, privatni i hibridni oblak, te osnovne usluge koje oblak nudi (infrastruktura kao usluga-IaaS, platforma kao usluga-PaaS, softver kao usluga-SaaS). Ovaj dio rada pružit će temeljno razumijevanje oblaka, što je ključno za daljnje istraživanje sigurnosnih aspekata.

Drugi dio rada je posvećen analizi sigurnosnih prijetnji i rizika. Istraživat će glavne prijetnje kao što su gubitak podataka, neovlašteni pristup, DDoS (Distributed Denial of Service – distribuirano uskraćivanje usluge) napadi i unutarnje prijetnje. Cilj je razumjeti kako ove prijetnje mogu ugroziti podatke pohranjene u oblaku i koje posljedice mogu imati za organizacije.

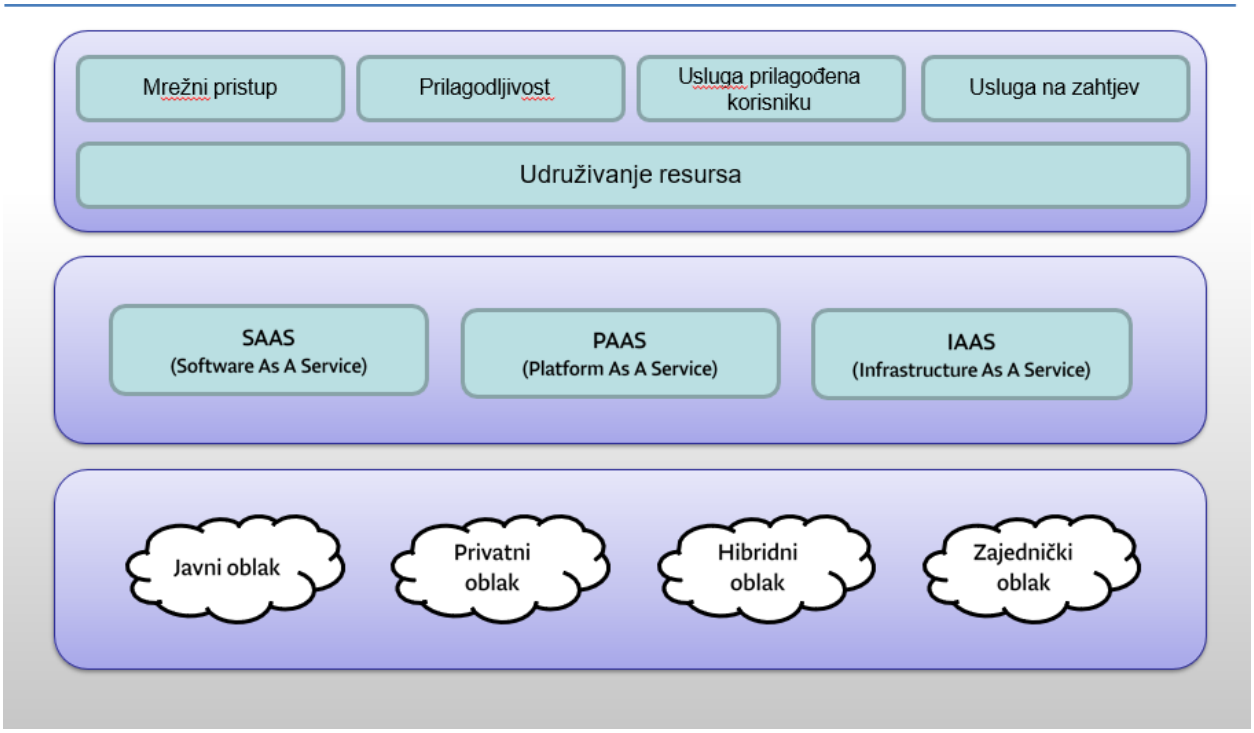
U trećem dijelu rada fokusira se na sigurnosne mjere i najbolje prakse, obrađujući tehnike šifriranja podataka, upravljanje pristupom i autentifikacijom, te pohranu podataka i planove za oporavak u slučaju katastrofe. Istražuje kako te mjere mogu pomoći organizacijama u zaštiti podataka i smanjenju rizika od gubitka podataka ili prekida rada mreže uslijed kibernetičkih napada.

Četvrti dio rada je posvećen pravnim i regulatornim okvirima. Istražit ću međunarodne regulative kao što su GDPR i HIPAA, te lokalne zakone i regulative koje se primjenjuju u našoj zemlji. Razumijevanje ovih okvira ključno je za osiguranje usklađenosti i izbjegavanje pravnih posljedica.

U završnom dijelu rada analizirat ću suvremene alate i tehnologije za sigurnosnu pohranu podataka, kao što su AWS Security, Microsoft Azure Security i Google Cloud Security. Također, istražit ću buduće trendove u ovom području, uključujući primjenu umjetne inteligencije i strojnog učenja u sigurnosti, te kvantno šifriranje.

2. Računalstvo u oblaku

Računalstvo u oblaku predstavlja model isporuke IT usluga putem interneta. Umjesto tradicionalnog modela u kojem korisnici posjeduju i održavaju vlastite fizičke servere i infrastrukturu, računalstvo u oblaku omogućuje pristup računalnim resursima kao što su poslužitelji, pohrana podataka i aplikacije putem interneta, često na temelju modela plaćanja prema korištenju. Ovaj pristup nudi mnoge prednosti uključujući skalabilnost, fleksibilnost i smanjenje operativnih troškova.[1]



Slika 1. Koncept računalstva u „oblaku“

2.1. Tipovi oblaka

Računalstvo u oblaku može se podijeliti na nekoliko glavnih tipova, ovisno o načinu implementacije i dostupnosti resursa:

- Javni oblak (Public Cloud): U javnom oblaku, usluge se pružaju putem interneta od strane trećih strana pružatelja usluga oblaka. Resursi se dijele među različitim korisnicima, a primjer ovakvih pružatelja usluga su Amazon Web Services (AWS), Microsoft Azure i Google Cloud Platform (GCP).[2]

- Privatni oblak (Private Cloud): Privatni oblak namijenjen je korištenju unutar jedne organizacije. Resursi nisu dijeljeni s drugim organizacijama, što omogućuje veću kontrolu nad sigurnošću i privatnošću podataka. Privatni oblaci mogu biti implementirani lokalno na vlastitoj infrastrukturi organizacije ili putem vanjskih pružatelja usluga.

- Hibridni oblak (Hybrid Cloud): Hibridni oblak kombinira elemente javnog i privatnog oblaka, omogućujući organizacijama da koriste prednosti oba pristupa. Na primjer, organizacija može koristiti privatni oblak za osjetljive podatke i aplikacije, dok za manje kritične resurse koristi javni oblak.[3]

2.2. Osnove usluge oblaka

Računalstvo u oblaku nudi različite vrste usluga koje se često klasificiraju prema modelu isporuke:

- Infrastruktura kao usluga (IaaS): IaaS pruža osnovne računalne resurse poput virtualnih mašina, skladištenja i mrežnih resursa. Korisnici imaju kontrolu nad operativnim sustavima i aplikacijama, dok pružatelj usluge upravlja infrastrukturom. Primjeri IaaS pružatelja su AWS EC2, Google Compute Engine i Microsoft Azure VMs.

- Platforma kao usluga (PaaS): PaaS pruža okruženje za razvoj, testiranje i implementaciju aplikacija bez potrebe za upravljanjem osnovnom infrastrukturom. Pruža razvojne alate, baze podataka i middleware. Primjeri PaaS pružatelja su Google App Engine, Microsoft Azure App Services i Heroku.[3]

- Softver kao usluga (SaaS): SaaS omogućuje korisnicima pristup softverskim aplikacijama putem interneta. Pružatelji usluga upravljaju aplikacijama i infrastrukturom, a korisnici plaćaju pretplatu za korištenje aplikacija. Primjeri SaaS aplikacija su Google Workspace, Microsoft Office 365 i Salesforce.

	VLASTITA MREŽNA INFRASTRUKTURA	INFRASTRUKTURA U „OBLAKU"
SIGURNOST	IKT odjel vlasnika mreže odgovoran za sigurnost svih podataka i aktivnosti u mreži	Pružatelj usluge rukovodi tehničkom administracijom sigurnosti i nudi alate za upravljanje ranjivošću
POUZDANOST	Kvarovi u najslabijim točkama i prirodna katastrofa može cijelu prekinuti rad cijele mreže	Dodana zalihnost pojedinih elemenata mreže i raspodijeljeni sustavi na različitim lokacijama
TROŠKOVI	Početno ulaganje za sklopovlje i programsku podršku, troškovi povećanja kapaciteta, nadogradnje i održavanja	Plaćanje samo za ono što se koristi, uz opasnost da se zbog korisnikove krive procjene potreba plate kapaciteti i usluge koje se ne koriste
STRUČNOST	Znatna ulaganja u stručno osoblje i daljnju izobrazbu	Samo vještine potrebne za korištenja usluga u „oblaku"

Slika 2. Razlika infrastrukture vlastite mreže i u oblaku

2.3. Prednosti i izazovi korištenja oblaka

Prednosti

Računalstvo u oblaku nudi brojne prednosti koje ga čine atraktivnim za organizacije:

- Skalabilnost: Oblak omogućuje brzo prilagođavanje kapaciteta prema potrebama korisnika, bez potrebe za velikim početnim ulaganjima u hardver.

- Fleksibilnost: Korisnici mogu pristupiti resursima i aplikacijama s bilo koje lokacije putem interneta.

- Troškovna učinkovitost: Plaćanje prema korištenju omogućuje organizacijama da optimiziraju troškove i izbjegnu nepotrebna ulaganja u vlastitu infrastrukturu.
- Brza implementacija: Resursi u oblaku mogu se brzo implementirati i konfigurirati, što skraćuje vrijeme potrebno za postavljanje novih projekata i aplikacija.[4]
- Održavanje i ažuriranja: Pružatelji usluga oblaka brinu se o održavanju infrastrukture i redovitim ažuriranjima, što omogućuje korisnicima da se fokusiraju na svoje poslovne ciljeve

Izazovi

Unatoč brojnim prednostima, korištenje oblaka donosi i određene izazove koje organizacije moraju uzeti u obzir:

- Sigurnost: Sigurnost podataka u oblaku jedan je od glavnih izazova. Organizacije moraju osigurati da su njihovi podaci zaštićeni od neovlaštenog pristupa i cyber napada.
- Privatnost: Pohrana podataka kod trećih strana može predstavljati izazove vezane uz privatnost i usklađenost s regulativama.
- Regulative: Različite zemlje i industrije imaju specifične regulative vezane uz pohranu i zaštitu podataka, što može otežati globalno korištenje oblaka.
- Ovisnost o pružatelju usluga (vendor lock-in): Korištenje specifičnih usluga pružatelja oblaka može otežati prelazak na drugog pružatelja usluga ili povratak na vlastitu infrastrukturu.
- Performanse: Performanse aplikacija mogu varirati ovisno o mrežnoj povezivosti i kapacitetima pružatelja usluga.[4]

Pregled tehnologije oblaka pruža osnovu za razumijevanje kako računalstvo u oblaku funkcionira, te koje su njegove prednosti i izazovi. U narednim poglavljima istražit ćemo sigurnosne aspekte pohrane podataka u oblaku, uključujući glavne prijetnje, rizike i sigurnosne mjere koje se koriste za zaštitu podataka.

3. Sigurnosni segmenti pohrane podataka u oblaku

Sigurnosni segmenti pohrane podataka u oblaku uključuju šifriranje podataka, upravljanje identitetom i pristupom, sigurnosno kopiranje i oporavak, te kontinuirano praćenje i otkrivanje prijetnji. Ovi elementi zajedno osiguravaju zaštitu podataka od neovlaštenog pristupa, gubitka i kibernetičkih napada napada u oblačnim okruženjima.[5]

3.1. Prijetnje i rizici

Gubitak podataka

Gubitak podataka može nastati uslijed različitih razloga, uključujući tehničke kvarove, ljudske pogreške, zlonamjerne aktivnosti ili prirodne katastrofe. Podaci u oblaku mogu biti izgubljeni zbog nedovoljno pouzdanih mehanizama za sigurnosno kopiranje ili zbog nedostupnosti usluga pružatelja oblaka.

Neovlašteni pristup

Neovlašteni pristup podacima jedan je od najvažnijih sigurnosnih izazova u oblaku. Napadači mogu pokušati dobiti pristup podacima putem krađe identiteta, slabe autentifikacije ili iskorištavanjem ranjivosti u sustavu.[4]

DDoS napadi

Distributed Denial of Service (DDoS) napadi mogu ugroziti dostupnost usluga u oblaku preopterećenjem resursa. Ovi napadi mogu uzrokovati privremenu nedostupnost podataka i aplikacija, što može imati ozbiljne posljedice za poslovanje organizacija.

Unutarnje prijetnje

Unutarnje prijetnje dolaze od zaposlenika ili suradnika koji imaju pristup podacima i mogu ih zloupotrijebiti. Ovo može uključivati krađu podataka, namjerno oštećenje podataka ili slučajnu pogrešku koja dovodi do gubitka podataka.[5]

Zlonamjerni softver (malware)

Zlonamjerni softver može inficirati sustave u oblaku i ugroziti sigurnost podataka. To uključuje viruse, crve, ransomware i druge oblike malwarea koji mogu oštetiti ili ukrasti podatke.

3.2. Sigurnosne mjere

Šifriranje podataka (u prijenosu i u mirovanju)

Šifriranje je ključna mjera zaštite podataka. Podaci u oblaku trebaju biti šifrirani kako u prijenosu (dok putuju mrežom) tako i u mirovanju (dok su pohranjeni). Korištenje jakih enkripcijskih algoritama osigurava da podaci budu nečitljivi neovlaštenim osobama.

Upravljanje pristupom i autentifikacija

1. Dvofaktorska autentifikacija (2FA): Korištenje 2FA povećava sigurnost pristupa podacima zahtijevajući dodatni korak verifikacije, poput jednokratne lozinke (OTP) poslane na mobilni uređaj.
2. Upravljanje identitetom i pristupom (IAM): IAM sustavi omogućuju kontrolu i nadzor nad pristupom korisnika i uređaja do resursa u oblaku. Ovo uključuje definiranje uloga i prava pristupa kako bi se osiguralo da samo ovlaštene osobe imaju pristup određenim podacima.

Planovi sigurnosnog kopiranja i oporavka od katastrofe (Backup i disaster recovery planovi)

Redovito sigurnosno kopiranje podataka i implementacija disaster recovery planova ključni su za minimiziranje gubitaka podataka. Organizacije trebaju osigurati da imaju adekvatne strategije za povratak podataka u slučaju gubitka ili korupcije.[5]

Praćenje i revizija sustava (monitoring and auditing)

Kontinuirano praćenje i revizija sustava omogućuju otkrivanje neobičnih aktivnosti i potencijalnih sigurnosnih prijetnji. Alati za praćenje mogu identificirati sumnjivo ponašanje, a revizijski zapisi (logovi) pomažu u istraživanju incidenata i usklađenosti s regulativama.[6]

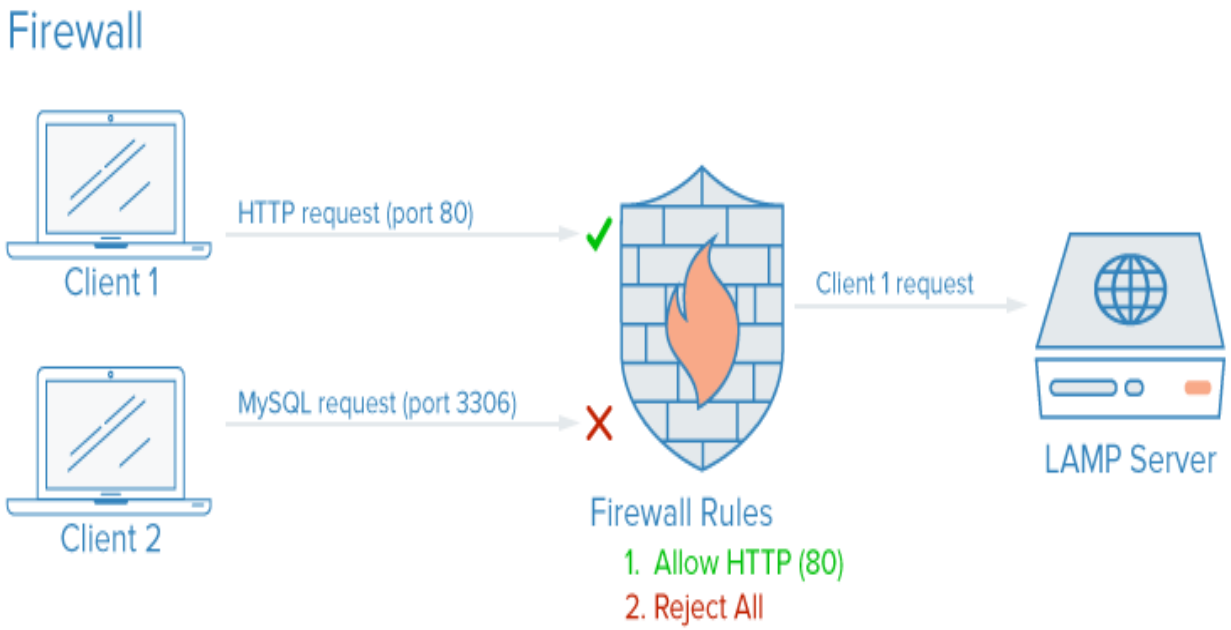
Osvješćivanje zaposlenika o sigurnosti

Edukacija zaposlenika o sigurnosnim prijetnjama i najboljim praksama ključna je za smanjenje rizika od unutarnjih prijetnji. Zaposlenici trebaju biti svjesni važnosti sigurnosti podataka, prepoznavanja „phishing“ napada i pridržavanja sigurnosnih politika organizacije.[6]

3.3. Tehnološka rješenja

Vatrozid i mrežna sigurnost

Vatrozid („Firewall“) i drugi mrežni sigurnosni alati štite infrastrukturu oblaka od neovlaštenih pristupa i cyber napada (slika 3.). Ovi alati omogućuju filtriranje prometa, prepoznavanje napada i blokiranje sumnjivih aktivnosti.[7]



Slika 3. Prikaz vatrozida

Intrusion Detection and Prevention Systems (IDPS)

IDPS sustavi pomažu u prepoznavanju i sprječavanju napada na mrežu i sustave. Oni analiziraju mrežni promet i sustave kako bi identificirali i reagirali na potencijalne sigurnosne prijetnje u stvarnom vremenu.[6]

Security Information and Event Management (SIEM)

SIEM sustavi prikupljaju, analiziraju i koreliraju sigurnosne podatke iz različitih izvora kako bi pružili cjelovit pregled sigurnosnog stanja sustava. SIEM omogućuje brzu identifikaciju i odgovor na sigurnosne incident[8]

Sigurnosni aspekti pohrane podataka u oblaku predstavljaju ključni izazov za organizacije koje koriste oblak. Pravilna implementacija sigurnosnih mjera i najboljih praksi može značajno smanjiti rizike i osigurati zaštitu podataka. U nastavku rada istražit ćemo pravne i regulatorne okvire koji definiraju obveze organizacija u vezi s zaštitom podataka u oblaku.

4. Pravni okviri

Međunarodne regulative

Opća uredba o zaštiti podataka (GDPR):

GDPR (General Data Protection Regulation) je regulativa Europske unije koja je stupila na snagu 25. svibnja 2018. godine. Cilj GDPR-a je osigurati zaštitu osobnih podataka svih građana EU-a i regulirati način na koji organizacije obrađuju te podatke. GDPR se primjenjuje na sve organizacije koje obrađuju podatke građana EU, bez obzira na njihovu lokaciju.[9]

Glavne odredbe GDPR-a uključuju:

- Pravo na pristup: Pojedinci imaju pravo znati koje podatke organizacije prikupljaju o njima i kako se ti podaci obrađuju.
- Pravo na zaborav: Pojedinci mogu zahtijevati brisanje svojih osobnih podataka.
- Prijenos podataka: Pojedinci imaju pravo prenijeti svoje podatke drugom pružatelju usluga.
- Obavijesti o povredi podataka: Organizacije su obvezne obavijestiti nadzorna tijela o povredi podataka unutar 72 sata.
- Upravitelj podataka: Organizacije koje obrađuju osobne podatke moraju imenovati službenika za zaštitu podataka (DPO).

Health Insurance Portability and Accountability Act (HIPAA):

HIPAA je američki zakon koji osigurava zaštitu zdravstvenih informacija pacijenata. HIPAA regulira način na koji zdravstvene organizacije obrađuju, pohranjuju i dijele zdravstvene podatke.[10]

Ključne odredbe HIPAA-e uključuju:

- Pravila o privatnosti: Regulira uporabu i otkrivanje zdravstvenih informacija.
- Pravila sigurnosti: Postavljaju standarde za zaštitu elektroničkih zdravstvenih informacija.

- Pravilo obavijesti o povredi: Zahtijeva obavještavanje pacijenata i nadležnih tijela o povredi podataka.

ISO/IEC 27001

ISO/IEC 27001 je međunarodni standard za upravljanje informacijskom sigurnošću. Ovaj standard pruža okvir za upravljanje rizicima vezanim za sigurnost informacija i uključuje zahtjeve za implementaciju sigurnosnih kontrola. [11]

Ključni elementi ISO/IEC 27001 uključuju:

- Procjena rizika: Identifikacija i procjena rizika vezanih za informacijsku sigurnost.
- Sigurnosne kontrole: Implementacija tehničkih i organizacijskih mjera za zaštitu informacija.
- Kontinuirano poboljšanje: Redovita revizija i poboljšanje sustava upravljanja informacijskom sigurnošću.

ISO 27001:2022

ISO 27001:2022 je međunarodni standard za upravljanje informacijskom sigurnošću, koji pruža okvir za zaštitu povjerljivosti, integriteta i dostupnosti informacija u organizacijama. Ovaj standard omogućuje organizacijama da uspostave, implementiraju, održavaju i neprestano poboljšavaju sustav upravljanja informacijskom sigurnošću (ISMS). Verzija iz 2022. godine donosi ažurirane kontrole sigurnosti kako bi se prilagodila novim prijetnjama i tehnologijama, naglašavajući važnost upravljanja rizicima, usklađenosti s regulativama i zaštite osjetljivih podataka. Implementacija ISO 27001:2022 pomaže organizacijama da izgrade povjerenje kod svojih klijenata i partnera te da osiguraju kontinuitet poslovanja.[11] [12]

4.1. Lokalni zakoni

Zakon o zaštiti osobnih podataka

U mnogim zemljama postoje specifični zakoni koji reguliraju zaštitu osobnih podataka. Na primjer, u Hrvatskoj je na snazi Zakon o provedbi Opće uredbe o zaštiti podataka (GDPR), koji dopunjava GDPR i specificira dodatne mjere i obveze za organizacije. [1] [13]

Ključne odredbe zakona uključuju:

- Obveze voditelja obrade: Definiraju odgovornosti organizacija u vezi s obradom osobnih podataka.
- Prava ispitanika: Definiraju prava pojedinaca u vezi s njihovim osobnim podacima.
- Kazne i sankcije: Propisuju kazne za kršenje odredbi zakona.
- Pravila o čuvanju podataka (Data Retention Laws)
- U mnogim zemljama postoje pravila koja zahtijevaju da organizacije čuvaju određene vrste podataka tijekom određenog razdoblja. Ova pravila često obuhvaćaju podatke povezane s poslovanjem, financijama i komunikacijom.[13]

Ključni elementi pravila o čuvanju podataka uključuju:

- Vrste podataka koje treba čuvati: Definiranje specifičnih vrsta podataka koje organizacije moraju čuvati.
- Trajanje čuvanja podataka: Specificiranje vremenskog razdoblja tijekom kojeg se podaci moraju čuvati.
- Zaštita čuvanih podataka: Zahtjevi za zaštitu podataka tijekom razdoblja čuvanja.[14]

Regulative vezane uz specifične industrije

Osim općih zakona i regulativa, postoje i specifične regulative koje se primjenjuju na određene industrije (slika 4.).

- Financijski sektor: Regulativa kao što je Basel III postavlja standarde za upravljanje rizicima i zaštitu podataka u bankarstvu.
- Telekomunikacije: Regulativa koja zahtijeva čuvanje podataka o komunikaciji i zaštitu korisničkih podataka.
- Zdravstvo: Pored HIPAA-e, mnoge zemlje imaju dodatne regulative koje zahtijevaju zaštitu zdravstvenih informacija.[14]

Slika 4. Prikaz zaštite podataka

4.2. Implementacija pravnih zahtjeva

Usklađenost s regulativama (Compliance)

Usklađenost s regulativama ključna je za izbjegavanje pravnih sankcija i zaštitu ugleda organizacije. Organizacije trebaju razviti strategije za osiguranje usklađenosti s relevantnim zakonima i regulativama.[15]

Ključni koraci za osiguranje usklađenosti uključuju:

- Identifikacija relevantnih regulativa: Utvrđivanje koje se regulative primjenjuju na organizaciju i njezine operacije.
- Procjena trenutne usklađenosti: Procjena trenutnog stanja usklađenosti i identificiranje potencijalnih nedostataka.
- Implementacija potrebnih mjera: Implementacija tehničkih i organizacijskih mjera za postizanje usklađenosti.
- Kontinuirana revizija i poboljšanje: Redovita revizija i poboljšanje procesa za osiguranje trajne usklađenosti.

Uloga službenika za zaštitu podataka (DPO)

Službenik za zaštitu podataka (DPO) ključna je osoba u organizaciji koja je odgovorna za osiguranje usklađenosti s regulativama o zaštiti podataka. DPO nadzire sve aktivnosti vezane uz obradu podataka i osigurava da organizacija postupa u skladu s relevantnim zakonima.[15]

Odgovornosti DPO-a uključuju:

- Savjetovanje i edukacija: Savjetovanje organizacije o obvezama vezanim uz zaštitu podataka i edukacija zaposlenika.
- Praćenje usklađenosti: Praćenje usklađenosti organizacije s regulativama i internim politikama zaštite podataka.
- Surađivanje s nadzornim tijelima: Surađivanje s nadzornim tijelima za zaštitu podataka i odgovaranje na njihove upite.
- Upravljanje incidentima: Upravljanje incidentima povrede podataka i koordinacija odgovora na incidente.[16]

4.3. Izazovi koji dolaze s lokalnim zakonima i implementacijom

Kompleksnost regulativa

Različite zemlje i industrije imaju različite regulative, što može otežati organizacijama postizanje i održavanje usklađenosti. Organizacije moraju biti svjesne svih relevantnih regulativa i razviti strategije za upravljanje njihovim zahtjevima.

Troškovi usklađenosti

Postizanje usklađenosti s regulativama može biti skupo, posebno za manje organizacije. Troškovi mogu uključivati tehničke mjere za zaštitu podataka, troškove za edukaciju zaposlenika, te troškove za angažiranje pravnih i sigurnosnih stručnjaka.

Brzo mijenjanje regulativa

Pravni i regulatorni okviri često se mijenjaju kako bi odgovorili na nove prijetnje i tehnološke promjene. Organizacije moraju biti spremne prilagoditi svoje procese i mjere kako bi ostale usklađene s novim zahtjevima.

Ograničenja resursa

Nedostatak resursa, uključujući financijska sredstva i stručnjake za zaštitu podataka, može otežati postizanje i održavanje usklađenosti. Organizacije moraju učinkovito upravljati svojim resursima kako bi ispunile sve zahtjeve.

Pravni i regulatorni okviri igraju ključnu ulogu u osiguravanju sigurnosti podataka u oblaku. Organizacije moraju razumjeti relevantne regulative, implementirati potrebne mjere i kontinuirano pratiti usklađenost kako bi zaštitile svoje podatke i izbjegle pravne posljedice. U sljedećem dijelu rada istražit ćemo suvremene alate i tehnologije za sigurnosnu pohranu podataka u oblaku, te prikazati buduće trendove u ovom području.

5. Suvremeni alati i tehnologije za sigurnost podataka

5.1. Alati za šifriranje

Šifriranje podataka u mirovanju (data-at-rest encryption)

Šifriranje podataka u mirovanju osigurava zaštitu podataka dok su pohranjeni na diskovima ili drugim medijima za pohranu. Ovaj oblik šifriranja koristi se za sprječavanje neovlaštenog pristupa podacima u slučaju fizičke krađe medija ili „hakiranja“ poslužitelja.[17]

Popularni alati i tehnologije za šifriranje podataka u mirovanju uključuju:

- BitLocker: Alat za šifriranje cijelog diska koji je dio Windows operativnog sustava, omogućava šifriranje particija diska kako bi se zaštitili podaci.
- VeraCrypt: Besplatni open-source alat za šifriranje koji podržava šifriranje cijelog diska ili pojedinačnih datoteka i direktorija.
- AWS Key Management Service (KMS): Amazonov alat koji omogućava jednostavno upravljanje ključevima za šifriranje podataka pohranjenih na AWS-u.
- Šifriranje podataka u prijenosu (data-in-transit encryption)
- Šifriranje podataka u prijenosu osigurava zaštitu podataka dok se prenose preko mreža, sprječavajući neovlašteni pristup i presretanje podataka tijekom prijenosa.[18]

Popularni protokoli i alati za šifriranje podataka u prijenosu uključuju:

- Transport Layer Security (TLS): Kriptografski protokol koji osigurava privatnost i integritet podataka između komunikacijskih aplikacija.
- Secure Sockets Layer (SSL): Prethodnik TLS-a, koji se još uvijek koristi u mnogim aplikacijama za šifriranje podataka tijekom prijenosa.
- IPsec: Skupina protokola za osiguranje internetskog prometa putem šifriranja i autentifikacije.[17][18]
-

5.2. Upravljanje identitetom

Sustavi za upravljanje identitetom i pristupom omogućuju organizacijama kontrolu nad time tko ima pristup resursima u oblaku.[20]

Ključne komponente IAM sustava uključuju:

- Autentifikacija: Proces provjere identiteta korisnika. Primjeri alata za autentifikaciju uključuju okvire za jednokratnu prijavu (SSO) kao što su Okta i Azure Active Directory.
- Autorizacija: Proces određivanja prava pristupa korisnika resursima. Ovo uključuje definiranje korisničkih uloga i politika pristupa.
- Upravljanje identitetom: Proces upravljanja korisničkim identitetima tijekom cijelog njihovog životnog ciklusa, uključujući kreiranje, ažuriranje i brisanje identiteta.

Popularni IAM alati i sustavi uključuju:

- Okta: SSO i IAM platforma koja omogućuje upravljanje korisničkim pristupom aplikacijama i resursima.
- Azure Active Directory (AAD): Microsoftova IAM usluga koja omogućuje upravljanje pristupom Azure resursima i aplikacijama.
- Google Cloud Identity: Googleova platforma za upravljanje identitetima i pristupom resursima na Google Cloud Platformi.[19][20]

Upravljanje identitetom koristi se za kontrolu pristupa sustavima i podacima unutar organizacije, osiguravajući da samo ovlašteni korisnici mogu pristupiti određenim resursima. Dobro upravljanje identitetom poboljšava sigurnost smanjujući rizik od neovlaštenog pristupa i omogućava organizacijama da učinkovito upravljaju korisničkim pravima i dozvolama. S druge strane, loše upravljanje identitetom može dovesti do sigurnosnih propusta, kao što su prevelike privilegije korisnika, što povećava rizik od internih prijetnji i potencijalnih napada. Također, složeni sustavi za upravljanje identitetom mogu biti izazovni za implementaciju i održavanje, zahtijevajući stalno praćenje i ažuriranje.

5.3. Alati za oporavak i kopiranje

Sigurnosno kopiranje i oporavak podataka ključni su za zaštitu podataka od gubitka i osiguranje kontinuiteta poslovanja.[21]

Ključne funkcionalnosti ovih alata uključuju:

- Automatizirano sigurnosno kopiranje: Redovito stvaranje sigurnosnih kopija podataka bez potrebe za ručnom intervencijom.
- Obnavljanje podataka: Brz i jednostavan postupak vraćanja podataka iz sigurnosnih kopija u slučaju gubitka podataka.
- Verzije podataka: Pohranjivanje više verzija podataka kako bi se omogućilo vraćanje na prethodne verzije u slučaju pogreške ili korupcije podataka.

Popularni alati za sigurnosno kopiranje i oporavak podataka uključuju:

- Veeam Backup & Replication: Alat za sigurnosno kopiranje i oporavak podataka koji podržava virtualizirane, fizičke i cloud infrastrukture.
- Acronis True Image: Alat za sigurnosno kopiranje i oporavak podataka koji nudi potpunu zaštitu podataka na računalima i mobilnim uređajima.
- AWS Backup: Amazonova usluga koja omogućuje automatizirano sigurnosno kopiranje i oporavak podataka pohranjenih na AWS-u.

5.4. Alati za praćenje

Web-mjesta koriste alate za praćenje za prikupljanje podataka o ponašanju pri pregledavanju. Alati za praćenje prikupljaju podatke o načinu vaše interakcije s web-mjestom, kao što je to sadržaj na koji kliknete. Omogućuju i funkcionalnost na nekim web-mjestima, primjerice odjeljke komentara ili gumbe za dijeljenje članaka na društvenim mrežama te personalizirane oglase.

Neki alati za praćenje prikupljaju podatke o vama na više web-mjesta. Na primjer, alat za praćenje može pratiti kada odete u vašu omiljenu internetsku trgovinu i na web-mjesto s novostima. Zbog toga se ponekad možete osjećati kao da vas oglas prati diljem weba.[22]

Ključne funkcionalnosti ovih alata uključuju:

- Praćenje u stvarnom vremenu: Kontinuirano praćenje aktivnosti i događaja u sustavu kako bi se brzo otkrile sigurnosne prijetnje.
- Revizijski zapisi: Evidencija svih relevantnih događaja i aktivnosti, koja omogućuje analizu i istraživanje incidenata.
- Upozorenja: Automatsko slanje upozorenja o sumnjivim aktivnostima ili sigurnosnim incidentima.

Popularni alati za praćenje i reviziju uključuju:

- Splunk: Platforma za praćenje i analizu podataka koja omogućuje prikupljanje, pretraživanje i analizu podataka iz različitih izvora.
- Elastic Stack (ELK): Skup alata koji uključuje Elasticsearch, Logstash i Kibana za pretraživanje, analizu i vizualizaciju podataka.
- AWS CloudTrail: Amazonova usluga koja omogućuje praćenje aktivnosti korisnika i API poziva na AWS-u, te prikupljanje revizijskih zapisa.[22]

5.5. Alati za zaštitu DDos napada

DDoS napad cilja web-mjesta i poslužitelje ometanjem mrežnih usluga u pokušaju iscrpljivanja resursa aplikacije. Napadači iza tih napada preplavljuju web-mjesto nasumičnim prometom, što rezultira lošom funkcionalnošću web-mjesta ili potpunim izbacivanjem s mreže.[23]

Ključne funkcionalnosti ovih alata uključuju:

- Prepoznavanje napada: Brzo prepoznavanje DDoS napada pomoću analize mrežnog prometa.
- Ublažavanje napada: Automatske mjere za smanjenje utjecaja napada, kao što su filtriranje prometa i raspodjela opterećenja.
- Prilagodba i skalabilnost: Mogućnost prilagodbe i skaliranja obrambenih mjera prema intenzitetu napada.[23][24]

Popularni alati za zaštitu od DDoS napada uključuju:

- AWS Shield: Amazonova usluga koja pruža zaštitu od DDoS napada za aplikacije i resurse na AWS-u.
- Cloudflare: CDN i sigurnosna platforma koja nudi zaštitu od DDoS napada, optimizaciju performansi i druge sigurnosne značajke.
- Azure DDoS Protection: Microsoftova usluga koja pruža zaštitu od DDoS napada za aplikacije i resurse na Azure platformi.[24]

5.6. Tehnologija za sigurnost privatnosti osobnih podataka

Osiguranje privatnosti podataka ključna je komponenta sigurnosne pohrane podataka u oblaku.

Ključne tehnologije za osiguranje privatnosti podataka uključuju:

- Anonimizacija i pseudonimizacija: Tehnike za zaštitu identiteta pojedinaca uklanjanjem ili zamjenom identifikacijskih informacija.
- Diferencijalna privatnost: Tehnika koja dodaje šum podacima kako bi zaštitila privatnost pojedinaca prilikom analize podataka.
- Homomorfno šifriranje: Tehnika koja omogućuje obradu šifriranih podataka bez potrebe za njihovim dešifriranjem, osiguravajući tako privatnost tijekom obrade.

Popularni alati i tehnologije za osiguranje privatnosti podataka uključuju:

- IBM Data Privacy Passports: Alat koji omogućuje kontrolu pristupa i zaštitu podataka pomoću šifriranja i politika privatnosti.
- Microsoft Azure Confidential Computing: Tehnologija koja omogućuje obradu podataka u šifriranom obliku kako bi se osigurala privatnost podataka.
- Google Cloud Confidential Computing: Googleova tehnologija koja omogućuje šifriranu obradu podataka u oblaku.

Suvremeni alati i tehnologije za sigurnosnu pohranu podataka u oblaku pružaju niz rješenja za zaštitu podataka od različitih prijetnji. Organizacije moraju pažljivo odabrati i integrirati ove alate kako bi osigurale sveobuhvatnu zaštitu svojih podataka i uskladile se s relevantnim pravnim i regulatornim zahtjevima. U sljedećem dijelu rada istražit ćemo buduće trendove u sigurnosnoj pohrani podataka u oblaku i njihove potencijalne utjecaje na organizacije.

6. Razvoj novih tehnologija za zaštitu podataka

Kvanta kriptografija

Kvanta kriptografija predstavlja značajan napredak u području sigurnosti podataka koristeći principe kvantne mehanike za stvaranje sigurnih komunikacijskih kanala. Ova tehnologija koristi kvantne bitove ili qubite za distribuciju kriptografskih ključeva, čime omogućava apsolutnu sigurnost komunikacija.

Ključne komponente kvanta kriptografije:

- Quantum Key Distribution (QKD): Tehnika koja koristi kvantne fotone za stvaranje sigurnih ključeva. QKD omogućava detekciju prisutnosti napadača jer bilo kakvo presretanje kvantnih fotona mijenja njihovu prirodu, čime se otkriva pokušaj prisluškivanja.
- Otpornost na kvantne računare: Kvantni računari prijete postojećim kriptografskim sustavima zbog svoje sposobnosti da brzo razbije klasične šifre. Kvantna kriptografija nudi rješenja koja su otporna na napade kvantnih računara.[25]

Primjene kvanta kriptografije:

- Financijski sektor: Zaštita transakcija i komunikacija unutar financijskih institucija.
- Vladine agencije: Osiguranje povjerljivih vladinih informacija i komunikacija.
- Obrambene institucije: Sigurnost vojnih komunikacija i osjetljivih podataka.

Ključne inovacije u šifriranju uključuju:

- Homomorfno šifriranje: Omogućava obradu šifriranih podataka bez potrebe za njihovim dešifriranjem, čime se omogućuje analiza podataka u šifriranom stanju i očuvanje privatnosti.
- Post-kvantno šifriranje: Razvija se kako bi se pripremili za eru kvantnih računara koji mogu ugroziti postojeće kriptografske metode. Ove tehnike su dizajnirane da budu otporne na napade kvantnih računara.[25]

6.1. Umjetna inteligencija i strojno učenje

Umjetna inteligencija (AI) i strojno učenje (ML)

AI i ML postaju sve važniji u analizi sigurnosnih prijetnji i upravljanju podacima. Ove tehnologije omogućuju automatsko prepoznavanje obrazaca i anomalija u velikim količinama podataka, poboljšavajući sposobnost otkrivanja i reagiranja na sigurnosne prijetnje.[26]

Primjene AI i ML u sigurnosti podataka uključuju:

1. Prepoznavanje prijetnji: AI i ML algoritmi mogu identificirati neobične obrasce u mrežnom prometu ili korisničkim aktivnostima, što može ukazivati na sigurnosne prijetnje kao što su napadi i malware.
2. Automatizacija sigurnosnih odgovora: Automatizacija procesa odgovora na prijetnje, uključujući blokiranje sumnjivih aktivnosti i obavještavanje administratora, omogućava brži odgovor i smanjenje ljudskih pogrešaka.
3. Prediktivna analitika: Korištenje ML modela za predviđanje budućih prijetnji na temelju povijesnih podataka i trendova.[26]

Primjeri primjene AI i ML:

1. Sigurnosni alati i platforme: Alati kao što su IBM QRadar i Splunk integriraju AI i ML za poboljšanje detekcije i analize sigurnosnih prijetnji.
2. Pružatelji usluga u oblaku, AWS i Microsoft Azure, koriste AI i ML za poboljšanje sigurnosti svojih usluga, uključujući prepoznavanje prijetnji i automatsko upravljanje incidentima.

6.2. Razvoj sigurnosnih politika

Povećana regulacija i standardizacija

Kako rastu prijetnje i složenost u oblačnoj sigurnosti, regulatori i industrijske organizacije razvijaju sve strože standarde i politike za upravljanje sigurnošću podataka.[27]

1. NIS2 (Direktiva o sigurnosti mrežnih i informacijskih sustava)

NIS2 je ažurirana verzija prvotne NIS direktive usvojene 2016. godine, a njen cilj je jačanje kibernetičke sigurnosti unutar EU. Ključne promjene uključene u NIS2 su sljedeće:

- Proširenje opsega: NIS2 obuhvaća širi raspon sektora, uključujući zdravstvo, digitalnu infrastrukturu, javne usluge i financijske institucije.
- Pojačana sigurnosna pravila: Uvodi strožije zahtjeve za sigurnosne mjere, uključujući upravljanje rizicima, otkrivanje incidenata i mjere za prevenciju kibernetičkih prijetnji.
- Odgovornost: Postrožava se odgovornost menadžmenta za kibernetičku sigurnost, s potencijalnim kaznama za nepoštivanje propisa.
- Suradnja i izvještavanje: Organizacije moraju brzo prijaviti kibernetičke incidente nadležnim tijelima, a jača se i međunarodna suradnja u borbi protiv kibernetičkih prijetnji.

NIS2 ima za cilj poboljšati otpornost EU na kibernetičke prijetnje i osigurati da kritične infrastrukture budu bolje zaštićene.

2.DORA (Digital Operational Resilience Act)

DORA je regulativa usmjerena na financijski sektor unutar EU, s ciljem osiguravanja digitalne otpornosti financijskih institucija. Regulativa se fokusira na to kako institucije upravljaju rizicima povezanim s informacijskom tehnologijom (IT) i digitalnim uslugama. Ključne točke DORA-e uključuju:

- IT upravljanje rizicima: Financijske institucije moraju uvesti stroge procese za upravljanje IT rizicima, uključujući redovito testiranje sustava i provjeru sigurnosti.
- Otpornost na digitalne prijetnje: Institucije moraju osigurati da su njihovi sustavi otporni na kibernetičke napade, prekide rada ili druge digitalne prijetnje koje bi mogle ugroziti financijsku stabilnost.
- Incident reporting: Financijske institucije moraju brzo prijavljivati digitalne incidente regulatornim tijelima, čime se omogućuje bolja procjena rizika na razini EU.
- Suradnja s trećim stranama: DORA regulira i odnose s vanjskim pružateljima IT usluga, uključujući oblak, kako bi se osiguralo da su i oni usklađeni s visokim standardima otpornosti.

DORA ima za cilj poboljšati cjelokupnu otpornost financijskog sektora na digitalne prijetnje i pomoći institucijama da odgovore na digitalne rizike na održiv način.

Ključni aspekti razvoja sigurnosnih politika uključuju:

- Kompilacija i usklađivanje s regulativama: Organizacije će morati uskladiti svoje sigurnosne politike s novim regulativama i standardima kao što su GDPR, CCPA i ISO/IEC 27001.
- Sigurnost podataka u oblaku: Razvijanje politika koje specifično adresiraju sigurnosne izazove u oblačnim okruženjima, uključujući upravljanje pristupom, enkripciju i zaštitu privatnosti.

Primjeri budućih politika i regulativa:

- Regulative o privatnosti: Očekuje se da će se regulative kao što su GDPR i CCPA dalje razvijati kako bi se adresirali novi izazovi i tehnologije.
- Industrijski standardi: Organizacije poput NIST (National Institute of Standards and Technology) i ISO nastavljaju razvijati nove standarde za sigurnost podataka u oblačnim okruženjima.

6.3. Razvoj tehnologija za privatnost osobnih podataka

Tehnologije za privatnost podataka

Kako se sve više pažnje posvećuje privatnosti korisnika, tehnologije koje omogućuju zaštitu privatnosti podataka postaju ključne.

Ključne tehnologije za privatnost podataka uključuju:

- Diferencijalna privatnost: Tehnika koja dodaje šum podacima kako bi se zaštitila privatnost pojedinaca u skupnim analizama, dok se istovremeno omogućava korisna analiza podataka.
- Anonimizacija i pseudonimizacija: Procesi koji uklanjaju ili maskiraju identifikacijske informacije kako bi se zaštitila privatnost korisnika dok se podaci i dalje mogu koristiti za analizu.

Primjeri primjene tehnologija za privatnost podataka:

- Analitika i istraživanje: Korištenje diferencijalne privatnosti za analizu velikih skupova podataka bez otkrivanja osobnih informacija.
- Zdravstvo: Anonimizacija zdravstvenih podataka kako bi se omogućila istraživanja i analiza bez ugrožavanja privatnosti pacijenata.[28]

Budući trendovi u sigurnosnoj pohrani podataka u oblaku uključuju razvoj naprednih tehnologija za zaštitu podataka, integraciju umjetne inteligencije i strojnog učenja, evoluciju sigurnosnih politika i regulativa, proširenje uporabe arhitekture hibridnih i višestrukih ovlaka te razvoj tehnologija za privatnost podataka. Ove promjene i inovacije imaju potencijal značajno poboljšati sigurnost i privatnost podataka u oblačnim okruženjima. Organizacije će morati prilagoditi svoje strategije i alate kako bi ostale ispred prijetnji i osigurale zaštitu svojih podataka u brzo mijenjajućem tehnološkom pejzažu.

7. Primjer napada na sustav

Ponuditelj treba navesti opis usluge i rješenja za oporavak u slučaju katastrofe (Disaster Recovery Solution – DRS) za informatičku infrastrukturu i podatkovni centar korisnika.

S obzirom na složenost okoline i ograničene ljudske resurse, cilj korisnika je da s ovom nabavom osigura DRS koje je skalabilno, fleksibilno i jednostavno za uporabu.

7.1. Specifikacija zahtjeva

Okvirni sporazum se sklapa s dobavljačem za usluge/rješenje za oporavak u slučaju katastrofe (Disaster Recovery as a Service – DraaS). Kako bi osigurao kontinuitet poslovanja, korisnik traži uslugu oporavka u slučaju katastrofe kao zaokruženu ICT uslugu (DRaaS) te uslugu implementacije i kolokacije uređaja za sigurnosnu pohranu podataka. Za potrebe takve usluge traži se cjelokupno rješenje (DRaaS), koje se sastoji od infrastrukture, sustava za replikaciju i zaštitu podataka, komunikacijskog rješenja i održavanja cjelokupnog rješenja. DRaaS za korisnik mora biti udaljen barem 25 km od primarne lokacije korisnika, Primarna funkcija rješenja je redovito repliciranje virtualnih poslužitelja sa primarne na DR virtualnu okolinu koja se nalazi na drugoj (DR) lokaciji u CDP (Continuous Data Protection) načinu radu.

Mreža na obje lokacije mora moći koristiti isti privatni adresni prostor istovremeno (Layer 2). Dobavljač mora osigurati konstantan VPN pristup putem interneta do DR lokacije. Za potrebe rješenja Dobavljač mora osigurati jednu (1) javnu IP adresu. Usluga mora biti upravljiva nezavisno, bez intervencije pružatelja usluge, dostupna za testiranje i u slučaju havarije pet (5) dana mjesečno ili trideset (30) dana godišnje, a u slučaju potrebe aktivna sukladno njegovim procedurama i zahtjevima. Neiskorišteni dani kumulativno se zbrajaju za vrijeme trajanja usluge. Upravljiva usluga nezavisno o pružatelju usluge znači da korisnik može samostalno upravljati infrastrukturom, vatrozidom i sustavom za replikaciju i zaštitu podataka bez potrebe za angažmanom pružatelja usluge (self-service). Korisnik mora sam moći upravljati prebacivanjem rada s primarne na DR lokaciju bez angažiranja pružatelja usluge.

Dobavljač mora osigurati važeće licence za rad cjelokupnog rješenja tijekom korištenja usluge od strane korisnika. Dobavljač mora održavati cjelokupno ponuđeno rješenje. Pri dostavi ponude Dobavljač mora opisati način rada tehničke podrške i izdati potvrdu da DR lokacija odgovara traženim zahtjevima. Za virtualizaciju poslužitelja mora se koristiti VMware vSphere softver sa svim pripadajućim servisima koji osiguravaju traženi nivo dostupnosti informatičkog sustava.

VM	vCPU, kom	vRAM, GB	HDD, GB	OS
Server01	4	8	30	MS win
Server02	4	8	30	MS win
Server03	4	8	110	MS win
Server04	4	16	23	MS win
Server05	4	16	60	MS win
Server06	4	8	160	MS win
Server07	4	8	160	MS win
Server08	2	4	40	MS win
Server09	4	8	260	MS win
Server10	4	32	1200	MS win
Server11	8	16	620	MS win
Server12	2	4	50	MS win
Server13	2	16	120	MS win
Server14	8	16	150	linux
Server15	4	8	350	linux
Server16	8	56	700	MS win
Server17	4	16	100	MS win
Server18	4	22	550	linux
Server19	12	54	650	MS win
Server20	12	62	610	MS win
Server21	4	24	200	kinux
Server22	4	8	100	linux
Server23	2	4	1100	appliance
Server24	4	8	90	MS win
Server25	8	16	380	linux
Server26	4	4	50	linux
Server27	2	4	40	linux
Server28	2	4	60	linux
ukupno	148	490	9023	

Sustav mora jamčiti:

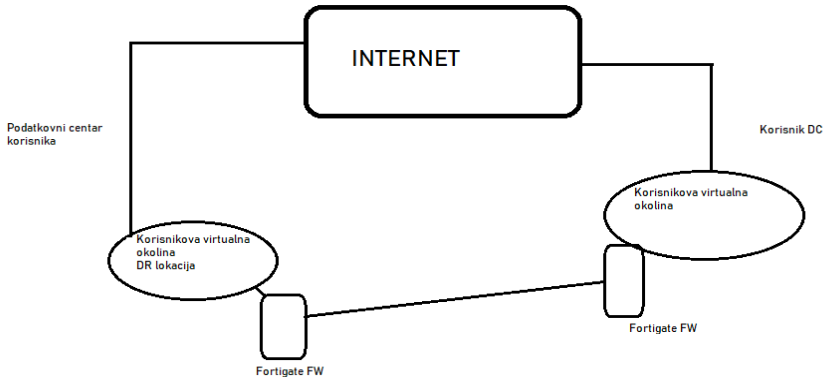
- SLA 99.9%
- Gubitak IP Paketi <0,1%
- Monitoring 24/7/365

Oprema koja se nalazi na primarnoj lokaciji HGK i koju treba podržati DRS

Korisnikova virtualna infrastruktura je VMware virtualizacijsko okruženje. Korisnik na svojoj lokaciji ima 2 Forti E500 uređaja te koristi javne IP adrese pružatelja usluga pristupa Internetu.

7.2. Mreža povezanosti

Za osiguravanje stabilne povezanosti glavne lokacije podatkovnog centra korisnika s lokacijom podatkovnog centra, namijenjenom za DRS, potrebno je koristiti svjetlovodnu infrastrukturu i MPLS mrežu, čime se osigurava brza i pouzdana povezanost. Korisnik će za DR lokaciju koristiti internetsku vezu pružatelja usluge pristupa internetu svog pružatelja te usluge, telekomunikacijskog operatora. Dobavljač DRS na DR lokaciji osigurava pristup internetu putem vlastite mreže te dodjeljuje javnu adresu iz svojeg raspona za potrebe „back-door“ pristupa na DR lokaciju. Na DR lokaciji treba bit osigurana kolokacija za smještaj korisničke opreme i veza između kolocirane opreme i operatora.



Slika 5. Prikaz mreže

Ukupni resursi:

DraaS, Zerto:

Zerto licenca	Backup prostor (GB)
29	**12 000**

VM	vCPU, kom	vRAM, GB	HDD, GB
29	148	490	9023

Ethernet link: 1 Gbit/s

7.3. Popis poslužitelja koji se trebaju replicirati

R.br.	Parametar	Vrijednosti
5.1	Broj Windows Server poslužitelja	18
5.2	Broj Linux poslužitelja	9
5.3	Ostali poslužitelji	2
5.4	Količina podataka za replikaciju u GB	9023

R.br.	Server	TIP (fizički/virtualni)	vCPU (core)	RAM/GB	disk ukupno (GB)	OS
7.1	Server 01	virtualni	4	8	30	WinSvr
7.2	Server 02	virtualni	4	8	30	WinSvr
7.3	Server 03	virtualni	4	8	110	WinSvr
7.4	Server 04	virtualni	4	16	23	WinSvr
7.5	Server 05	virtualni	4	16	60	WinSvr
7.6	Server 06	virtualni	4	8	160	WinSvr
7.7	Server 07	virtualni	4	8	160	WinSvr
7.8	Server 08	virtualni	2	4	40	WinSvr
7.9	Server 09	virtualni	4	8	260	WinSvr
7.10	Server 10	virtualni	4	32	1200	WinSvr
7.11	Server 11	virtualni	8	16	620	WinSvr
7.12	Server 12	virtualni	2	4	50	WinSvr
7.13	Server 13	virtualni	2	16	120	WinSvr
7.14	Server 14	virtualni	8	16	150	Linux
7.15	Server 15	virtualni	4	8	350	Linux
7.16	Server 16	virtualni	8	56	700	WinSvr
7.17	Server 17	virtualni	4	16	100	WinSvr
7.18	Server 18	virtualni	4	22	550	Linux
7.19	Server 19	virtualni	12	54	650	WinSvr
7.20	Server 20	virtualni	12	62	610	WinSvr
7.21	Server 21	virtualni	4	24	200	Linux
7.22	Server 22	virtualni	4	8	100	Linux
7.23	Server 23	virtualni	2	4	1100	Appliance
7.24	Server 24	virtualni	4	8	90	WinSvr
7.25	Server 25	virtualni	16	32	1030	Appliance
7.26	Server 26	virtualni	8	16	380	Linux
7.27	Server 27	virtualni	4	4	50	Linux
7.28	Server 28	virtualni	2	4	40	Linux
7.29	Server 29	virtualni	2	4	60	Linux

7.4. Managed Hosted server – samouslužna infrakstruktura

Red Br.	Tražene tehničke karakteristike	Minimalna količina
1.	vCPU na fizičkim procesorima - Intel(R) Xeon(R)	148
3.	vRAM – DDR4 RAM ili bolji *	490 GB
4.	SAS disk *	12000 GB
5.	NL-SAS disk *	0 GB
6.	Visoko dostupni Enterprise class SAN storage s min dva kontrolera *	1
7.	Infrastruktura mora biti visoko dostupna (poslužitelji u cluster-u s VMware HA i VMware DRS) *	1

- *omogućiti uvid korisniku tijekom cijelog vremena korištenja

8. Zaključak

Zaključak završnog rada o sigurnosnoj pohrani podataka u oblaku naglašava ključnu ulogu koju oblak igra u modernom poslovanju, ali i izazove koje donosi u pogledu sigurnosti podataka. Oblak nudi nevjerojatne prednosti poput skalabilnosti, fleksibilnosti i dostupnosti, što omogućava organizacijama da optimiziraju svoje operacije i smanje troškove infrastrukture. Međutim, te iste prednosti otvaraju i nove sigurnosne rizike koji zahtijevaju pažljivo upravljanje.

U radu su razmatrani glavni izazovi sigurnosne pohrane podataka u oblaku, uključujući prijetnje poput neovlaštenog pristupa, gubitka podataka i tehničkih kvarova, kao i izazove povezane s usklađenošću s regulativama i standardima. Važno je napomenuti da se sigurnosni rizici mogu učinkovito ublažiti implementacijom odgovarajućih mjera, poput šifriranja podataka, naprednog upravljanja identitetom i pristupom, te redovitog sigurnosnog kopiranja i oporavka podataka.

Tehnološki napredak, kao što su kvantna kriptografija i integracija umjetne inteligencije, donosi nove mogućnosti za poboljšanje sigurnosti podataka u oblaku. Kvantna kriptografija obećava iznimno visoku razinu sigurnosti koja će biti otporna na buduće kvantne računare, dok umjetna inteligencija omogućava napredne sustave za prepoznavanje prijetnji i automatsko upravljanje sigurnosnim incidentima. Međutim, ove tehnologije još uvijek su u fazi razvoja i zahtijevaju daljnja istraživanja i prilagodbu prije nego što postanu široko primjenjive.

Budući trendovi u sigurnosnoj pohrani podataka u oblaku sugeriraju daljnji rast rješenja u hibridnom ili višestrukom oblaku, kao i rješenja, koja kombiniraju najbolje aspekte različitih oblačnih okruženja kako bi optimizirala performanse, sigurnost i troškove. Organizacije će sve više morati balansirati između različitih pružatelja usluga kako bi osigurale maksimalnu sigurnost i usklađenost s rastućim regulativnim zahtjevima.

Zaključno, sigurnosna pohrana podataka u oblaku nije samo tehnički izazov već i strateški prioritet za svaku organizaciju koja koristi oblak. Uspješna implementacija sigurnosnih mjera zahtijeva holistički pristup koji uključuje tehničke, proceduralne i organizacijske aspekte. Organizacije koje usvoje ovaj pristup bit će bolje pripremljene za suočavanje s budućim sigurnosnim izazovima, čime će osigurati dugoročni kontinuitet poslovanja, povjerenje klijenata i zaštitu svojih najvrjednijih resursa—podataka. Oblak, kao ključna komponenta modernih IT infrastruktura, može biti sigurno i pouzdano okruženje za pohranu podataka, ali samo ako se primjenjuju odgovarajuće sigurnosne mjere i stalno prati razvoj novih prijetnji i tehnologija.

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU

Završni/diplomski/specijalistički rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, Emanuel Bučaj (*ime i prezime*) pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog/specijalističkog (*obrisati nepotrebno*) rada pod naslovom Sigurnosna pohrana podataka u oblaku (*upisati naslov*) te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(*upisati ime i prezime*)
Emanuel Bučaj
(vlastoručni potpis)

Sukladno članku 58., 59. i 61. Zakona o visokom obrazovanju i znanstvenoj djelatnosti završne/diplomske/specijalističke radove sveučilišta su dužna objaviti u roku od 30 dana od dana obrane na nacionalnom repozitoriju odnosno repozitoriju visokog učilišta.

Sukladno članku 111. Zakona o autorskom pravu i srodnim pravima student se ne može protiviti da se njegov završni rad stvoren na bilo kojem studiju na visokom učilištu učini dostupnim javnosti na odgovarajućoj javnoj mrežnoj bazi sveučilišne knjižnice, knjižnice sastavnice sveučilišta, knjižnice veleučilišta ili visoke škole i/ili na javnoj mrežnoj bazi završnih radova Nacionalne i sveučilišne knjižnice, sukladno zakonu kojim se uređuje umjetnička djelatnost i visoko obrazovanje.

9. Literatura

[1] Računalstvo u oblaku - https://hr.wikipedia.org/wiki/Ra%C4%8Dunarstvo_u_oblaku

[2] Računalstvo u oblaku - https://courses.minnalearn.com/hr/courses/digital-revolution/the-cloud-computing-revolution/how-is-the-cloud-built-and-how-does-it-work/

[3] Računalstvo u oblaku - https://www.guru99.com/hr/types-of-cloud-computing.html

[4] Računalstvo u oblaku - https://www.guru99.com/hr/advantages-disadvantages-cloud-computing.html

[5] Sigurnost u oblaku - https://www.microsoft.com/hr-hr/security/business/security-101/what-is-cloud-security

[6] Sigurnost u oblaku - https://www.storm.hr/hr/rjesenje/sigurnosna-pohrana-podataka-i-oporavak-od-katastrofe

[7] Vatrozid - https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[8] SIEM - https://www.microsoft.com/hr-hr/security/business/security-101/what-is-siem

[9] GDPR - https://gdprinformer.com/vodic-kroz-gdpr

[10] HIPAAhttps://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[11] ISO 27001 - https://en.wikipedia.org/wiki/ISO/IEC_27001

[12] ISO 27001:2022 - https://www.ti-solutions.hr/iso/iec-27001---informacijska-sigurnost?gad_source=1&gclid=Cj0KCQjw2ou2BhCCARIsANAwM2Gf-YVGIejdvgBVnXMickNKBcRmY1MIPdJ7d6FAZo9EEzqWIwLuGF0aAvG3EALw_wcB

[13] GDPR - https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868?lang=hr

[14] Čuvanje podataka u oblaku - https://www.zakon.hr/z/3112/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-%28EU%29-2016-679-

[15] Zaštita osobnih podataka - https://seminar.hr/zadace-sluzbenika-za-zastitu-osobnih-podataka/

[16] Zaštita osobnih podataka - https://azop.hr/sluzbenik-za-zastitu-podataka-2/

[17] Alati za zaštitu osobnih podataka - https://arc-rec-project.eu/wp-content/uploads/2021/01/Vodic-za-informacijsku-sigurnost.pdf

[18] Alati za šifriranje - https://www.cis.hr/sigurnosni-alati/kriptiranje-podataka.html

[19] Upravljanje identitetom - https://www.microsoft.com/hr-hr/security/business/security-101/what-is-identity-access-management-iam

[20] Upravljanje identitetom - https://www.cert.hr/wp-content/uploads/2005/08/CCERT-PUBDOC-2005-08-132.pdf

[21] Alati za oporavak - https://support.microsoft.com/hr-hr/windows/stvaranje-pogona-za-oporavak-abb4691b-5324-6d4a-8766-73fab304c246

[22] Alati za praćenje - https://support.microsoft.com/hr-hr/microsoft-edge/dodatne-informacije-o-sprje%C4%8Davanju-pra%C4%87enja-u-pregledniku-microsoft-edge-5ac125e8-9b90-8d59-fa2c-7f2e9a44d869

[23] Alati za DDoS napade - https://www.cert.hr/wp-content/uploads/2022/10/zastita_od_ddos_napada.pdf

[24] DDoS napad - https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-ddos-attack

[25] Kvantna kriptografija - https://hr.wikipedia.org/wiki/Kvantna_kriptografija

[26] Umjetna inteligencija i strojno učenje - https://www.cadcam-group.eu/hr/knowledge/sto-su-umjetna-inteligencija-i-strojno-ucenje-i-zasto-su-vazni/

[27] Buduća politika - https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf

[28] Razvoj tehnologija za privatnost- https://gdprinformer.com/gdpr-clanci/privatnost-nove-tehnologije

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, „Above the Clouds: A Berkeley View of Cloud Computing", 2009

   https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

2. Marinescu, Dan C. „Cloud computing: theory and practice", Morgan Kaufmann, 2017 https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/212-Cloud-Computing-Theory-and-Practice-Dan-C.-Marinescu-Edisi-2-2017.pdf

3. I. Lovrek, T. Lovrić, D. Lučić: "Regulatory Aspects of Cloud Computing", Proceedings SoftCOM 2012 20th International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Hvar, Croatia, 2012

4. I. Lovrek, A. Carić and D. Lučić: „Future Network and Future Internet: A Survey of Regulatory Perspective", Proceedings Proceedings SoftCOM 2013 21st International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Primošten, Croatia, 2013

5. D. Lučić, A. Carić and I. Lovrek, „Standardisation and Regulatory Context of Machine-to-Machine Communication", Proceedings ConTEL 2015 13th International Conference on Telecommunications, Graz, Austria, 2015, pp. 1-7.

6. D. Lučić, M. Weber and I. Lovrek, "Electronic Communications as Smart City Enablers", Proceedings 2016 International Conference on Smart Systems and Technologies (SST), Osijek; Croatia, 2016, pp. 241 – 247

7. M. Weber, D. Lučić and I. Lovrek, "Internet of Things Context of the Smart City", *Proceedings 2017 International Conference on Smart Systems and Technologies (SST)*, Osijek; Croatia, 2017, pp. 187 – 195