KORPORATIVNA INFORMACIJSKA SIGURNOST

Biljanović, Paula

Master's thesis / Specijalistički diplomski stručni

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:271092

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Paula Biljanović

KORPORATIVNA INFORMACIJSKA SIGURNOST

ZAVRŠNI RAD

Karlovac, 2021.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Paula Biljanović

CORPORATE INFORMATION SECURITY

Final paper

Karlovac, 2021.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Paula Biljanović

KORPORATIVNA INFORMACIJSKA SIGURNOST

ZAVRŠNI RAD

Mentor:

dr. sc. Damir Kralj, prof. v. š.

Karlovac, 2021.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Specijalistički diplomski stručni studij sigurnosti i zaštite

Usmjerenje: Zaštita na radu Karlovac, 24.02.2021.

ZADATAK ZAVRŠNOG RADA

Student: Paula Biljanović Matični broj: 0422418012

Naslov: Korporativna informacijska sigurnost

Opis zadatka:

-na osnovi dostupnih izvora te vlastitih iskustava i saznanja stečenih kroz školovanje i praksu, ukratko analizirati važnost informacijske sigurnosti te istražiti kako pravna regulativa (domaća i EU) definira pojam korporativne (poslovne) informacijske sigurnosti te kako obavezuje tvrtke na njezino provođenje;

-osvrnuti se na položaj evidencija po ZNR u okviru ukupnih korporativnih evidencija te opisati njihov položaj u okviru poslovnih informacijskih sustava;

-u eksperimentalnom dijelu rada definirati bitne kategorije korporativne sigurnosti, opisati stupnjeve njihove važnosti i funkcionalno područje koje pokrivaju, a sukladno mogućnostima ove definicije potkrijepiti i nekim dostupnim primjerima iz prakse.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
24.02.2021.	22.04.2021.	30.04.2021.

Mentor: Predsjednik Ispitnog povjerenstva:

dr.sc. Damir Kralj, prof. v. š. dr.sc. Vladimir Tudić, prof. v. š.

PREDGOVOR

Izjavljujem da sam ovaj rad izradila samostalno koristeći se navedenom literaturom i znanjem koje sam stekla tijekom studiranja.

Zahvaljujem se mentoru dr. sc. Damiru Kralju, prof. v. š. na pruženoj stručnoj pomoći, savjetima i razumijevanju tijekom izrade završnog rada.

Zahvaljujem se svojoj mami na pruženoj ljubavi, pomoći, potpori i razumijevanju tijekom mojega studiranja.

Paula Biljanović

SAŽETAK

Korporativno upravljanje sigurnošću obuhvaća sve sigurnosne segmente poslovnog sustava: sigurnost vlasništva, sigurnost ugovorenih poslova, administrativnu sigurnost, fizičku i tehničku sigurnost, sigurnost osoblja, sigurnost kontinuiteta rada, zaštitu od požara, zaštitu intelektualnog vlasništva, djelovanje u izvanrednim uvjetima, informacijsku sigurnost te još neke dijelove korporativne sigurnosti.

Informacijska sigurnost danas treba biti dio korporativnog upravljanja i korporativne sigurnosti. Obuhvaća IT komponente, ali i komponente informacijske sigurnosti koji nisu IT. Za svaki poslovni sustav informacije su temeljni poslovni resurs, njegova krucijalna imovina.

Ključne riječi: korporativna informacijska sigurnost, baze podataka, skladišta podataka, sigurnosne prijetnje, računalni oblaci

SUMMARY

Corporate security management covers all security segments of the business system: property security, contract security, administrative security, physical and technical security, staff security, business continuity security, fire protection, intellectual property protection, emergency operations, information security and other parts corporate security.

Information security today needs to be part of corporate management and corporate security. It includes IT components, but also non-IT information security components. For any business system, information is a fundamental business resource, its crucial asset.

Keywords: corporate information security, databases, data warehouse, security threats, cloud computing

Sadržaj

1. UVOD

Korporativno upravljanje sigurnošću obuhvaća sve sigurnosne segmente poslovnog sustava: sigurnost vlasništva, sigurnost ugovorenih poslova, administrativnu sigurnost, fizičku i tehničku sigurnost, sigurnost osoblja, sigurnost kontinuiteta rada, zaštitu od požara, zaštitu intelektualnog vlasništva, djelovanje u izvanrednim uvjetima, informacijsku sigurnost te još neke dijelove korporativne sigurnosti. Informacijska sigurnost danas treba biti dio korporativnog upravljanja i korporativne sigurnosti. Obuhvaća komponente informacijske tehnologije (IT), ali i komponente informacijske sigurnosti koji nisu IT. Za svaki poslovni sustav informacije su temeljni poslovni resurs, njegova krucijalna imovina. Bez obzira na veličinu i oblik poslovnih sustava (pripadnost javnom ili privatnom sektoru, profitnoj ili neprofitnoj orijentaciji), svi oni prikupljaju, obrađuju, pohranjuju i prenose informacije na više načina: elektronički, fizički i verbalno. Pri tome se informacije pojavljuju u mnogim oblicima: pisanim dokumentima, klasičnim i računalima podržanim bazama podataka, slikama, dijagramima, poslovnim pravilima, nalaze se na mnogobrojnim nositeljima. Budući da su temeljni resurs, imaju visoku poslovnu vrijednost. [1]

Cilj ovog rada je na osnovi dostupnih izvora te vlastitih iskustava i saznanja stečenih kroz školovanje i praksu, ukratko analizirati važnost informacijske sigurnosti te istražiti kako pravna regulativa definira pojam korporativne informacijske sigurnosti te kako obvezuje tvrtke na njezino provođenje.

Metodologija za pisanje ovog rada bila je analiza i istraživanje literature povezane sa informacijskom sigurnosti i poslovnim sustavima, te proučavanje mrežnih izvora s ciljem detaljnog pojašnjenja glavnih elemenata poslovne informacijske sigurnosti.

2. KORPORATIVNO UPRAVLJANJE I INFORMACIJSKA SIGURNOST

Informacijska sigurnost obvezatni je dio svakog korporativnog upravljanja. No, nepoznavanje odnosa između korporativnog upravljanja, korporativne sigurnosti, korporativnog upravljanja informatikom, korporativne informacijske sigurnosti i IT sigurnosti, može izazvati konfuziju. Zbog toga nekoliko slijedećih napomena nisu na odmet. Naročito značajne informacije su one o viziji, misiji, strategiji i strateškim ciljevima poslovnog sustava, informacije o poslovnim procesima čija bi degradacija ugrozila ostvarenje temeljnih poslovnih obveza, informacije o poslovnim procesima koje su posebno osjetljive i čije „curenje“ bi bilo nespojivo s prirodom konkretnog poslovnog sustava, informacije o poslovnim procesima koje, ukoliko se modificiraju, mogu imati vrlo negativne posljedice na ostvarenje misije poslovnog sustava, informacije o procesima kojima se ostvaruju zakonske, regulatorne ili ugovorne obveze. Također, vitalne informacije svakog poslovnog sustava su one o njegovoj strateškoj orijentaciji, načinu njegovog orijentacijskog funkcioniranja i pripadajućim odgovornostima, informacije o osoblju, osobito one čije bi odavanje ugrozilo privatnost, visokovrijedne druge informacije čije prikupljanje, pohranjivanje, obrada i prijenos imaju visoke troškove. Važne su i informacije o IT-u: instaliranoj računalnoj opremi, elektroničkim medijima, perifernoj opremi, sistemskoj programskoj opremi, korisničkim aplikacijama, telekomunikacijskim mrežama, IT zaposlenicima, lokacijama itd. Kao i kod drugih oblika poslovne imovine, postoje mnogobrojni izvori prijetnji od napada na informacijsku imovinu, koji, ukoliko se dogode, a ne postoji uspostavljena dovoljno dobra informacijska sigurnost, mogu izazvati velike neželjene posljedice. Skupine takvih prijetnji su: tehničke pogreške, neautorizirani pristupi IT opremi ili podacima, prekidi u pružanju IT potpore poslovnim procesima, prirodne nepogode, fizička oštećenja, kompromitiranje podataka i informacija i sl. [1]

Međutim, danas najveće prijetnje dolaze od ljudi – hakera, računalnih kriminalaca, terorista, industrijske špijunaže, nelojalnih vlastitih zaposlenika. Da li će se dogoditi negativne posljedice napada na informacijsku imovinu, ovisi od toga da li postoje adekvatne sigurnosne mjere i da li su one pravilno inkorporirane u cjelokupni sustav sigurnosti. Ukoliko je njihova razina nedovoljna, poslovni sustav je ranjiv i postoji rizik da će doći do ugrožavanja ove imovine. [1]

3. KLJUČNI ELEMENTI INFORMACIJSKIH SUSTAVA

3.1. Baze podataka

Modeliranje podataka je postupak izrade jedinstvenoga modela podataka i obavlja se tijekom procesa razvitka poslovnoga upravljačkoga informacijskoga sustava. Nastoje se razviti takvi modeli podataka u kojima će se što preciznije odražavati stvarni logički odnosi među podatcima, uz istodobno uspostavljanje njihove kontrolirane redundancije. Drugim riječima, pokušavaju se stvoriti takvi modeli podataka u kojima će se jedan podatak, ako je ikako moguće, pojavljivati samo na jednome mjestu u cjelokupnoj strukturi podataka poslovnoga informacijskoga sustava.

Ovisno o potrebama što se javljaju u pojedinim fazama razvitka poslovnoga informacijskoga sustava, razlikuju se tri vrste modela podataka:

1. Konceptualni modeli podataka
2. Logički modeli podataka
3. Fizički modeli podataka.

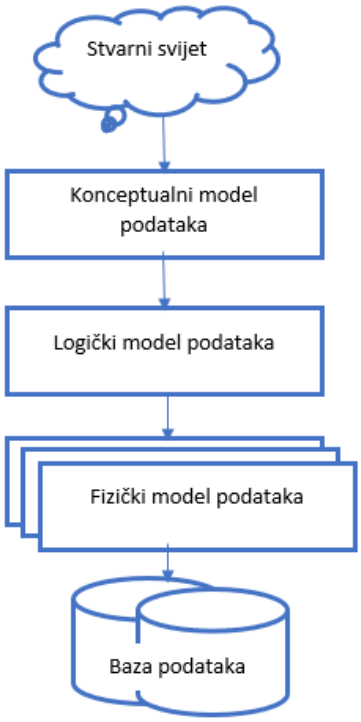
Konceptualni modeli podataka predstavljaju konceptualni opis stvarnih objekata pomoću entiteta opisanih osnovnim svojstvima - atributima.

Logičke modele podataka stvaraju i koriste stručnjaci informatičari (projektanti) kao osnovu za oblikovanje i razvitak novoga tipa organizacije podataka – baza podataka. Logički modeli opisuju odnose u koje dolaze pojedini entiteti unutar informacijskog sustava, što je uvjetovano funkcionalnim modelom informacijskog sustava. To je temelj za izradu programske podrške.

Fizički modeli podataka predstavljaju skup osnovnih tablica oslobođenih nepotrebnih redundancija, koje se pohranjuju (fizički) u bazu podataka, a prema potrebi će biti stavljane u odnose određene logičkim modelom informacijskog sustava.

Modeli podataka razvijaju se upravo navedenim redoslijedom: kao prvi stvaraju se konceptualni modeli, iz njih se izvode logički modeli, da bi se na kraju procesa razvili najkonkretniji - fizički modeli podataka.

Povezivanjem tih triju modela i njihovom implementacijom u elektroničko računalo nastaje konačni rezultat procesa modeliranja podataka - baza podataka kao dosada najuspješniji poznat oblik pohranjivanja podataka u računalu (ili računalima) poslovnih informacijskih sustava (Slika 1.).



Slika 1. Modeliranje podataka [2]

Baza podataka predstavlja skup datoteka, organiziranih na jednoobrazan (unificiran) način, te povezanih tako da uključuju minimalnu redundanciju podataka i omogućuju korisnicima pristup podatcima uz minimalna ograničenja. Dakle, koncept baze podataka izrasta (evoluira) iz koncepta datoteka podataka, odnosno predstavlja njegovo unaprjeđenje.

Jednoobraznost (unificiranost) strukture baze podataka ostvaruje se primjenom usklađenih (kompatibilnih) modela podataka na temelju kojih se strukturiraju datoteke što čine bazu podataka. Danas najčešće korišteni model je relacijski model, koji predstavlja modificirani oblik tablične organizacije podataka. Takav se model u praksi dokazao kao vrlo dobra osnova za izgradnju tzv. relacijske baze podataka (eng. *Relational Data Base*), kao skupa povezanih datoteka strukturiranih u obliku dvodimenzionalnih relacijskih tablica.

Relacijska se tablica sastoji od većega broja redaka - relacija - te od određenoga broja stupaca - atributa. Podatci u relacijskim tablicama se po potrebi mogu jednostavno reorganizirati poduzimanjem jedne ili više od triju mogućih relacijskih operacija: 1) selekcije; 2) projekcije; 3) spajanja (udruživanja).

Operacijom selekcije (eng. *Selection*), izdvajaju se iz relacijske tablice oni redci koji imaju zajedničku vrijednost nekoga odabranoga atributa, odnosno samo neki redci tablice i od njih se stvara nova relacijska tablica. Tako će se, primjerice, iz relacijske tablice svih studenata nekog fakulteta izdvojiti samo studenti 2. godine.

Operacijom projekcije (eng. *Projection*), izdvajaju se iz relacijske tablice neki postojeći atributi, odnosno stupci, koji više iz nekoga razloga nisu zanimljivi ili potrebni. Tablica se, dakle, reducira (sažima) po stupcima, čime nastaje nova, stupčano reducirana relacijska tablica.

Operacijom spajanja ili udruživanja (eng. *Join*), spajaju se dvije zasebne relacijske tablice preko zajedničkih vrijednosti atributa, čime nastaje nova relacijska tablica.

Sve se te operacije, koje mogu biti prilično složene, obavljaju sasvim jednostavnim naredbama odgovarajućega programskoga alata za rad s bazom podataka.[2] Općenito naredbe se izvode u standardnom upitnom jeziku (eng. *Structured Query Language*, SQL) kao primjenjivom u gotovo svim sustavima za upravljanje bazama podataka.

3.2. Skladište podataka

Koncept baze podataka pokazao se i dokazao u mnogim slučajevima kao izuzetno učinkovit način organiziranja podataka u računalu, odnosno njegovim memorijama. Skladišta podataka imaju sljedeća četiri obilježja:

1. usmjerenost predmetima (funkcionalnim područjima)
2. sadržajna nepromjenjivost
3. integriranost
4. vezanost uz vrijeme (vremenska određenost).

Predmetna usmjerenost znači da se podatci organiziraju oko predmeta, odnosno funkcionalnih područja (kao što je, primjerice, prodaja), a ne oko operativnih aplikacija (poput, primjerice, obrade narudžbi). Suprotno tome, operativne baze podataka organizirane su oko poslovnih aplikacija, pa su, dakle, usmjerene aplikacijama.

Sadržajna nepromjenjivost znači da se podatci koji su jednom pohranjeni u skladište podataka uglavnom ne mijenjaju. Svatko tko koristi skladište podataka može biti siguran da će njegov upit rezultirati jednakim odgovorom, neovisno o tome kada i kako često ga postavljao. Operativne baze podataka u sadržajnom su smislu izrazito promjenjive, pa je malo vjerojatno da će istovjetan upit ponovljen dva puta proizvesti isti odgovor, jer će u međuvremenu sadržaj takve baze podataka biti ažuriran, dakle, izmijenjen.

Integriranost znači da su podatci konzistentni, odnosno da se prikazuju na dosljedan način. Tako se, primjerice, datumi uvijek pohranjuju u istome formatu. Integracija je problem u mnogim tvrtkama, a posebno u onima koje koriste različite tehnologije za rukovanje podatcima. Zato se, prije unosa u skladište podataka, podatci moraju integrirati. U tome smislu, integracija predstavlja proces kojim se podatci podvrgavaju nakon što "napuste" aplikacijsku bazu podataka, a prije no što "uđu" u skladište podataka.

Vezanost uz vrijeme (vremenska određenost) znači da se u skladištu podataka pohranjuju povijesni (historijski) podatci. Gotovo sa svim upitima što se upućuju skladištu podataka povezan je neki vremenski element. U operativnim se bazama podataka, suprotno tome, ne pohranjuju povijesni, već samo aktualni (najsvježiji, najažurniji) podatci. Razlog zbog kojega se u skladištu podataka pohranjuju povijesni podatci jest taj što se predviđanje budućih događaja i procesa ne može izvršiti vjerodostojno bez poznavanja povijesti tih, a možda i nekih drugih, činjenica, događaja i procesa. Može se, dakle, zaključiti da su skladišta podataka usmjerena budućnosti, premda njihov sadržaj odražava prošlost. Mjesto skladišta podataka u okviru informacijskog sustava poduzeća prikazano je na Slici 2. [2]

Slika 2. Mjesto skladišta podataka u okviru informacijskog sustava poduzeća [2]

3.2.1. Mjesto i funkcije skladišta podataka u informacijskome sustavu poduzeća

Skladište podataka u informacijskome sustavu poduzeća je mjesto na kojemu se skupljaju i pohranjuju poslovni podatci, ali isto tako i izvor informacija koje će se koristiti u odlučivanju i pri stvaranju tzv. poslovne inteligencije (eng. *Business Intelligence*).[2]

Primarne funkcije skladišta podataka su sljedeće:

- Skladište podataka je odraz poslovnih pravila što se primjenjuju u poduzeću - ne samo na razini pojedine poslovne funkcije ili organizacijske jedinice - prilikom donošenja strateških poslovnih odluka. Skladište podataka mora biti oblikovano tako da se može brzo i jednostavno prilagođavati promjenama u poslovnim pravilima, što uključuje sposobnost prihvaćanja novih podataka, kao i promjena u hijerarhijskim i, općenito, logičkim odnosima među podatcima.
- Skladište podataka predstavlja točku u kojoj se skupljaju podatci koji će poslužiti za stvaranje integriranih, predmetno usmjerenih informacija. Zato pri modeliranju skladišta podataka treba primijeniti neku od tehnika koje podržavaju predmetnu orijentaciju i osiguravaju dovoljnu prilagodljivost kako bi se s vremenom mogli integrirati i podatci što proizlaze iz nekih dodatnih izvora.
- Skladište podataka je "muzej" strateških informacija, čija se povijest može povezati s podatcima i s odnosima među njima. Ova funkcija skladišta podataka iziskuje primjenu tehnike modeliranja koja omogućuje jednostavnu ugradnju povijesne perspektive u pohranjeni sadržaj.
- Skladište podataka je izvor stabilnih podataka, neovisnih o možebitnim promjenama u procesima. Iz toga izrasta potreba za modelom neosjetljivim na utjecaje operativnih poslovnih procesa koji stvaraju podatke.

To su, kao što je naglašeno, primarne funkcije skladišta podataka. Premda u dizajnu skladišta podataka ne smije biti nikakvih elemenata koji bi otežavali ili čak onemogućavali postavljanje upita, odgovaranje na upite koji iziskuju brz odgovor nije primarna već sekundarna funkcija skladišta podataka. Drugim riječima, skladište podataka ne mora nužno biti brzo u odgovaranju na upite, tako da naglasak pri oblikovanju ne treba biti na njegovoj brzini obavljanja takvih zadataka, jer je to zadaća nekih drugih softverskih sustava i alata. Za skladište podataka važno je da bude vjerodostojno, pouzdano i stabilno. [2]

Skladište bi podataka trebalo udovoljavati mnogim zahtjevima. Među njima se posebno ističu sljedeći:

1. U njemu mora biti sadržana velika količina detaljnih podataka. Poduzeće mora imati pregled nad svime što se zbivalo tijekom njegovog rada i poslovanja u prošlosti, kako bi moglo odrediti svoje postupke u sadašnjosti i u budućnosti.
2. Skladište podataka treba kontinuirano nadopunjavati, tj. osvježavati podatcima o izvršenim poslovnim transakcijama. Nema tome dugo da se mjesečno ažuriranje podataka smatralo zadovoljavajućim, ali tempo suvremenoga poslovanja to više ne može tolerirati. Danas je čak i dnevno ažuriranje često neprihvatljivo, pa se osvježavanje podataka nastoji, kadgod je to moguće, provoditi u stvarnome vremenu, tj. odmah nakon što se neki poslovni događaj zbio ili nakon što je neki proces završio.
3. Skladište podataka mora služiti velikom broju ljudi - menadžerima i zaposlenicima poduzeća, njegovim klijentima i poslovnim partnerima. Zato treba osigurati jednostavne i učinkovite postupke pristupanja sadržaju skladišta podataka i njegove uporabe u svim segmentima poslovanja.
4. Neki od zaposlenika željet će postavljati upite i pretraživati čitavo skladište podataka kako bi došli do nekih zaključaka, i to žurno. Nije dobro pokušavati predvidjeti u koje će sve svrhe skladište podataka biti korišteno - treba ga oblikovati tako da ono može poslužiti svakoj, možda i sasvim nepredvidivoj, unaprijed nepoznatoj svrsi.
5. Skladište podataka mora biti uvijek raspoloživo. Poduzeće si ne smije dopustiti "luksuz" da ono gdjekad ne bude dostupno onome kome je potrebno, jer ta osoba tada neće moći obaviti svoj posao, primjerice, pružiti odgovarajuću uslugu klijentu ili klijentima i može se dogoditi da ih poduzeće zbog toga zauvijek izgubi.
6. Skladište podataka mora biti proširivo. Ako je strategija poduzeća širenje poslovanja i povećanje tržišnoga udjela - a trebala bi biti takva - onda i skladište podataka mora pratiti tu strategiju. Uz to, poslovne aktivnosti i kampanje bivaju s vremenom sve suptilnije i sofisticiranije, a skladište podataka ih mora podržavati sve kvalitetnijim, a to obično znači i brojnijim i detaljnijim informacijama. Praksa pokazuje kako nisu rijetki primjeri da se obujam skladišta podataka udvostručuje u razdoblju od samo 18 mjeseci.

7. Valja poduzeti rigorozne mjere zaštite cjelovitosti i tajnosti osjetljivih podataka pohranjenih u skladištu, kako oni ne bi bili dostupni neovlaštenim korisnicima. Time će se poduzeće zaštititi od zlouporaba podataka iz skladišta podataka koje mogu biti izvorom značajnih materijalnih i nematerijalnih šteta i gubitaka.

Ukratko, skladište podataka je "zlatni rudnik" informacija, pa predstavlja moćno sredstvo za upravljanje poslovanjem uopće, a posebice odnosima s klijentima. Da bi svi njegovi potencijali mogli biti u potpunosti iskorišteni, prilikom njegova uspostavljanja, implementacije i korištenja treba se čvrsto pridržavati navedenih sedam zahtjeva. [2]

3.3. Razlika između baze podataka i skladišta podataka

- Baza podataka je skup povezanih podataka koji predstavljaju neke elemente iz stvarnog svijeta, dok je skladište podataka informacijski sustav koji pohranjuje povijesne i komutativne podatke iz jednog ili više izvora (Tablica 1.).
- Baza podataka dizajnirana je za bilježenje podataka, dok je skladište podataka dizajnirano za analizu podataka.
- Baza podataka orijentirana je na aplikacijsko prikupljanje podataka, dok je skladište podataka predmetno orijentirano prikupljanje podataka.
- Baza podataka koristi internetsku transakcijsku obradu (eng. *Online transaction processing*, OLTP), dok skladište podataka koristi mrežnu analitičku obradu (eng, *Online Analytical processing*, OLAP).
- Tablice i spajanja baza podataka složeni su jer su normalizirani, dok su tablice i spajanja skladišta podataka jednostavne jer su denormalizirane.
- Tehnike modeliranja odnosa entiteta koriste se za dizajniranje baze podataka, dok se tehnike modeliranja podataka koriste za dizajniranje skladišta podataka. [3]

Tablica 1. Razlike između baze podataka i skladišta podataka [3]

Parametar	Baza podataka	Skladište podataka
Svrha	Dizajnirana za snimanje	Dizajnirano za analizu
Metoda obrade	Baza podataka koristi internetsku transakcijsku obradu (OLTP)	Skladište podataka koristi internetsku analitičku obradu (OLAP)
Upotreba	Baza podataka pomaže u obavljanju osnovnih operacija u poslovanju	Skladište podataka omogućuje analizu poslovanja
Tablice i spojevi	Tablice i spojevi baze podataka složeni su jer su normalizirani	Tablica i spajanja jednostavna su u skladištu podataka jer su denormalizirana
Orijentacija	Aplikacijski orijentirana	Predmetno orijentirana
Ograničenje pohrane	Općenito ograničeno na jednu aplikaciju	Pohranjuje podatke iz bilo kojeg broja aplikacija
Dostupnost	Podaci su dostupni u stvarnom vremenu	Podaci se osvježavaju iz izvornih sustava prema potrebi
Tehnika	Snimanje podataka	Analiziranje podataka
Vrsta podataka	Podaci pohranjeni u bazi podataka su ažurni	Trenutni i povijesni podaci pohranjuju se u skladište podataka
Vrsta upita	Koriste se jednostavni upiti za transakcije	U svrhu analize koriste se složeni upiti

Zašto koristiti bazu podataka?

1. Nudi sigurnost podataka i njihov pristup (Tablica 2.).
2. Baza podataka nudi razne tehnike za pohranu i dohvat podataka.
3. Baza podataka djeluje kao učinkovit rukovatelj za uravnoteženje zahtjeva više aplikacija koji koriste iste podatke.
4. Sustav za upravljanje bazama podataka nudi ograničenja integriteta kako bi se postigla visoka razina zaštite kako bi se spriječio pristup zabranjenim podacima.
5. Baza podataka omogućuje vam pristup istodobnim podacima na takav način da istodobno istim podacima može pristupiti samo jedan korisnik. [3]

Tablica 2. Upotreba baza podataka [3]

Sektor	Upotreba
Bankarstvo	Upotreba u bankarskom sektoru za informacije o klijentima, aktivnosti povezane s računom, plaćanja, depozite, zajmove, kreditne kartice itd.
Zrakoplovne kompanije	Koristi se za informacije o rezervacijama i rasporedu.
Sveučilišta	Za pohranu podataka o studentima.
Telekomunikacije	Pomaže u pohrani evidencije poziva, mjesečnih računa, održavanja stanja itd.
Financije	Pomaže u skladištenju informacija vezanih uz zalihe, prodaju i kupnju dionica i obveznica.
Prodaja	Koristi se za pohranu podataka o kupcu, proizvodu i prodaji.
Proizvodnja	Koristi se za upravljanje podacima lanca opskrbe, za praćenje proizvodnje i stanja zaliha.
Ljudski resursi	Pojedinosti o plaćama zaposlenika, odbitcima, generiranju plaća itd.

Zašto koristiti skladište podataka?

1. Skladište podataka pomaže poslovnim korisnicima da pristupe kritičnim podacima iz nekih izvora na jednom mjestu (Tablica 3.).
2. Pruža dosljedne informacije o raznim višefunkcionalnim aktivnostima.
3. Pomaže u integraciji mnogih izvora podataka kako biste smanjili opterećenje na proizvodnom sustavu.
4. Skladište podataka pomaže vam smanjiti ukupno vrijeme obrade za analizu i izvještavanje.
5. Skladište podataka pomaže korisnicima da pristupe kritičnim podacima iz različitih izvora na jednom mjestu, tako da štedi vrijeme korisnika za preuzimanje podataka iz više izvora. Također možete lako pristupiti podacima iz oblaka.
6. Skladište podataka omogućuje vam pohranu velike količine povijesnih podataka kako biste analizirali različita razdoblja i trendove za buduća predviđanja.
7. Povećava vrijednost operativnih poslovnih aplikacija i sustava upravljanja odnosima s kupcima.
8. Odvaja analitičku obradu od transakcijskih baza podataka, poboljšavajući izvedbu oba sustava.
9. Dionici i korisnici možda precjenjuju kvalitetu podataka u izvornim sustavima. Skladište podataka pruža preciznija izvješća. [3]

Tablica 3. Upotreba skladišta podataka [3]

Sektor	Upotreba
Bankarstvo	Koristi se u bankarskom sektoru za učinkovito upravljanje resursima dostupnim na radnom mjestu.
Zrakoplovne kompanije	Koristi se za operacije upravljanja zrakoplovnim sustavima poput dodjele posade, analiza rute i programa popusta.
Zdravstvo	Skladište podataka koristi se za strategiju i predviđanje ishoda, izradu izvještaja o liječenju pacijenta itd..
Osiguranje	Skladišta podataka široko se koriste za analizu obrazaca podataka, trendova kupaca i brzo praćenje kretanja na tržištu.
Maloprodaja	Pomaže u praćenju predmeta, prepoznavanju uzorka kupca, promocijama i također se koristi za određivanje cijena.
Telekomunikacije	U ovom sektoru skladište podataka koristi se za promociju proizvoda, odluke o prodaji i donošenje odluka o distribuciji.

4. RAZVOJ RAČUNALNIH OBLAKA

Razvojem informacijskih tehnologija na tržištu se neprekidno javlja potreba za inovacijama i unaprjeđenjem trenutnog stanja informacijskih sustava. Upravo ta težnja za inovacijama dovela je do nastanka računalstva u oblaku. Napretkom računalnih i telekomunikacijskih tehnologija poboljšane su mogućnosti prijenosa, pohrane, zaštite, obrade i sigurnosti podataka.

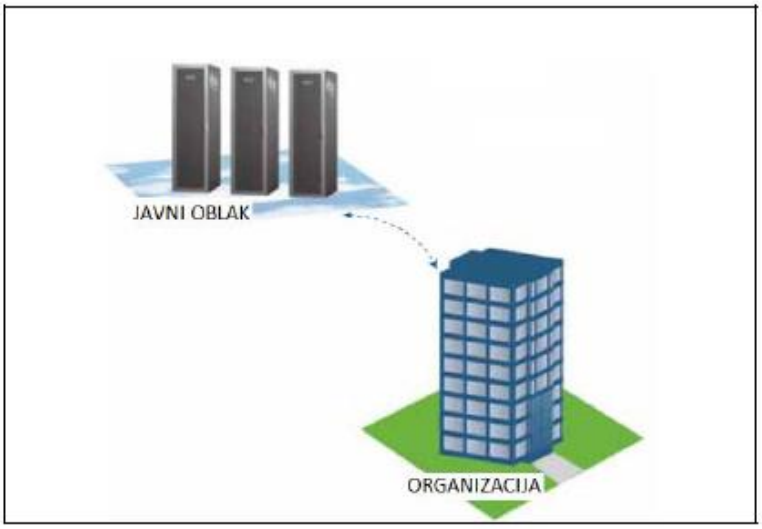
Računalstvo u oblaku može se definirati kao mogućnost iznajmljivanja virtualnog poslužitelja. Korisnici na virtualnom poslužitelju mogu pohranjivati podatke i po volji im pristupati. Računalstvo u oblaku može se definirati i s obzirom na to koriste li ga stručnjaci ili obični korisnici. Obični korisnici će računalstvo u oblaku definirati kao novi i jeftiniji način korištenja programskih rješenja koja će se unajmljivati prema potrebi. Informatički stručnjaci definirati će ga kao novi poslovni model ili novu tehnološku platformu za smještaj, pokretanje i korištenje informatičke programske podrške. [4]

4.1. Modeli izvedbe

4.1.1. Javni oblak

Platforma računalnih oblaka dostupna i otvorena za javnost, neovisno o tome radi li se o pojedincima ili organizacijama. U vlasništvu je tvrtke koja prodaje usluge računalnih oblaka. U slučaju javnih platformi postavlja se pitanje sigurnosti vlastitih podataka. Aplikacije različitih korisnika često se nalaze na istim poslužiteljima, sustavima za pohranjivanje i mrežama. Javni oblaci smanjuju sigurnosne rizike i troškove pružanjem promjenjive infrastrukture. Oni čine privremeno zakupljenu infrastrukturu organizacija. Ako je javni oblak realiziran s pažnjom usmjerenom na izvedbu, sigurnost i položaj podataka druge aplikacije pokrenute na oblaku ne bi trebale stvarati probleme prema arhitekturi oblaka i krajnjim korisnicima. Jedna od prednosti javnih oblaka je da oni mogu biti puno veći nego što mogu biti privatni oblaci. [4]

Javni oblaci (Slika 3.) nude mogućnost povećavanja ili smanjivanja zakupljenog dijela oblaka i prebacivanje odgovornosti, ako se pojave neplanirani rizici, s organizacija na davatelja usluga. Dijelovi javnog oblaka mogu biti i pod isključivom uporabom samo jednog korisnika, čineći tako privatni podatkovni centar (eng. *datacenter*). Zauzimanje tzv. slika virtualnih strojeva (eng. *virtual machine images*) u javnom oblaku ne daje korisnicima potpuni uvid u infrastrukturu oblaka, dok zakupljivanje podatkovnih centara daje korisnicima veći uvid u samu infrastrukturu. Tada korisnici mogu upravljati ne samo sa slikama virtualnih strojeva, nego i poslužiteljima, sustavima pohrane, mrežnim uređajima i mrežnim topologijama. Stvaranje privatnog virtualnog podatkovnog centra s komponentama koje se nalaze u istom objektu smanjuje problem postojanja mnoštva različitih lokacija podataka zato što je brzina prijenosa puno veća pri povezivanju objekata unutar istog oblaka. [4]



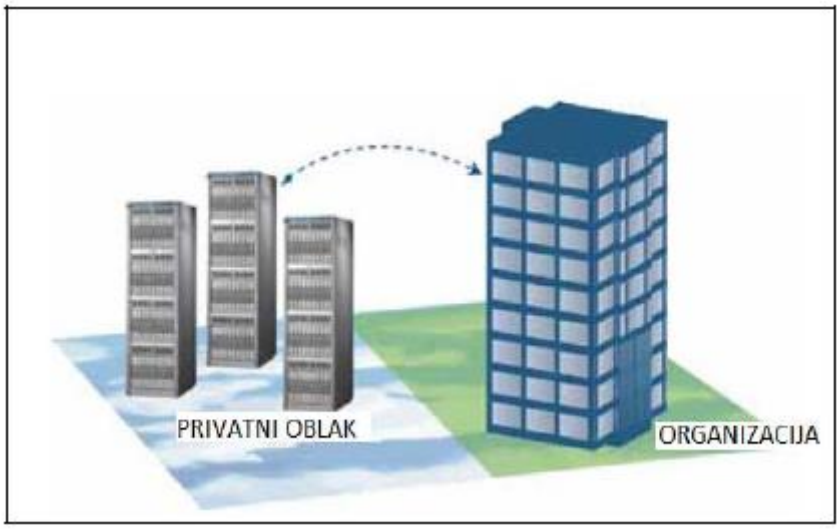
Slika 3. Javni oblak [4]

4.1.2. Privatni oblak

Infrastruktura računalnih oblaka dostupna je isključivo jednoj organizaciji. Njome može upravljati sama organizacija ili netko drugi. Organizacije koriste privatne oblake kada trebaju ili žele veći nadzor nad podacima nego što ga mogu imati korištenjem javnog oblaka. Privatni oblaci su napravljeni isključivo za uporabu jednog klijenta, pružajući mu najveći nadzor nad podacima i najveću sigurnost imovine

pohranjene na oblaku. Organizacija posjeduje infrastrukturu i ima nadzor nad raspodjelom aplikacija na vlastitoj infrastrukturi.

Privatni oblaci (Slika 4.) mogu biti raspoređeni i unutar organizacijskog podatkovnog centra. IT službe kompanija ili davatelji usluga grade privatne oblake i upravljaju njima. Organizacije koje posjeduju privatni oblak na njemu mogu instalirati programe, aplikacije, pohranjivati podatke i upravljati strukturom oblaka. Također, privatni oblaci pružaju kompanijama visoku razinu nadzora nad korištenjem resursa oblaka jer korištenjem privatnog oblaka organizacije imaju potrebne vještine i mogućnosti za uspostavljanje i upravljanje okolinom. [4]



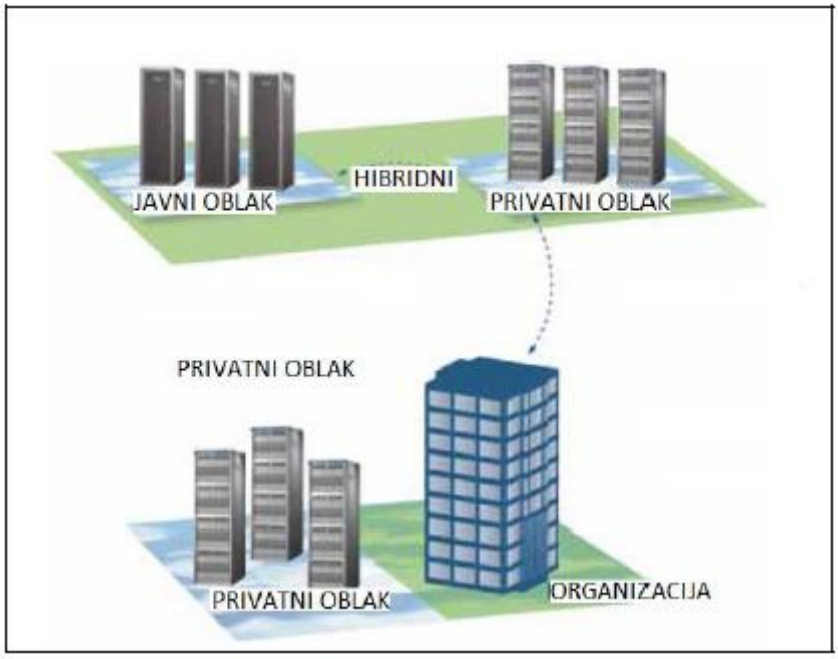
Slika 4. Privatni oblak [4]

4.1.3. Zajednički oblak

Nekoliko organizacija dijeli strukturu oblaka. Infrastruktura podržava posebne zajednice koje imaju zajedničke potrebe, misije, zahtjeve sigurnosti i slično. Njima mogu upravljati same organizacije ili netko drugi (pružatelj usluga računalnih oblaka).[4]

4.1.4. Hibridni oblak

Strukturu oblaka čine dva ili više različitih oblaka (privatni, zajednički ili javni) koji ostaju jedinstveni entiteti, ali su međusobno povezani standardiziranim ili prikladnim tehnologijama koje omogućavaju efikasan prijenos podataka ili aplikacija. Hibridni oblaci povezuju javne i privatne modele oblaka (Slika 5.). Mogućnost proširivanja privatnog oblaka s resursima javnog oblaka može se koristiti za održavanje uslužnih razina kako bi se lakše izdržala velika opterećenja. To se najčešće može vidjeti kod uporabe oblaka za pohranu podataka kako bi podržali Web 2.0 aplikacije. Hibridni oblak se također može koristiti za upravljanje planiranim velikim opterećenjima. Privatni oblaci mogu se koristiti za izvođenje periodičkih zadataka koji se jednostavno raspoređuju na javne oblake. Hibridni oblaci susreću se sa složenosti određivanja kako raspodijeliti aplikacije po javnom i privatnom oblaku. Pokraj ovog problema u obzir se mora uzeti i odnos između podataka i obrade resursa. Ako su podaci mali ili aplikacije ne pamte stanja, hibridni oblak može biti bolje rješenje od prepisivanja velike količine podataka u javni oblak (u kojem se izvodi jednostavna obrada). [4]



Slika 5. Hibridni oblak [4]

Uslijed povećavanja zahtjeva korisnika i prilika na tržištu pojavljuje se potreba za uvođenjem novih modela računalnih oblaka. Primjer toga je i nedavno pojavljivanje privatnog oblaka (eng. *Private colud*) – načina upotrebljavanja infrastrukture javnog oblaka za privatne ili poluprivatne potrebe i povezivanje tih resursa s unutarnjim resursima korisničke baze podataka. Uobičajeno se to postiže povezivanjem korisnika u privatnu virtualnu mrežu (eng. *virtual private network*). Kod dizajniranja oblaka dizajneri trebaju paziti na arhitekturalno razmještanje podataka. Način razmještaja podataka ima velik utjecaj na buduću prilagodljivost, sigurnost i mobilnost rezultirajućeg rješenja. [4]

4.2. Usluge računalstva u oblaku

- **SaaS** (eng. *Software as a Service*) - Oblik računalnog oblaka koji preko preglednika dostavlja jednu aplikaciju mnoštvu korisnika. Korištenjem ovog modela korisnici ne moraju investirati u nove poslužitelje i licencirane programe. Troškovi davatelja usluga su pri tome manji u odnosu na tradicionalnu uslugu čuvanja podataka na poslužitelju.

- **Uslužno računalstvo** (eng. *Utility computing*) - Uslužno računalstvo je relativno nova forma na tržištu informacijskih tehnologija. Koriste ju Amazon, Sun, IBM i drugi koji nude uslugu pohrane virtualnih poslužitelja kojima se pristupa na zahtjev korisnika. Pružatelj usluga osigurava računalne resurse i infrastrukturu korisniku prema potrebi. U budućnosti bi ovaj model mogao zamijeniti dio baza podataka jer korisnici uz pomoć tehnologije računalnih oblaka mogu pohranjivati mnoštvo podataka na virtualnim poslužiteljima. Druge organizacije pružaju rješenja koja pomažu korisnicima u stvaranju virtualnih baza podataka.[4]

- **Web usluge u oblaku** (eng. *Web services in the cloud*) - Web usluge su usko povezane sa SaaS modelom. Organizacije koje pružaju web usluge nude sučelja (eng. *application programming interface*) koja razvojnim inženjerima omogućuju iskorištavanje funkcionalnosti preko interneta. Web usluge mogu imati veliki raspon, pa tako sežu od diskretnih poslovnih usluga (poput Strike Iron i Xignite), pa sve do jako dobro razvijenog sučelja, koje se može pronaći kod Google Mapsa, automatske obrade podataka nakon plaćanja te standardnih usluga obrade kreditnih kartica.

- **PaaS** (eng. *Platform as a service*) – PaaS je još jedna inačica SaaS modela. Ovaj model računalnog oblaka kao uslugu pruža razvojnu okolinu. Korisnik gradi vlastite aplikacije koje se pokreću na infrastrukturi davatelja usluge, te putem preglednika dostavljaju korisniku.

- **MSP** (eng. *managed service providers*) – MSP je jedan od najstarijih oblika računalnih oblaka. Upravljana usluga je aplikacija namijenjena IT službi, a ne krajnjem korisniku. Primjer je usluga skeniranja zloćudnih programa koji se šire porukama elektroničke pošte ili usluge upravljanja aplikacijama (na primjer tu uslugu pruža Mercury).

- **Usluge komercijalnih platformi** (eng. *Service commerce platforms*) - Ove su platforme hibrid SaaS i MSP modela. Usluga komercijalnih platformi nudi čvorište (eng. *hub*) s kojim korisnici komuniciraju. Najčešće se upotrebljava u web trgovinama, poput skupih upravljačkih sustava koji korisnicima dozvoljavaju naručivanje mobilnih usluga zajedničkih platformi. Platforme tada koordiniraju pružanje usluga određivanjem cijene unutar specifikacija koje je postavio korisnik. Poznati primjeri davatelja ove usluge su Rearden Commerce i Ariba.[4]

- **Integracija interneta** (eng. *Internet integration*) - Danas je integracija usluga računalnih oblaka i dalje u svojim ranim fazama. Način međusobnog povezivanja zasnovan na oblaku bi se možda trebao nazivati *sky computing* s mnoštvom izoliranih oblaka na koje se korisnici individualno moraju spajati. S druge strane kako sve više organizacija primjenjuje virtualizaciju i SOA arhitekturu (eng. *Serviceoriented architecture*), povećava se potreba za dobro povezanim uslugama koje se nalaze na internetu. Ideja podesive infrastrukture je da se jednog dana svakoj organizaciji napravi čvor u oblaku.[4]

Postoji pet ključnih karakteristika koje pokazuju odnos i razlike sustava računalnih oblaka u odnosu na tradicionalni pristup u računalstvu. Tih pet ključnih karakteristika su:

Pružanje usluge na zahtjev korisnika (eng. *On-demand self-service*) - Korisnik može samostalno odabrati i pokrenuti računalne resurse. Može birati vrijeme posluživanja i mrežni prostor za pohranu podataka bez potrebe za interakcijom s djelatnicima pojedinog davatelja usluge. U principu, danas većina poslužitelja svoje usluge temelji upravo na pristupu da korisnici plaćaju usluge u ovisnosti o vremenu i obujmu u kojem ih koriste. Ovaj model računalnih oblaka pomaže u podržavanju izvedbenih i kapacitivnih aspekata objekata koji ovise o razini usluge. *Self-service* priroda računalnih oblaka organizacijama omogućuje stvaranje elastične okoline koja se povećava i smanjuje ovisno o radnim uvjetima i ciljanim performansama. „Plati po korištenju“ priroda računalnih oblaka se može smatrati kao najam opreme koja se plaća ovisno o tome koliko je opreme, na koje vrijeme i s kojim uslugama iznajmljeno. Virtualizacija je ključ ovoga modela. Organizacije koje koriste informacijske tehnologije shvaćaju da im virtualizacija omogućava brzo i jednostavno stvaranje kopija postojećih okolina, ponekada uključujući više virtualnih strojeva kako bi podržala ispitivanja, razvoj i pohranu aktivnosti. Trošak ovih okolina je jako malen jer one mogu postojati na istom poslužitelju kao proizvodna okolina. Isto tako, nove aplikacije se mogu razvijati i rasprostirati u novim virtualnim strojevima na postojećim fizičkim poslužiteljima, otvorenima za uporabu preko interneta. [4]

Aplikacije mogu biti skalirane, ako su uspješne na tržištu. Mogućnost korištenja i plaćanja samo onih resursa koji su korišteni prebacuje rizik koliko infrastrukture zauzeti od organizacije koja razvija aplikaciju na davatelja usluga računalnih oblaka. Također pomiče i odgovornost za arhitekturalne odluke s arhitekata aplikacije na razvojne inženjere. Ovi pomaci odgovornosti mogu povećati rizike. [4]

Širok mrežni pristup (eng. *Broad network access*) - Mogućnosti su dostupne putem mreže i njima se pristupa koristeći standardne mehanizme koji promoviraju heterogenu uporabu „tankih“ i/ili „bogatijih“ klijentskih platformi (na primjer, mobilni uređaji i laptopi) kao i tradicionalnih programskih usluga temeljenih na „oblaku“. Ovo je vrlo blisko Microsoftovoj P+U/program+usluga (eng. *S+S / softwafe+service*) strategiji (ideja je da se bilo koji uređaj može spojiti na sustav od bilo kuda).

Udruživanje resursa (eng. *Resource pooling*) - Računalni resursi pružatelja usluga spajaju se kako bi poslužili sve korisnike koristeći model više zakupljenih jedinica (eng. *Multi-Tenant model*), s različitim fizičkim i virtualnim resursima, koji se dinamički dodjeljuju i uklanjaju prema zahtjevima korisnika. Korisnik uobičajeno nema nadzor i znanje o točnom mjestu uporabljenih resursa, ali ipak ga može odrediti na većoj razini apstrakcije (na primjer na razini države). Primjeri resursa uključuju mrežni prostor, procesore, memoriju, mrežnu propusnost te virtualne strojeve.

Brza elastičnost (eng. *Rapid elasticity*) - Mogućnosti koje korisnicima nude računalni oblaci mogu biti ubrzano i elastično pokrenute, u nekim slučajevima i automatski, kako bi se po potrebi ostvarilo proporcionalno povećanje ili smanjenje mogućnosti kada one više nisu potrebne. Krajnjem korisniku mogućnosti koje koristi mogu izgledati kao da nemaju ograničenja i mogu se kupiti u bilo kojoj količini u bilo koje vrijeme. [4]

Odmjerena usluga (eng. *Measured service*) - Sustavi koji koriste računalne oblake automatski provjeravaju i optimiraju uporabu resursa. Uporaba resursa se optimira utjecajem na mjerenje sposobnosti apstrakcije prikladne potrebnom tipu usluge (na primjer pohrana podataka, širina pojasa, aktivni korisnički računi). Uporaba resursa se može pratiti, provjeravati i o njoj se mogu raditi izvješća pružajući tako transparentan uvid davateljima usluge i korisnicima. Važno je primijetiti da se računalni oblaci često (ali ne uvijek) koriste zajedno s virtualizacijskim tehnologijama. Međutim, ne postoje zahtjevi koji usko povezuju apstrakciju sredstava i virtualizacijske tehnologije pa se u mnogim ponudama virtualizacija operacijskih sustava ipak ne koristi. [4]

4.3. Ekonomski aspekt

Korištenjem računalnih oblaka moguće je izbjeći velike troškove kupnje skupih sklopovlja, programa i usluga. Korisnici usluga računalnih oblaka plaćaju samo ono što koriste. Uglavnom ne postoje zahtjevi za plaćanje unaprijed, a troškovi su jako mali u odnosu na korištenje vlastite IT infrastrukture. Ovaj pristup organizaciji IT rješenja korisnicima nudi jednostavan pristup podacima i mnoštvu različitih aplikacija. Druge prednosti ovoga pristupa su podijeljena infrastruktura i niski troškovi nadzora. Općenito, korisnici uvijek mogu raskinuti ugovor gdje su usluge često pokrivene sporazumima o razmjeni usluga s financijskim kaznama. Korištenjem računalnih oblaka organizacije mogu uštedjeti na kapitalnim troškovima, ali s druge strane pri korištenju računalnih oblaka organizacije moraju biti jako oprezne. Ovisno o potrebama organizacije, troškovi usluge mogu biti i jako skupi, pa korištenje računalnih oblaka ne mora dovesti do velikih financijskih ušteda. U situacijama kada bi glavni troškovi bili relativno mali, ili kada organizacija ima veću fleksibilnost u svom osnovnom proračunu nego u operacijskom proračunu model računalnih oblaka i nema nekog velikog financijskog smisla. Drugi faktori koji utječu na bilo koje druge potencijalne uštede uključuju učinkovitost organizacije baze podataka pojedine organizacije u usporedbi s oblakom nekog dobavljača, postojeće troškove organizacije, razinu prihvaćanja računalnih oblaka i tip funkcionalnosti koju oblak posjeduje. [4]

4.4. Arhitekture u oblaku

Arhitektura programskih sustava uključenih u računalne oblake tipično uključuje višestruku međusobnu komunikaciju komponenata oblaka. Komunikacija se obavlja preko aplikacijskog programskog sučelja, uobičajeno preko web poslužitelja. Ovo približno sliči tzv. Unix filozofiji posjedovanja više programa od kojih svaki dobro radi jednu stvar, a zajedno rade povezani preko univerzalnih sučelja. Arhitekture računalnih oblaka rješavaju nekoliko ključnih problema koji su bitni za obradu velike količine podataka. U tradicionalnoj obradi podataka teško je dobiti toliko računala koliko je pojedinoj aplikaciji potrebno. Također, teško je dobiti potrebna računala u trenutku kada su potrebni. Pojavljuju se mnoge poteškoće u raspodjeli i koordiniranju mnoštva poslova na različitim sustavima, pokretanju procesa na njima i osiguravanju alternativnih rješenja (npr. rezervno računalo) u slučaju da jedan od korištenih zakaže. Teško je automatski procijeniti poraste i padove dinamičkog opterećenja. Arhitektura računalnih oblaka rješava sve te probleme. Aplikacije izgrađene na arhitekturi računalnih oblaka pokreću se u oblaku gdje fizičko mjesto infrastrukture određuje davatelj usluge. Oni iskorištavaju jednostavna programska sučelja (eng. *application programming interface*) dostupnih usluga na internetu. Raspoređivanje se izvodi na zahtjev, a logika raspodjele i pouzdana logika usluga ostaje implementirana i skrivena u oblaku. Korištenje resursa u arhitekturi računalnih oblaka je, po potrebi, ponekada kratkotrajno, a ponekada se javlja više puta, ali s određenim razmacima. Zbog toga je ova arhitektura jako iskoristiva i optimalna. Kako bi razvojni inženjeri iskoristili što više prednosti računalnih oblaka moraju biti u mogućnosti reorganizirati aplikacije. Aplikacije se reorganiziraju tako da najbolje iskoriste arhitekturalne i razvojne paradigme koje računalni oblak podržava. Prednosti iskorištavanja aplikacija korištenjem arhitekture računalnih oblaka uključuju smanjivanje vremena odziva, minimalizaciju rizika, smanjivanje troškova pristupa, povećavanje brzine inovacija i mnoge druge. [4]

Prednosti gradnje aplikacija uz pomoć arhitekture računalnih oblaka su:

Smanjivanje vremena izvođenja i vremena odziva - Aplikacijama koje u suštini koriste oblake za izvršavanje mnoštva različitih poslova, omogućuju izvođenje na mnoštvu različitih poslužitelja. Na primjer, izvođenje se može omogućiti na 1000 poslužitelja i tako ubrzavati obavljanje posla. Obrada na takav način može biti gotova za 1/1000 vremena koje bi bilo potrebno jednom poslužitelju. Neki korisnici na vlastitom CPU (eng. *Central Processing Unit*) ne mogu izvršiti određene zadatke, pa se tada odlučuju za korištenje računalnih oblaka. Korištenjem računalnih oblaka korisnici imaju pristup aplikacijama koje im mogu ponuditi brzo vrijeme odziva, jer se korisnički zahtjev obrađuje na mnoštvu virtualnih strojeva. Izvođenje zadatka na virtualnom stroju može optimirati vrijeme odziva raspodjelom poslova na zahtjev korisnika.

Gotovo ne postoji plaćanje infrastrukture unaprijed - Ako korisnik mora izgraditi veliki sustav, a želi ga izgraditi u potpunosti u svojem vlasništvu, to ga može jako puno koštati u startu. Korisnik bi tada morao investirati u sklopovlje (sklopovi, napajanja, usmjernici i dr.), upravljanje sklopovljem (upravljanje napajanjem, hlađenjem) i u operacijsko osoblje. Zbog velikih troškova organizacija bi trebala nekoliko odobrenja od uprave prije nego što bi projekt mogao započeti. Korištenjem uslužnog računalstva stvari se mijenjaju. Više ne postoje fiksni ili početni troškovi.

Smanjivanje rizika - IT organizacije koriste oblake za smanjivanje sigurnosnih rizika kojima su podložni poslužitelji. Zakupljivanjem aplikacije u oblaku, glavni problemi davatelja usluga postaju raspodjela i rizik zakupljivanja premalo ili previše infrastrukture. U sve većem broju slučajeva davatelji usluga računalnih oblaka imaju veliku infrastrukturu koja može podnijeti rast zakupljenog prostora i rad individualnog korisnika, smanjujući tako financijske rizike kojima korisnici mogu biti podložni.

Infrastruktura koja funkcionira točno na vrijeme (eng. *just in time infrastructure)* - Pri zakupljivanju aplikacija u oblaku programeri u početku možda i ne znaju kolike kapacitete moraju točno zakupiti, pa može doći do zakupljivanja prevelikog ili premalog dijela oblaka. Rješenja imaju mali rizik jer programeri mogu zakupljivati nove kapacitete kako im rastu potrebe, a ako u početku zakupe previše prostora arhitekture računalnih oblaka isto tako mogu i osloboditi infrastrukturu jednako brzo kako su ju i zakupili. [4]

Mali početni troškovi - Postoje mnoga svojstva računalnih oblaka koja pomažu u reduciranju početnih troškova. Korištenjem ove tehnologije korisnici iznajmljuju infrastrukturu (dakle oni ju ne kupuju) pa troškovi nisu veliki, a kapitalne investicije mogu čak biti jednake nuli. Danas postoji mnoštvo različitih organizacija koje nude usluge računalnih oblaka. Zahvaljujući tome, kupci imaju veće mogućnosti izbora, a organizacije kako bi ostale konkurentne, smanjuju troškove kupnje ciklusa obrade i pohrane, što pomaže u daljnjem reduciranju početnih troškova korištenja računalnih oblaka. Aplikacije se jako brzo razvijaju, čime se smanjuje vrijeme potrebno za njihov izlazak na tržište. Brzim izlaskom na tržište organizacije koje su napravile aplikaciju mogu dobiti veliku početnu prednost u odnosu na konkurenciju. Nudeći nešto novo one mogu diktirati cijenu i zarađivati više, sve dok neka konkurentska organizacija ne napraviti neku sličnu, ali jeftiniju aplikaciju. Nakon toga organizacije se počinju boriti za prevlast na tržištu, a to čine kvalitetom i cijenom.

Povećan tempo inovacija - Računalstvo u oblaku povećava tempo inovacija. Niski početni troškovi pri ulasku na nova tržišta dovode izjednačavanju uvjeta na tržištu. Novim korisnicima niski početni troškovi omogućuju brz razvoj novih proizvoda po nižim cijenama, što im omogućuje ravnomjernije natjecanje s već dobro uhodanim organizacijama, čiji razvojni procesi mogu biti značajno veći. Veća razina nadmetanja povećava stupanj i tempo inovacija. Cijela industrija profitira postojanjem mnogo inovatora koji koriste programe otvorenog koda i tako povećavaju broj inovacija.

Učinkovitije korištenje resursa - Administratori sustava uglavnom se brinu oko nabavke sklopovlja kako ne bi ostali bez potrebnih kapaciteta, i oko boljeg iskorištavanja infrastrukture (kada imaju dovoljna sredstva i idealne količine kapaciteta). Korištenjem arhitekture računalnih oblaka oni mogu bolje i učinkovitije upravljati resursima. Učinkovitije upravljaju resursima jer imaju mogućnost pristupa aplikacijama samo kada su im one potrebne, a nakon toga ih jednostavno mogu prestati koristiti. [4]

Troškovi na temelju uporabe - Stil naplaćivanja troškova po uporabi omogućuje naplaćivanje samo onih infrastruktura koje su korištene. Korisnik nije odgovoran za cijelu infrastrukturu oblaka. Ovo je ključna razlika između aplikacija koje se nalaze na samom računalu korisnika i web aplikacija. Aplikacije na radnoj površini ili tradicionalne klijent/poslužitelj aplikacije izvode se na korisnikovoj vlastitoj infrastrukturi (PC-u ili poslužitelju), dok kod aplikacija s arhitekturom računalnih oblaka korisnik ne koristi vlastitu infrastrukturu i naplaćuje mu se samo dio infrastrukture koji je koristio.

Potencijal smanjivanja vremena obrade - Paralelizacija je jedan od izvrsnih načina ubrzavanja obrade. Ako jedan računski zahtjevan ili osjetljiv posao pokrenemo na jednom stroju i za njegovo izvršavanje je potrebno 500 sati, s arhitekturom računalnih oblaka bilo bi moguće razdijeliti posao na 500 slučajeva i obaviti ga u jednom satu. Dostupnost elastične infrastrukture aplikacijama pruža mogućnost iskorištavanja paralelizacije, što je financijski jako pogodno i smanjuje potrebno vrijeme obrade. [4]

4.5. Sigurnosni problemi i rizici

Privilegirani korisnički pristup - Obrada osjetljivih podataka izvan organizacije donosi određenu razinu rizika. Vanjske usluge zaobilaze fizičke i logičke provjere kao i nadzor osoblja. Korisnici bi trebali prikupiti što više informacija o ljudima koji upravljaju podacima. Trebali bi od davatelja usluga zatražiti informacije o zapošljavanju i nadzoru privilegiranih administratora i provjerama ovlasti njihovih pristupa.

Nadzorna usklađenost - Korisnici su odgovorni za sigurnost i integritet vlastitih podataka čak i kada su oni pohranjeni kod pružatelja usluga. Zato, prije nego što odaberu kojeg davatelja usluga žele izabrati moraju se o njemu dobro informirati. Tradicionalni pružatelji usluga se podvrgavaju vanjskim revizijama i sigurnosnom certificiranju, na taj način dokazujući korisnicima svoje vrijednosti i prednosti pred drugima. Davatelji usluga koji odbijaju pristupiti ovim ispitivanja pokazuju da ih korisnici mogu angažirati samo za najjednostavnije usluge. [4]

Adresa podataka - Korisnik nema točan uvid gdje su njegovi podaci u oblaku pohranjeni. On ne mora znati čak ni državu u kojoj će biti pohranjeni. Korisnik može od davatelja usluge zatražiti pohranjivanje podataka na točno određenim adresama i davanje ugovorne obveze o poštivanju zahtjeva privatnosti u interesu korisnika.

Odvajanje podataka - Podaci se u oblaku uobičajeno nalaze u zajedničkoj okolini s podacima drugih korisnika. Zaštitno kodiranje pri tome može biti korisno, ali ne rješava sve probleme. Korisnik prije odabira organizacije mora saznati što je učinjeno za odvajanje podataka. Davatelji usluga trebali bi pružiti dokaze da su napravljene sheme zaštitnog kriptiranja ispitane. Pogreške u zaštitnom kriptiranju podatke mogu učiniti potpuno neupotrebljivim.

Oporavljanje - Iako korisnik ne zna gdje su njegovi podaci spremljeni, davatelj usluga računalnih oblaka bi trebao reći korisniku što će se dogoditi s podacima u slučaju neplaniranih nesreća. Svaka ponuda poslužitelja koja ne nudi dupliciranje podataka i aplikacija na više različitih mjesta je ranjiva i podložna totalnom gubitku podataka.

Podrška istraživanja - Korištenjem računalnih oblaka istraživanja neprikladnih ili ilegalnih aktivnosti mogu biti nemoguća ili jako složena. Poslužitelji računalnih oblaka su jako teški za istraživanje zbog potrebe za autentikacijom i zbog toga što se na jednom oblaku spremaju podaci mnogih korisnika, a podaci jednog korisnika mogu biti podijeljeni i na više različitih data centara i poslužitelja. Ako korisnik ne može dobiti pismenu potvrdu da računalni oblak podržava određene oblike istraživanja tada se može zaključiti da zahtjevi za istraživanjem i otkrivanjem neće biti mogući. Pismena potvrda davatelja usluge bi trebala sadržavati podatke kojima davatelj usluge potvrđuje da je već uspješno provodio takve aktivnosti. [4]

4.6. Zlouporaba računalnih oblaka

Korisnici računalnih oblaka često imaju privid neograničenih mogućnosti uporabe, što naravno nije utemeljena činjenica. Možda najveći takav privid imaju korisnici IaaS sustava. Navedeni model korisnicima daje neograničene mogućnosti uporabe mrežnih resursa i pohrane podataka. Neki davatelji usluga nude i besplatnu, ali ograničenu, uporabu usluga računalnih oblaka u određenom probnom periodu. Sve navedeno smanjuje stupanj sigurnosti korištenja računalnih oblaka.

Zlonamjerni korisnici relativno jednostavno i nekažnjeno iskorištavaju sigurnosne propuste tako da razvijaju tehnologije koje će im omogućiti učinkovitiji pristup i iskorištavanje podataka drugih korisnika, a pri tome neće ugroziti vlastiti identitet. Davatelji usluga računalnih oblaka su neprekidna meta zlonamjernih korisnika, djelomično zbog relativno slabih autentikacijskih sustava, a djelomično zbog izostanka svijesti o sigurnosnim rizicima krajnjih korisnika sustava. Najviše napada preživjeli su davatelji PaaS modela računalnih oblaka, ali u zadnje vrijeme istraživanja pokazuju sve veću učestalost napada i na Iaas model pružanja usluge. U budućnosti će davatelji usluga veću pažnju morati posvetiti sprječavanju probijanja lozinki i ključeva, DDoS napadima (eng. *Distributed Denial of Service*), pokušaju izvođenja dinamičkih napada i sličnim napadačkim tehnikama. [4]

Da bi se korisnici i davatelji usluga zaštitili od napada trebali bi:

- uvesti složeniju početnu registraciju i provjeru procesa,
- poboljšati praćenje i koordinaciju prijevara koje se izvode preko kreditnih kartica,
- uvesti cjelokupno provjeravanje mrežnog prometa korisnika te
- ugraditi nadzor javnih crnih lista na kojima su navedeni zlonamjerni korisnici (tj. adrese s kojih se korisnici prijavljuju) kako bi se zaštitili vlastiti sustavi. [4]

4.6.1. Zlonamjerni korisnici koji napade izvode iznutra

Većina organizacija je jako dobro upoznata s opasnostima koje im mogu donijeti dobro upućeni zlonamjerni korisnici. Ova prijetnja predstavlja još veći problem korisnicima usluga računalnih oblaka. Prijetnja predstavlja problem pogotovo kada se u obzir uzme osnovni nedostatak transparentnosti procesa i procedura davatelja usluga. Na primjer, davatelji usluga ne otkrivaju način na koji svojim korisnicima daju pristup fizičkim i virtualnim sredstvima, niti način na koji prate korisnike, analiziraju i izvještavaju o suradnji. Ova situacija stvara privlačnu mogućnost iskorištavanja, koju zlonamjerni korisnici rado iskorištavaju. Razina odobrenog pristupa oblaku omogućuje iskorištavanje povjerljivih podataka ili dobivanje potpunog nadzora nad uslugom s jako malom mogućnošću otkrivanja identiteta napadača. Utjecaj koji zlonamjerni korisnici „iznutra“ mogu imati na organizaciju definitivno se ne smije zanemariti, pogotovo kada se u obzir uzme njihova razina pristupa i mogućnost prodiranja u organizacije. Neki od načina na koji zlonamjerni korisnici mogu utjecati na organizaciju su povreda ugleda, financijski utjecaj i gubitak produktivnosti. Kada organizacija prihvati poslužitelje računalnih oblaka ljudski utjecaj postaje još veći. Jako je važno upoznati korisnike računalnih oblaka s postupcima koje poduzima davatelj usluga da bi spriječio napade iznutra. [4]

Da bi se korisnici i davatelji usluga zaštitili od napada trebaju:

1. provoditi strogi nadzor nad lancem nabave i provoditi cjelokupne procjene isporučitelja,
2. odrediti zahtjeve za ljudskim resursima kao dio pravnog ugovora,
3. zahtijevati transparentnost u informacijskoj sigurnosti i praksi upravljanja, kao usklađenost izvještavanja i
4. odrediti proces obavještavanja o sigurnosnim problemima. [4]

4.6.2. Gubitak i neovlašteno otkrivanje podataka

Postoje brojni načini na koje zlonamjerni korisnici mogu ugroziti važne podatke organizacije. Primjer toga je brisanje ili promjena podataka bez kopije originalnog sadržaja. Raskidanje veze između dijela podataka pohranjenog na nekom drugom dijelu poslužitelja i cjelokupnog izvornog podatka može podatak učiniti nepovratnim (jednako kao što to može učiniti pohrana podataka na nesiguran medij za pohranu).

Gubitak ključa za kodiranje može dovesti do uništavanja bitnih podataka. Neovlaštenim stranama mora biti zabranjen pristup osjetljivim podacima. U oblaku raste prijetnja ugrožavanja podataka zbog mnoštva različitih međudjelovanja između rizika i izazova koji su jedinstveni za oblak ili, još opasnije, zbog arhitekturalnih ili operacijskih svojstava oblaka. Gubitak ili neovlašteno otkrivanje podataka mogu imati poguban utjecaj na poslovanje. Mogu ugroziti ugled i reputaciju organizacije, dovesti do prekida poslovne suradnje s organizacijama koje koriste oblak, poslovnim partnerima ili gubitka povjerenja korisnika.

Gubitak ključnog intelektualnog vlasništva može imati natjecateljske i financijske utjecaje, jer će mnoge druge organizacije ili zlonamjerni korisnici pokušati doći do tih podataka i iskoristiti ih za vlastitu dobrobit. Ovisno o podacima koji su izgubljeni ili su djelomično procurili na tržište može doći do kršenja ljudskih prava (npr. objavljivanja inkriminirajućih podataka o nekome pojedincu, iskorištavanje dobivanih informacija u želji da se smanji financijska moć ili ugled pojedinca) i pravnih posljedica (npr. pokretanje sudskih postupaka protiv pojedinca ili organizacije zbog sadržaja pronađenih podataka). Do iskorištavanja podataka organizacija ili pojedinačnih korisnika može doći zbog nedovoljnog sigurnosnog nadzora, zatim nepravilnog korištenja šifri i programskih ključeva, operacijskih neuspjeha i pouzdanosti podatkovnih centara. Prijetnja se pojavljuje na svim modelima pružanja usluge. [4]

Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- implementirati sučelje s dobrom kontrolom pristupa,
- kriptirati podatke i zaštiti njihov integritet podataka,

- analizirati zaštitu podataka za vrijeme dizajna i izvođenja te nakon što korisnici oduče za prestanak korištenja poslužitelja,
- davatelji usluga bi trebali trajno ukloniti korisničke podatke sa poslužitelja.

Korisnici bi trebali sklopiti ugovor s davateljima usluge koji sadrži detalje oko postojanja sigurnosnih mjera i strategije pridržavanja. [4]

4.6.3. Krađa korisničkih imena

Krađom korisničkog imena napadači mogu iskorištavati usluge koje plaćaju korisnici. Zlonamjerni korisnici napadima poput krađe identiteta, prijevara i iskorištavanja programskih ranjivosti još uvijek postižu uspjehe u narušavanju sigurnosti korisnika. Korisnici često koriste iste vjerodajnice i lozinke, što povećava broj ovakvih napada. Korištenjem računalnih oblaka pojavljuju se nove prijetnje. Ako napadač dobije pristup vjerodajnicama, on može promatrati aktivnosti i transakcije, upravljati podacima te usmjeravati korisnike na zlonamjerne stranice. Korisnički računi ili usluge postaju napadačima nova meta s kojom mogu iskorištavati korisnikov identitet za izvođenje daljnjih napada. Krađa korisničkih imena, obično u obliku krađe vjerodajnica (eng. *credentials*), korisnicima predstavlja jednu od najvećih prijetnji. S ukradenim vjerodajnicama zlonamjerni napadači mogu pristupiti kritičnim podacima, i tako ugroziti povjerljivost, integritet i dostupnost tih usluga. Organizacije bi trebale biti svjesne ovih tehnika kao i uobičajenih načina zaštite od istih. Prijetnja se pojavljuje na svim modelima pružanja usluge računalnih oblaka. [4]

Da bi se korisnici i davatelji usluga zaštitili od napada potrebno je:

- zabraniti dijeljenje pristupnih vjerodajnica između korisnika i poslužitelja,
- gdje god je moguće koristiti snažne dvofaktorske autentikacijske tehnike,
- izvoditi proaktivno praćenje za otkrivanje neovlaštenih aktivnosti i
- razumijevati sigurnosne politike i SLA (eng. *service level agreement*) davatelja usluga računalnih oblaka. [4]

5. SIGURNOSNE PRIJETNJE KOD MOBILNIH UREĐAJA

Mobilni uređaji i mreže dio su današnje svakodnevice. Veliki napredak u bežičnim tehnologijama i rastuća potražnja za mobilnošću tokom telefoniranja i pristupa internetu rezultirali su potrebom za izgradnjom boljih mobilnih mreža. Telekomunikacijska industrija znatno se razvila od izuma telefona i napredovala u mobilnu mrežu. Tokom razvoja, nastale su pet generacija mobilnih mreža. Mobilne mreže značajno su poboljšane u sve traženijem prijenosu podataka i multimedijskih sadržaja. Korisnicima se nudi poboljšana funkcionalnost mobilnih uređaja, kao što je neometano pretraživanje web sadržaja, gledanje televizije, pristup elektroničkoj pošti i navigaciji. Obzirom da je sve popularnije pristupati internetu preko mobilnih uređaja, javljaju se i opasnosti koje uvijek vrebaju kada se korisnici povezuju na internet. Uvijek postoje sigurnosni rizici i prijetnje od zlonamjernih napadača. Zato je potrebno pravilno zaštititi sve komunikacijske kanale. Uz to, vrlo su česte prijevare preko telefona i zlouporabe prijenosa govora. [5]

Najopasnije su sigurnosne prijetnje za mobilne uređaje u sljedećih sedam područja:

- tekstualne poruke,
- kontakti i adresar,
- video,
- prijepisi telefonskih razgovora,
- povijest poziva,
- dokumentacija te
- upotreba međuspremnika. [5]

5.1. Tekstualne poruke

Gotovo svi mobilni uređaji korisniku pružaju mogućnost slanja i blokiranja poruka. Napadači mogu korisniku poslati posebno oblikovane poruke sa zloćudnim programskim kodom koji mogu iskoristiti za krađu osobnih podataka i ostalih podataka koji se nalaze na mobilnom telefonu. Osim opisanih poruka, napadač može korisniku poslati poruku u kojoj ga navodi na otkrivanje osjetljivih podataka. Takav oblik napada se naziva *SMiShing*, prema već poznatom obliku napada na osobnim računalima *phishingu*. Primjer zloćudnog programa kojeg napadač može podmetnuti korisniku je tekstualna poruka koja koristi funkcije za upravljanje SMS porukama za slanje lažnih poruka ljudima koji se nalaze u adresaru. Ova metoda napada je slična napadu korištenjem poruka elektroničke pošte na osobnim računalima, no napad upotrebom SMS poruka ima veću mogućnost uspjeha jer žrtva obično nije svjesna da postoji takva sigurnosna prijetnja. [5]

5.2. Adresar

U korporacijskom okruženju adresar je jedna od najvažnijih aplikacija na mobilnom uređaju. Krađa kontaktnih podataka može imati kobne posljedice za zaposlenike i tvrtku. Napadač može, ukoliko uspješno podmetne zlonamjerni program, ukrasti podatke s mobilnog uređaja, među njima i kontaktne podatke osoba u adresaru. Napadač tada može osobama čije je kontakte ukrao slati poruke sa zlonamjernim programima u privitku, poruke koje sadrže poveznicu na web stranicu koja sadrži zloćudne programe i/ili poslati poruku u kojoj navodi korisnika na otkrivanje povjerljivih podataka. [5]

5.3. Video

Većina mobilnih telefona u današnje vrijeme ima kameru kojom se mogu snimati fotografije i video sadržaj. Napadač može podmetnuti posebno oblikovani programski kod kojim preuzima upravljanje kamerom na mobilnom uređaju. No kako korisnici uglavnom čuvaju svoje mobilne uređaje u džepu ili torbici, mjestima s kojih nije korisno slikati ili snimiti video sadržaj, vjerojatnost takve zlouporabe je vrlo mala. Veći sigurnosni problem je ukoliko napadač preuzme upravljanje nad mobilnim telefonom i sadržajem koji je pohranjen u direktoriju kamere. Na mobilnim telefonima je uobičajeno da postoji poseban direktorij za pohranu multimedijskog sadržaja kojem se može pristupiti putem kamere. U slučaju uspješnog napada, napadač može ugroziti sigurnost fotografija i video snimaka koje se nalaze na mobitelu. Napadač može postaviti posebno oblikovani program da pošalje sve slikovne datoteke njemu ili na neku adresu elektroničke pošte kojom upravlja. [5]

5.4. Snimke telefonskih razgovora

Mnogi mobilni telefoni imaju aplikacije koje mogu snimati telefonske razgovore. Mobilni uređaji imaju ograničen prostor za pohranu podataka i datoteka tako da se sadržaj ne može snimati neograničeno dugo. Ukoliko napadač podmetne posebno oblikovani program i preuzme upravljanje nad snimanjem zvuka, može snimati proizvoljno dugo i poslati si datoteku u poruci elektroničke pošte. [5]

5.4.1. Povijest poziva

Zapisi o pozivima mogu koristiti napadaču i on može podmetnuti posebno oblikovani program kako bi pročitao podatke o prijašnjim pozivima. Korisnici bi u svrhu zaštite trebali pratiti zapise o pozivima i povremeno ih obrisati. [5]

5.5. Dokumentacija

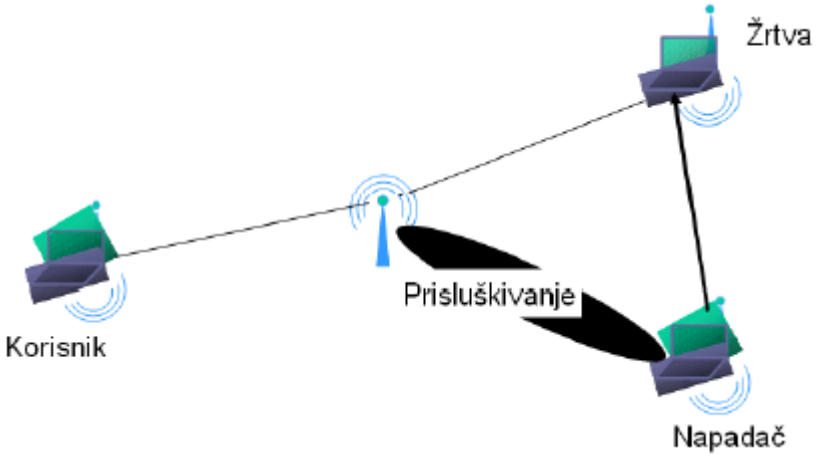
Mnogi korisnici mobilnih telefona čitaju i spremaju dokumente tipa Word, Excel ili PDF na svoje mobitele. Napadač može podmetnuti zlоćudni program kojim će ukrasti takve datoteke. Datoteke sa ekstenzijama .doc, .xls i .pdf su popularne mete napadača. Preporuča se da korisnici mobilnih telefona ne spremaju važne i povjerljive dokumente na svoje uređaje. [5]

5.6. Upotreba međuspremnika

Sigurnosni propusti vezani uz međuspremnike su neki od najčešćih programskih propusta. U slučaju postojanja programskog propusta vezanog uz međuspremnik, napadač ga može iskoristiti za prepisivanje spremnika. Ukoliko se to dogodi, napadač može podmetnuti proizvoljni programski kod. Operacijski sustavi mobilnih telefona vrlo su slični operacijskim sustavima osobnih računala i upotreba međuspremnika je uobičajena. [5]

5.7. Sigurnosne prijetnje u mobilnim mrežama

Prije pojave GPRS (eng. *General Packet Radio Service*) i UMTS (eng. *Universal Mobile Telecommunications System*) protokola, GSM (eng. *Global System for Mobile Communications*) mreže su korisnicima pružale dovoljnu sigurnosnu zaštitu. Pojavom GPRS i UMTS tehnologija koje su se ili nadograđivale ili su osmišljene tako da budu kompatibilne sa GSM sustavom, povećale su se brzine prijenosa i kapacitet komunikacijskih kanala. Također, povećao se broj usluga koji se nudi korisnicima, kao što je prijenos multimedijalnog sadržaja. Uspješan napad podrazumijeva da napadač posjeduje posebno prilagođen mobilni uređaj i/ili baznu stanicu (odašiljač). Slika 6. prikazuje napad u kojemu napadač prisluškuje komunikaciju i ometa ju. [5]



Slika 6. Napad s čovjekom u sredini. [5]

Napadač može izvesti napad uskraćivanja usluga slanjem posebno oblikovanih zahtjeva za odjavom ili obnovom položaja mobilnog uređaja iz područja u kojem se korisnik ne nalazi. Ukoliko izvodi napad s čovjekom u sredini, napadač se upotrebom prilagođenog mobitela ili bazne postaje ubaci između mreže i korisnika. Mobilni korisnici se identificiraju upotrebom privremenih identiteta, no postoje slučajevi kada mreža traži korisnika da pošalje svoj pravi identitet u obliku jasnog teksta. Napadi koje napadač može izvesti u ovoj situaciji su:

Pasivna krađa identiteta – napadač ima prilagođeni mobilni uređaj i pasivno čeka pojavu nove registracije ili rušenje baze podataka jer se u tim slučajevima od korisnika traži da pošalje svoje podatke u čistom tekstu.

Aktivna krađa identiteta – napadač ima prilagođenu temeljnu stanicu te potiče korisnika da se priključi na njegovu postaju. Zatim ga traži da mu pošalje IMSI. Napadač se može maskirati i pretvarati da je prava mobilna mreža. To može učiniti na sljedeće načine:

- **Ukidanjem enkripcije između korisnika i napadača** – napadač s prilagođenom baznom stanicom potiče korisnika na prijavu na njegovu lažnu postaju i kada korisnik koristi usluge postaje, opcija kriptiranja nije uključena. [5]

- **Ukidanjem enkripcije između korisnika i prave mreže** – u ovom slučaju tokom uspostave poziva mogućnosti kriptiranja mobilnog uređaja su promijenjene i mreži se čini kao da postoji razlika između algoritma kriptiranja i autentikacije. Nakon toga mreža može odlučiti uspostaviti nekriptiranu vezu. Napadač prekida vezu i lažno se predstavlja mreži kao korisnik. Napadač može izvesti napad lažno se predstavljajući kao običan korisnik:

  - Upotrebom ugroženog autentikacijskog vektora – napadač s prilagođenim mobilnim uređajem i ugroženim autentikacijskim vektorom oponaša korisnika prema mreži i ostalim korisnicima.
  - Prisluškivanjem postupka autentikacije – napadač s prilagođenim mobilnim uređajem koristi podatke koje je dobio prisluškivanjem.
  - Otimanjem odlaznih poziva u mrežama s isključenom enkripcijom.
  - Otimanjem dolaznih poziva kod kojih je isključena enkripcija.

Krađom mobilnog uređaja na kojem nije postavljen mehanizam zaključavanja, kao što je zaštita lozinkom, neovlašteni korisnik može zatražiti usluge na GPRS mreži pretvarajući se da je izvorni korisnik. [5]

6. PRAVNI OKVIR

Hrvatska ima uređen pravni okvir u području informacijske sigurnosti kojeg čine[1]:

- Nacionalni program informacijske sigurnosti u Republici Hrvatskoj
- Zakon o informacijskoj sigurnosti (NN 79/07) sa svoja dva provedbena akta[6]:
    - Uredba o mjerama informacijske sigurnosti (NN 46/08) i
    - Pravilnici i standardi informacijske sigurnosti
- Zakon o tajnosti podataka (NN 79/07, 86/12)[7]
- Zakon o pravu na pristup informacijama (NN 25/13)[8]
- Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11 i 106/12-pročišćeni tekst)[9]
- Zakon o autorskom pravu i srodnim pravima (NN 167/03, 79/07, 80/11, 125/11, 141/13 i 127/14 – pročišćeni tekst)[10]
- Kazneni zakon (124/13, 81/13, 79/12, 57/11)[11]
- Zakon o telekomunikacijama (NN 70/05, 60/04, 117/03, 158/03)[12]
- Zakon o zaštiti potrošača (NN 41/14, 56/13, 78/12)[13]
- Zakon o elektroničkoj ispravi (NN 150/05)[14]
- Zakon o elektroničkom potpisu (NN 30/14, 89/13, 107/10, 80/08, 10/02)[15]
- Zakon o elektroničkim komunikacijama (NN 71/14, 80/13, 133/12, 90/11, 73/08)[16]

Važni provedbeni akti nekih od ovih propisa su i:

- Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost
- Uredba o sadržaju, izgledu, načinu ispunjavanja i postupanju s upitnikom za sigurnosnu provjeru
- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima.[1]

Također, tvrtke donose i svoje interne pravne akte, najčešće u obliku raznih pravilnika, u koje ugrađuju obveze i načine postupanja zaposlenika u pogledu sigurnosti informacija. [1]

6.1. Zakon o informacijskoj sigurnosti

6.1.1. Osnovne odredbe

Članak 1.

(1) Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

(2) Ovaj se Zakon primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

(3) Ovaj se Zakon primjenjuje i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. [6]

Članak 2.

Pojedini pojmovi u smislu ovoga Zakona imaju sljedeće značenje:

- Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.
- Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

- Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.

- Područja informacijske sigurnosti predstavljaju podjelu informacijske sigurnosti na pet područja s ciljem sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti.

- Sigurnosna akreditacija informacijskog sustava je postupak u kojem se utvrđuje osposobljenost tijela i pravnih osoba iz članka 1. stavka 2. ovoga Zakona za upravljanje sigurnošću informacijskog sustava, a provodi se utvrđivanjem primijenjenih mjera i standarda informacijske sigurnosti.

- Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike. [6]

6.1.2. Mjere i standardi informacijske sigurnosti

Članak 3.

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama iz članka 1. stavka 2. i 3. ovoga Zakona. [6]

Članak 4.

(1) Mjere i standardi informacijske sigurnosti utvrđuju se za klasificirane i neklasificirane podatke.

(2) Mjere i standardi informacijske sigurnosti utvrđuju se sukladno stupnju tajnosti, broju, vrsti te ugrozama klasificiranih i neklasificiranih podataka na određenoj lokaciji.

(3) Za klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, trajno se provodi sigurnosna prosudba ugroza. [6]

Članak 5.

Mjere i standardi informacijske sigurnosti obuhvaćaju:

- nadzor pristupa i postupanja s klasificiranim podacima,
- postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka,
- planiranje mjera prilikom izvanrednih situacija,
- ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje. [6]

Članak 6.

(1) Mjere i standardi informacijske sigurnosti za zaštitu neklasificiranih podataka utvrđuju se u skladu s mjerama i standardima zakonom propisanim za zaštitu osobnih podataka građana.

(2) Mjere i standardi informacijske sigurnosti za zaštitu stupnja tajnosti »Ograničeno« utvrđuju se u skladu sa stavkom 1. ovoga članka, uz:

- prethodnu provjeru primjene propisanih mjera i standarda za neklasificirane podatke,
- primjenu mjera i standarda propisanih za stupanj tajnosti »Ograničeno«.[6]

Članak 7.

Mjere informacijske sigurnosti propisat će se uredbom koju donosi Vlada Republike Hrvatske, a standardi za provedbu mjera propisat će se pravilnicima koje donose čelnici središnjih državnih tijela za informacijsku sigurnost. [6]

6.1.3. Područja informacijske sigurnosti

Članak 8.

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podatka,
- sigurnost informacijskog sustava,
- sigurnost poslovne suradnje. [6]

Sigurnosna provjera

Članak 9.

(1) Sigurnosna provjera je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima.

(2) Osobe iz stavka 1. ovoga članka obvezne su ishoditi uvjerenje o sigurnosnoj provjeri osobe (certifikat).

(3) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, dužni su ustrojiti:

- popis osoba koje imaju pristup klasificiranim podacima,
- registar zaprimljenih certifikata s rokovima važenja certifikata. [6]

Fizička sigurnost

Članak 10.

(1) Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci.

(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«, izvršit će kategorizaciju objekata i prostora na sigurnosne zone, propisane mjerama i standardima informacijske sigurnosti. [6]

Sigurnost podatka

Članak 11.

(1) Sigurnost podatka je područje informacijske sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.

(2) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, koji koriste klasificirane i neklasificirane podatke u svom djelokrugu, dužni su primijeniti procedure o postupanju s klasificiranim i neklasificiranim podacima, o sadržaju i načinu vođenja evidencije o izvršenim uvidima u klasificirane podatke te nadzoru sigurnosti podataka, propisanim mjerama i standardima informacijske sigurnosti. [6]

Sigurnost informacijskog sustava

Članak 12.

(1) Sigurnost informacijskog sustava je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.

(2) Sigurnosna akreditacija informacijskog sustava provodi se za informacijski sustav u kojem se koriste klasificirani podaci stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«.

(3) Osobe koje sudjeluju u procesu iz stavka 1. ovoga članka trebaju posjedovati certifikat razine »Vrlo tajno« ili za jedan stupanj više od najviše razine tajnosti klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijskim sustavima pod njihovom nadležnosti.

(4) Mjere fizičke zaštite prostora u kojima se nalaze informacijski sustavi poduzet će se sukladno najvišoj razini tajnosti klasificiranih podataka koji se u njima obrađuju, pohranjuju ili prenose.

(5) Središnja državna tijela za informacijsku sigurnost ustrojavaju registar certificirane opreme i uređaja koji se koriste u klasificiranom informacijskom sustavu razine »Povjerljivo«, »Tajno« i »Vrlo tajno«. Registar certificirane opreme i uređaja ustrojava se na temelju preuzimanja odgovarajućih registara međunarodnih organizacija ili vlastitim certificiranjem u skladu s odgovarajućim međunarodnim normama. [6]

Sigurnost poslovne suradnje

Članak 13.

(1) Sigurnost poslovne suradnje je područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe iz članka 1. stavka 3. ovoga Zakona.

(2) Pravne i fizičke osobe koje pristupaju provedbi natječaja ili ugovora iz stavka 1. ovoga članka, obvezne su ishoditi uvjerenje o sigurnosnoj provjeri pravne osobe (certifikat poslovne sigurnosti).

(3) Pravne i fizičke osobe iz stavka 1. ovoga članka za osoblje, objekte i prostore obvezne su primijeniti utvrđene mjere i standarde informacijske sigurnosti za određeni stupanj tajnosti klasificiranih podataka.

(4) Tijela i pravne osobe iz članka 1. stavka 2. ovoga Zakona, ovlašteni su za podnošenje zahtjeva za izdavanje certifikata poslovne sigurnosti za pravne i fizičke osobe kojima dostavljaju klasificirane podatke stupnja tajnosti »Povjerljivo«, »Tajno« i »Vrlo tajno«.

(5) Pravne i fizičke osobe koje sudjeluju u međunarodnim poslovima za koje je obvezan certifikat poslovne sigurnosti, ovlaštene su za podnošenje zahtjeva za izdavanje certifikata.

(6) Certifikat poslovne sigurnosti izdaje središnje državno tijelo za informacijsku sigurnost. [6]

6.1.4. Središnja državna tijela za informacijsku sigurnost

Ured Vijeća za nacionalnu sigurnost

Članak 14.

Ured Vijeća za nacionalnu sigurnost je središnje državno tijelo za informacijsku sigurnost koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. [6]

Članak 15.

(1) Ured Vijeća za nacionalnu sigurnost donosi Pravilnik o standardima sigurnosne provjere, Pravilnik o standardima fizičke sigurnosti, Pravilnik o standardima sigurnosti podataka, Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava te Pravilnik o standardima sigurnosti poslovne suradnje.

(2) Ured Vijeća za nacionalnu sigurnost trajno usklađuje propisane mjere i standarde informacijske sigurnosti u Republici Hrvatskoj s međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti. [6]

Članak 16.

(1) Ured Vijeća za nacionalnu sigurnost koordinira i usklađuje rad tijela i pravnih osoba iz članaka 17., 20., 23. i 25. ovoga Zakona.

(2) Ured Vijeća za nacionalnu sigurnost surađuje s mjerodavnim institucijama stranih zemalja i organizacija u području informacijske sigurnosti te koordinira međunarodnu suradnju ostalih tijela i pravnih osoba iz stavka 1. ovoga članka. [6]

Zavod za sigurnost informacijskih sustava

Članak 17.

(1) Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavka 2. ovoga Zakona.

(2) Tehnička područja sigurnosti informacijskih sustava su:

– standardi sigurnosti informacijskih sustava,

– sigurnosne akreditacije informacijskih sustava,

– upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka,

– koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. [6]

Članak 18.

(1) Zavod za sigurnost informacijskih sustava pravilnikom će regulirati standarde tehničkih područja sigurnosti informacijskih sustava iz članka 17. stavka 2. ovoga Zakona.

(2) Zavod za sigurnost informacijskih sustava trajno usklađuje standarde tehničkih područja sigurnosti informacijskih sustava u Republici Hrvatskoj s međunarodnim standardima i preporukama te sudjeluje u nacionalnoj normizaciji područja sigurnosti informacijskih sustava. [6]

Članak 19.

Zavod za sigurnost informacijskih sustava obavlja poslove sigurnosne akreditacije informacijskih sustava u suradnji s Uredom Vijeća za nacionalnu sigurnost. [6]

6.1.5. Nacionalni CERT

Članak 20.

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet).

(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.

(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada. [6]

Članak 21.

CERT i Zavod za sigurnost informacijskih sustava surađuju na prevenciji i zaštiti od računalnih ugroza sigurnosti informacijskih sustava te sudjeluju u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava. [6]

6.2.Zaštita podataka na temelju Opće uredbe o zaštiti podataka

Općom uredbom o zaštiti podataka utvrđuju se detaljni zahtjevi za poduzeća i organizacije u pogledu prikupljanja osobnih podataka, njihove pohrane te upravljanja osobnim podacima. Primjenjuju se na europske organizacije koje obrađuju osobne podatke pojedinaca u EU-u te organizacije izvan EU-a koje su usmjerene na ljude koji žive u EU-u.

Opća uredba o zaštiti podataka primjenjuje se ako:

- vaše poduzeće obrađuje osobne podatke i ima poslovni nastan u EU-u, neovisno o tome gdje se odvija sama obrada podataka
- vaše poduzeće ima poslovni nastan izvan EU-a, no obrađuje osobne podatke u vezi s ponudom robe ili usluga pojedincima u EU-u ili prati ponašanje osoba unutar EU-a.

Poduzeća s poslovnim nastanom izvan EU-a koja obrađuju osobne podatke građana EU-a moraju imenovati **predstavnika u EU-u.** [17]

Opća se uredba o zaštiti podataka ne primjenjuje u sljedećim slučajevima:

- ako je ispitanik mrtav
- ako je ispitanik pravna osoba
- ako obradu obavlja osoba koja djeluje u svrhe koje ne ulaze u okvir njezine stručne, poslovne ili profesionalne djelatnosti. [17]

6.2.1.Osobni podaci

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, koji se naziva **ispitanik.** Osobni podaci uključuju informacije kao što su:

- ime i prezime
- adresa
- broj osobne iskaznice ili putovnice
- primanja
- kulturni profil
- adresa internetskog protokola
- podaci u posjedu bolnice ili liječnika (koji služi kao jedinstvena identifikacijska oznaka u zdravstvene svrhe). [17]

Posebne kategorije podataka

Ne možete obrađivati osobne podatke o nečijem:

- rasnom ili etničkom podrijetlu
- spolnoj orijentaciji
- političkim stavovima
- vjerskim ili filozofskim uvjerenjima
- članstvu u sindikatu
- genetskim, biometrijskim ili zdravstvenim podacima osim u posebnim slučajevima (npr. kad imate izričitu privolu ili kad je obrada u znatnom javnom interesu, na temelju prava EU-a ili nacionalnog prava)
- osobne podatke povezane s kaznenim osudama i djelima osim ako to nije dopušteno pravom EU-a ili nacionalnim pravom. [17]

Tijekom obrade osobni podaci mogu proći kroz više različitih poduzeća ili organizacija. U tom ciklusu dvije su ključne uloge u obradi osobnih podataka:

- **Voditelj obrade podataka** odlučuje o svrsi i načinu obrade podataka.
- **Izvršitelj obrade podataka** čuva i obrađuje podatke u ime voditelja obrade podataka. [17]

6.2.2. Nadzor obrade podataka

Službenik za zaštitu podataka kojeg prema potrebi imenuje poduzeće odgovoran je za nadzor kako se obrađuju osobni podaci te informiranje i savjetovanje zaposlenika koji obrađuju osobne podatke o njihovim obvezama. Taj službenik ujedno i surađuje s tijelom za zaštitu podataka te je kontaktna točka za pojedince i tijelo za zaštitu podataka.

Vaše poduzeće mora imenovati službenika za zaštitu ako:

- redovito ili sustavno prati pojedince ili obrađuje posebne kategorije podataka
- je ta obrada podataka vaša temeljna poslovna aktivnost
- obrađujete velik broj podataka.

Primjerice, ako obrađujete osobne podatke u svrhu oglašavanja putem tražilica na temelju ponašanja pojedinaca na internetu morate imati službenika za zaštitu podataka. Međutim, ako samo jednom godišnje klijentima šaljete promotivni materijal ne trebate imati službenika za zaštitu podataka. Isto tako, ako ste liječnik koji prikuplja podatke o zdravlju pacijenata vjerojatno ne morate imati službenika za zaštitu podataka. No ako obrađujete osobne podatke o genetici i zdravlju za potrebe bolnice, trebat će vam službenik za zaštitu podataka.

Službenik za zaštitu podataka može biti član osoblja vaše organizacije ili se s njime može sklopiti ugovor o vanjskim uslugama. Službenik za zaštitu podataka može biti pojedinac ili dio organizacije. [17]

6.2.3. Prijenos podataka izvan EU-a

Kad se osobni podaci prenose izvan EU-a, zaštita koju pruža Opća uredba o zaštiti podataka i dalje se primjenjuje na njih. To znači da ako izvozite podatke u inozemstvo, vaše poduzeće mora osigurati da se pridržava jedne od sljedećih mjera:

- EU smatra da su mjere treće zemlje odgovarajuće.
- Vaše poduzeće poduzima potrebne mjere kako bi se osigurala odgovarajuća zaštita, primjerice uključivanjem posebnih odredbi u ugovor s uvoznikom osobnih podataka iz treće zemlje.
- Vaše se poduzeće oslanja na posebne razloge prijenosa (odstupanja) kao što je privola pojedinca. [17]

6.2.4. Dopuštenja za obradu podataka

Pravila EU-a o zaštiti podataka propisuju da biste podatke trebali obrađivati na pošten i zakonit način za određenu i legitimnu svrhu te obrađivati samo podatke koji su neophodni za nju. Morate osigurati da ste ispunili jedan od sljedećih uvjeta za obradu osobnih podataka;

- imate **privolu** predmetnog pojedinca
- osobni su vam podaci potrebni za ispunjavanje **ugovorne obveze** prema pojedincu
- osobni su vam podaci potrebni kako biste ispunili **zakonsku obvezu**
- osobni su vam podaci potrebni za zaštitu **životnog interesa** pojedinca
- obrađujete osobne podatke u okviru **zadaće od javnog interesa**
- djelujete u ime **legitimnih interesa** svojeg poduzeća pod uvjetom da time nisu ozbiljno narušena temeljna prava i slobode pojedinca čije podatke obrađujete.

Ne možete obrađivati osobne podatke ako prava osobe imaju prevagu nad interesima vašeg poduzeća. [17]

6.2.5. Pristanak na obradu podataka

Općom uredbom o zaštiti podataka propisuju se stroga pravila za obradu podataka utemeljena na privoli. Cilj je tih pravila **osigurati da pojedinac razumije na što pristaje.** To znači da privola treba biti dobrovoljna, posebna, informirana i nedvosmislena te dana na temelju zahtjeva napisanog jasnim i jednostavnim jezikom. Privola bi se trebala dati afirmativnim činom, kao što je označavanje polja na internetu ili potpisivanje obrasca.

Kad netko pristane na obradu svojih osobnih podataka, možete ih obrađivati samo u svrhe za koje je privola dana. Morate im omogućiti i povlačenje privole. [17]

Posebna pravila za djecu

Ako prikupljate osobne podatke djece na temelju privole, primjerice pri korištenju korisničkih računa na društvenim medijima ili stranicama za učitavanje sadržaja **morate prvo dobiti privolu roditelja**, primjerice slanjem obavijesti roditelju ili skrbniku. Dobna granica do koje se netko smatra djetetom razlikuje se ovisno o tome gdje žive, no kreće se između 13 i 16 godina. [17]

6.2.6. Pravo na pristup i pravo na prenosivost podataka

Morate osigurati da pojedinci imaju **pravo na pristup svojim osobnim podacima** bez naknade. Ako primite takav zahtjev morate:

- reći im obrađujete li njihove osobne podatke
- informirati ih o obradi (svrha obrade, vrste osobnih podataka koje se upotrebljavaju, primatelji podataka itd.)
- dati im presliku njihovih osobnih podataka koji se obrađuju (u pristupačnom formatu).

Kad se obrada temelji na suglasnosti ili na ugovoru, pojedinac može zatražiti da mu vratite osobne podatke ili da ih prenesete drugom poduzeću. To se naziva pravo na prenosivost podataka. Trebali biste podatke dostaviti u uobičajenom i strojno čitljivom formatu. [17]

Pravo na ispravak i pravo na prigovor

Ako pojedinac smatra da su njegovi osobni podaci netočni, nepotpuni ili neprecizni, imaju **pravo tražiti da ih se ispravi ili dopuni** bez odgode.

U tom slučaju trebali biste sve primatelje podataka obavijestiti da su neki od osobnih podataka koje ste s njima podijelili izmijenjeni ili izbrisani. Ako su osobni podaci koje ste podijelili bili netočni, možda ćete morati o tome obavijestiti sve koji su ih vidjeli (osim u slučaju da bi to zahtijevalo nerazmjeran napor).

Pojedinac **može u bilo kojem trenutku prigovoriti obradi svojih osobnih podataka**, posebno u slučaju kad ih vaše poduzeće obrađuje na temelju vlastitog legitimnog interesa ili kao dio zadaće od javnog interesa. Ako vaš legitimni interes ne prevaguje nad interesom pojedinca morate prestati s obradom osobnih podataka.

Pojedinac može zatražiti i ograničenje obrade svojih osobnih podataka dok se utvrđuje prevaguje li vaš legitimni interes nad njegovim. Međutim, u slučaju izravnog marketinga, uvijek morate odmah prestati s obradom osobnih podataka na zahtjev pojedinca. [17]

6.2.7. Pravo na zaborav

U nekim okolnostima pojedinac može od voditelja obrade podataka zatražiti brisanje svojih osobnih podataka, primjerice ako podaci više nisu potrebni za ispunjenje svrhe obrade. Međutim, vaše poduzeće nije obvezno to učiniti u sljedećim slučajevima:

- obrada je nužna za poštovanje slobode izražavanja i informiranja
- morate čuvati osobne podatke za usklađivanje s pravnom obvezom
- postoje drugi razlozi od javnog interesa za pohranu podataka, primjerice u svrhe javnog zdravlja ili u svrhe znanstvenih i povijesnih istraživanja
- morate pohraniti podataka radi uspostavljanja pravnog zahtjeva. [17]

6.2.8. Tehnička i integrirana zaštita podataka

Tehnička zaštita podataka znači da poduzeće treba uzeti zaštitu podataka u obzir u ranim stadijima planiranja novih načina obrade osobnih podataka. U skladu s tim načelom, voditelj obrade podataka mora poduzeti sve potrebne tehničke i organizacijske mjere za provedbu načela zaštite podataka i zaštititi prava pojedinaca. To se može postići primjerice upotrebom pseudonima.

Integrirana zaštita podataka znači da bi osnovna postavka poduzeća trebala biti ona kojom se najviše štiti privatnost. Primjerice, ako su moguće dvije postavke privatnosti i jedna od postavki onemogućava da osobnim podacima pristupe druge osobe, ta postavka mora biti postavljena kao osnovna. [17]

6.2.9. Kršenje pravila i kazne

Neusklađenost s Općom uredbom o zaštiti podataka može za određene povrede dovesti do znatnih novčanih kazni u iznosu do 20 milijuna eura ili 4 % globalnog prometa vašeg poduzeća. Tijelo za zaštitu podataka može odrediti dodatne korektivne mjere, primjerice narediti vam da prekinete obradu osobnih podataka. [17]

7. KONTROLNE PREPORUKE ZA INFORMACIJSKE SUSTAVE I POVEZANE TEHNOLOGIJE

Za potrebe obrazovanja o sigurnosti u informacijskim sustavima osnovana je Udruga za reviziju i kontrolu informacijskog sustava (eng. *Information Systems Audit and Control Association,* ISACA). S više od 110.000 članova u 180 zemalja, ISACA je vodeći svjetski pružatelj znanja, certifikata, zagovaranja i obrazovanja o informacijskim sustavima na područjima sigurnosti i osiguranja, korporativnog upravljanja, upravljanja informacijskom tehnologijom i informacijskim rizicima te usklađenošću s propisima i standardima vezanima uz informacijske tehnologije. Osnovana 1969, neprofitna i neovisna ISACA održava međunarodne konferencije, objavljuje ISACA Journal i razvija međunarodne standarde, revizije i kontrole informacijskih sustava, koji pomažu članovima u osiguravanju povjerenja u, te vrijednosti od, informacijskih sustava. ISACA također unaprjeđuje i potvrđuje informacijske vještine i znanja kroz globalno prihvaćene certifikate. [18]

Kontrolne preporuke za informacijske sustave i povezane tehnologije (eng. *Control OBjectives for Information and related Technology,* COBIT) definiraju radni okvir koji određuje način implementacije upravljanja informacijskim i komunikacijskim sustavima i tehnologijom. Kritični elementi važni za opstanak i uspjeh organizacije su efikasno upravljanje informacijskom i komunikacijskom tehnologijom, a ono se ogleda u:

- povećanju zavisnosti o informacijama i njima pridruženim sustavima,
- povećanju ranjivosti i širokom spektru prijetnji informacijskoj tehnologiji,
- obujmu i troškovima postojećih i budućih investicija u informacijske sustave,
- potencijalu tehnologija za promjenom
- rada organizacije i poslovne prakse,
- stvaranju novih prilika i reduciranju troškova. [19]

COBIT definira radni okvir upravljanja informatičkim sustavom tako da je zadovoljeno slijedeće:

- poslovni procesi organizacije su u skladu s arhitekturom i funkcijom informatičkog sustava,
- rizici koji nastaju neispravnim ili nepotpunim funkcioniranjem informatičkim sustavom su smanjeni,
- omogućeno je upravljanje rizicima funkcioniranja informatičkog sustava na zadovoljavajući način i omogućeno je korištenje informatičkih resursa na racionalan način,
- upravama kompanija pomaže razumjeti koncept upravljanja informatičkim sustavima,
- definira odgovornosti koje su potrebne za normalno funkcioniranje sustava,
- usklađuje sustav s regulatornim obvezama i
- organizira aktivnosti unutar informacijskog sustava na prihvatljiv način.

COBIT spaja poslovne i informatičke ciljeve, pružajući mogućnost da se metrikama prati zrelost informatičkog sustava (eng. *Maturity Model*). COBIT daje menadžmentu mogućnost optimizacije informatičkih resursa kao što su aplikacije, informacije, infrastruktura i ljudi. Praksa koju preporučuje COBIT je produkt konsenzusa znanja mnogih stručnjaka i proizvod je dobre prakse, primjenjive u bilo kojoj organizaciji. [19]

7.1. Osnovna terminologija

Radi boljeg razumijevanja potrebno je definirati značenje pojedinih termina koji se u dokumentu i u COBIT publikacijama često upotrebljavaju:

- kontrola (eng. *control*) – sigurnosna politika, procedure i prakse koje osiguravaju da će poslovni ciljevi biti ostvareni te da će neželjeni događaji biti detektirani i njihov učinak smanjen ili izdvojen;

- cilj primjene kontrole (eng. *control objective*) – očekivani rezultat ili svrha primjene određene kontrole;
- proces – cilj kontrole višeg nivoa (eng. *high level control objective*).

COBIT definira generički model informatičkih procesa koji se mogu pojaviti u jednom informatičkom sustavu i na taj način opisuje model funkcioniranja informatičkog sustava poslovnom i informatičkom menadžmentu. Da bi se uspostavilo uspješno upravljanje njime, nužno je da informatički menadžment implementira potrebne kontrole koje su definirane za sve COBIT-om definirane informatičke procese. Budući da su ciljevi primjene kontrola unutar COBIT-a organizirani po IT procesima, tada okvir zapravo daje stvarnu vezu između primijenjenih kontrola, procesa i upravljanja informatičkim sustavima. [19]

7.2. COBIT publikacije

COBIT kao produkt predstavlja niz publikacija namijenjenih slijedećim sudionicima u upravljanju informatičkim sustavima:

- Upravi i visokom menadžmentu (eng. *Bord Briefing on IT Governance*) - publikacija je pisana za osobe u upravi organizacija te objašnjava problematiku koja se odnosi na upravljanje informatičkim sustavima i odgovornosti koje oni imaju.
- Informatičkom i operativnom menadžmentu (eng. *Management guideliness*) publikacija koja pomaže pri pronalaženju odgovora na pitanje kako daleko treba ići u kontroli informatičkih procesa, kako mjeriti performanse, koje prakse primijeniti te kako i što uspoređivati i mjeriti.
- Informatičkim stručnjacima koji se brinu o direktnoj primjeni kontrola, informatičkim revizorima i sigurnosnim stručnjacima. [19]

Skup preporuka namijenjen sudionicima je slijedeći:

- "COBIT okvirni model (eng. *Framework*)" - objašnjava kako COBIT organizira ciljeve upravljanja i dobru praksu upravljanja u četiri domene i njima pripadajuće procese.
- "Kontrola ciljeva (eng. *Control objectives*)" - opisuje 4 domene, 34 procesa i 318 ciljeva kontrola te dobru praksu u upravljanju svim aktivnostima u informatičkim sustavima.
- "Kontrola prakse (eng. *Control practices*)" - publikacija nije sastavni dio COBIT 4.0 publikacije, ali je nadopunjuje s detaljima koji su potrebni u praksi upravljanja i revizije te opisuje 1549 dobrih praksi primjenom kojih se može doći do ciljeva primjenjenih kontrola.
- "Vodič za informacijsku sigurnost (eng. *IT Assurance guide*)" - publikacija nije u sastavu COBIT 4.0 publikacije, a opisuje generički pristup reviziji informatičkih sustava.
- "Vodič za provedbu informacijskog upravljanja (eng. *IT Governance Implementation Guide*)" - publikacija opisuje metodologiju za implementaciju COBIT standarda i bazira se na inačici 3 COBIT-a i još nije usklađena s inačicom 4.
- "COBIT Brzi početak (eng. *Quickstart*)" - publikacija definira reducirani skup (oko 20%) kontrola i procesa specificiranih COBIT 4.0 publikacijom, a namijenjena je manjim organizacijama.
- "COBIT Osnovna linija sigurnosti (eng. *Security baseline*)" - opisuje osnovne korake pri implementaciji sigurnosti informatičkih sustava i namijenjena je prvenstveno menadžmentu.
- "COBIT mapiranje (eng. *Mapping*)" - opisuje područja preklapanja COBIT standarda i ostalih standarda s područja upravljanja i sigurnosti informatičkih sustava. [19]

7.3. Opis procesa u COBIT-U

7.3.1. Slika informatičkog sustava u kojem je primijenjen COBIT

Okvir definiran COBIT-om se može predstaviti trodimenzionalnim prostorom odnosno kockom koja sumira sve što je definirano COBIT okvirom. Kocka upravo predstavlja integralni prostor koji međusobno povezuje ciljeve, resurse i aktivnosti, tako da se tri dimenzije kocke odnose na međusobno povezane poslovne zahtjeve, informatičke resurse i informatičke procese. Tako se može kazati da se tri dimenzije kocke odnose na ostvarenje poslovnih ciljeva koji generiraju poslovne zahtjeve:

a) učinkovitost,
b) tajnost,
c) integritet,
d) dostupnost,
e) pouzdanost i
f) usklađenost;

koji se mogu ostvariti informatičkim procesima:

a) koji su podijeljeni u domene i
b) za čiju implementaciju su potrebne određene aktivnosti;

pri čemu se informatički procesi odnose na resurse:

a) aplikacije,
b) informacije,
c) infrastrukturu i
d) ljudi.

Model definiran COBIT-om koji je podijeljen na domene može također biti prikazan petljom u kojoj se nalaze sve četiri domene sa svojim definiranim procesima. [19]

7.3.2. Način opisa procesa

COBIT specificira procese po domenama, a za svaki je proces opisano slijedeće:

- opći opis procesa u kaskadnom obliku,
- detaljne kontrole,
- upute za mjerenje i
- model zrelosti.

COBIT specifikacije se sastoje od uvodnog dijela i nakon toga slijede opisi svakog pojedinog procesa što predstavlja glavninu publikacije, pri čemu je svaki opis procesa podijeljen u četiri sekcije. [19]

Prva sekcija publikacije

Opis procesa je dan pomoću kaskadnog prikaza koji slijedi nakon definicije procesa gdje se uglavnom govori o tome zašto je proces potreban odnosno čemu i kome će služiti. Kaskadni prikaz je isti za sve definirane procese i ima slijedeći izgled:

Kontrola procesa

ime procesa

koji zadovoljava poslovne ciljeve

nabrojeni poslovni ciljevi (može ih biti više)

fokusirajući se na

nabrojeni najvažniji informatički ciljevi

koji mogu biti ostvareni pomoću

nabrojene glavne kontrole

i mogu biti mjereni

nabrojena metrika

Na istoj stranici su prikazani informatički kriteriji na koje taj proces ima utjecaj, odnosno kakav utjecaj proces ima na efikasnost, tajnost, integritet, dostupnost, skladnost i pouzdanost. Utjecaj procesa na njih može biti primaran i sekundaran.

U opisu procesa je također navedeno na koja područja upravljanja je fokusiran proces pri čemu njegov utjecaj može biti primaran i sekundaran.

Područja upravljanja su:

- strateško usklađivanje,
- upravljanje resursima,
- upravljanje rizikom i
- mjerenje performansi.

Isto tako su definirani informatički resursi (aplikacije, informacije, infrastruktura, ljudi) na koje se odnosi opisivani proces. [19]

Druga sekcija publikacije

U drugoj sekciji su opisani detaljni ciljevi kontrola (eng. *Detailed Control Objectiv*e) za drugu skupinu procesa. U ovom dijelu publikacije su točno definirani načini kontrole koje je potrebno primijeniti u praksi kako bi se procesi što lakše kontrolirali. [19]

Treća sekcija publikacije

Treća sekcija se odnosi na upute za upravljanje (eng. *Management guidelines*) koje su podijeljene u tri podsekcije.

U prvoj podsekciji opisani su ulazi i izlazi za neki proces, odnosno tabelarno su prikazane oznake pojedinih procesa i njihovi rezultati koji se koriste kao ulazi za opisivani proces, a isto tako su tabelarno prikazani rezultati (izlazi) opisivanog procesa koji mogu biti ulazi drugim procesima.

U drugoj podsekciji je prikazana tabela aktivnosti i funkcija, tzv. RACI (eng. *Responsible, Accountable, Consulted and Informed*) tabela kojom su opisane odgovornosti delegirane pojedinim osobama u procesu izvođenja akcija. Budući da tabela vrlo jasno prikazuje odgovornosti pojedinih ljudi (pozicija), primjenom RACI tablica definiranih COBIT-om se može osigurati potpuno izvođenje akcija, a isto tako i njihovo uklapanje u cijeli sustav obzirom na činjenicu da su RACI tablicom definirane i funkcije koje moraju biti konzultirane i informirane kao što je prikazano u Tablici 4.

Funkcije koje se mogu pojaviti u RACI tabeli mogu biti slijedeće:

a) generalni direktor - CEO (eng. *Chief Executive Officer*),
b) direktor financija - CFO (eng. *Chief Financial Officer*),
c) poslovni direktori,
d) direktor informatike - CIO (eng. *Chief information Officer*),
e) vlasnici poslovnih procesa,
f) voditelji produkcije,
g) glavni arhitekt informatičkog sustava,
h) voditelji projekata - PMO (eng. *Project Management Officer)* i
i) revizori, stručnjaci za sigurnost i svi oni koji se ne bave operativnim radom.

Odgovornost pojedine osobe za neku akciju je označena slovom R,A,C ili I, što znači:

- ✓ R – nadležan za izvođenje (eng. *responsible*),
- ✓ A – glavni odgovoran (eng. *accountable*),
- ✓ C – konzultiran (eng. *consulted*),
- ✓ I – informiran (eng. *informed*).

Treća podsekcija se odnosi na metriku, te su za svaki proces definirani ciljevi akcija, procesa i generalni informatički ciljevi na koje se neki proces odnosi. Za svaki od tri cilja definirana je metrika, odnosno indikatori postizanja ciljeva koji su ujedno i indikatori performansi višeg cilja. [19]

Četvrta sekcija publikacije

Četvrta sekcija se odnosi na model zrelosti i u njoj se na deskriptivan način opisuju uvjeti koji moraju biti ispunjeni da bi neki proces dobio ocjenu od 0 do 5, što je detaljnije analizirano u prijašnjim poglavljima. [19]

Tablica 4. Periodizacija dosadašnjeg razvoja koncepata informacijske sigurnosti [1]

Faza	Fokus	Značajke	Nositelj/sudionici
1	IT sigurnost	Isključivo IT sigurnost, osobito njeni tehnički aspekti	IT specijalisti
2	Sigurnost podataka	Širenje sigurnosti na baze podataka, IT sigurnost je postala dio upravljanja IT funkcijom	CIO IT specijalisti
3	Sigurnost informacija u IT-u	Širenje područja i standardizacija dijelova IT sigurnosti	CIO Inženjer za sigurnost IT specijalisti
4	Sustavi informacijske sigurnosti (ISMS)	Širenje sigurnosti na cjelokupnu informacijsku imovinu, Primjena normi za upravljanje informacijskom sigurnošću	Uprava Izvršni menadžment CSO CIO IT specijalisti Procjenitelji sigurnosti
5	Korporativna informacijska sigurnost	Primjena koncepata korporativne informacijske sigurnosti s pripadajućim procesima, organizacijskim strukturama te podizanje odgovornosti na najvišu poslovodnu razinu	Uprava Izvršni menadžment Odbor za sigurnost CSO CIO Specijalisti za sigurnost Procjenitelji za sigurnost

8. ZAKLJUČAK

Postoje mnogobrojni izvori prijetnji od napada na informacijsku imovinu, koji, ukoliko se dogode, a ne postoji uspostavljena dovoljno dobra informacijska sigurnost, mogu izazvati velike neželjene posljedice. Skupine takvih prijetnji su: tehničke pogreške, neautorizirani pristupi informacijskoj opremi ili podacima, prekidi u pružanju informacijske potpore poslovnim procesima, prirodne nepogode, fizička oštećenja, kompromitiranje podataka i informacija i sl.

Korporativna informacijska sigurnost bavi se identifikacijom problema i njihovim rješavanjem i kao takva, ključna je za poslovanje svakog poduzeća. U poslovnoj sigurnosti bitno je odrediti informatičke procese koji moraju biti usklađeni s korporativnim prioritetima, jer korporativni prioriteti imaju veliki utjecaj na konstrukciju informatičkog sustava. Standardi poslovanja određuju primjenu informacijskih usluga koje imaju utjecaj na neke od informacijskih čimbenika kao što su učinkovitost, pouzdanost, cjelovitost, dostupnost i usklađenost. Stoga pri definiranju informatičkih rješenja koja mogu podržati željene korporativne ciljeve potrebno je definirati informacijske procese koji se oslanjaju na ljudske potencijale i informatičku infrastrukturu.

U svrhu smanjenja rizika koji nastaju neispravnim ili nepotpunim funkcioniranjem informatičkih sustava, mislim da bi tvrtke i poduzeća trebali definirati odgovornosti koje su potrebne za normalno funkcioniranje sustava te zaštititi informacije o poslovnim procesima. Bitno je voditi računa o svim sigurnosnim segmentima poslovnog sustava: fizičkoj i tehničkoj sigurnosti, zaštiti intelektualnog vlasništva, zaštiti podataka i sigurnosti osoblja, jer samo holističkim pristupom možemo rizike od gubitka vitalnih informacija za poslovanje svesti na minimum i time osigurati kontinuirano poslovanje poduzeća. Važno je držati se zakonskih i regulatornih obveza koje postaju sve veće i sve teže za primjenu. Pojavom Opće uredbe o zaštiti podataka uvelike su povećana i bolje definirana prava korisnika, ali su logistički zahtjevi za poduzeća koja se bave sakupljanjem i obradom postali znatno veći, što u konačnici znači veće troškove.

9. LITERATURA

[1] Krakar, Z., „Korporativna informacijska sigurnost“ Fakultet organizacije i informatike, Varaždin, 2014.

[2] Panian, Ž., Strugar I., „Informatizacija poslovanja“ Ekonomski fakultet, Zagreb, 2013.

[3] Guru99, „Database vs Data Warehouse: Key Differences“, dostupno na: https://www.guru99.com/ (7. ožujka 2021.)

[4] CARNet CERT, „Cloud computing“, dostupno na: https://www.cis.hr/ (2. veljače 2021.)

[5] CARNet CERT, „ Sigurnost mobilnih mreža“, dostupno na: https://www.cis.hr/ (13. veljače 2021.)

[6] Narodne novine, „Zakon o informacijskoj sigurnosti“ (NN 79/07), dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[7] Narodne novine, „Zakon o tajnosti podataka“ (NN 79/07, 86/12), dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[8] Narodne novine, „Zakon o pravu na pristup informacijama“ (NN 25/13) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[9] Narodne novine, „Zakon o zaštiti osobnih podataka“ (NN 103/03, 118/06, 41/08, 130/11 i 106/12 - pročišćeni tekst), dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[10] Narodne novine, „Zakon o autorskom pravu i srodnim pravima“ (NN 167/03, 79/07, 80/11, 125/11, 141/13 i 127/14 - pročišćeni tekst), dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[11] Narodne novine, „Kazneni zakon“ (124/13, 81/13, 79/12, 57/11) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[12] Narodne novine, „Zakon o telekomunikacijama“ (NN 70/05, 60/04, 117/03, 158/03) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[13] Narodne novine, „Zakon o zaštiti potrošača“ (NN 41/14, 56/13, 78/12) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[14] Narodne novine, „Zakon o elektroničkoj ispravi“ (NN 150/05) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[15] Narodne novine, „Zakon o elektroničkom potpisu“ (NN 30/14, 89/13, 107/10, 80/08, 10/02) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[16] Narodne novine, „Zakon o elektroničkim komunikacijama“ (NN 71/14, 80/13, 133/12, 90/11, 73/08) dostupno na: https://narodne-novine.nn.hr/ (10. ožujak 2021.)

[17] YourEurope, „ Zaštita podataka na temelju Opće uredbe o zaštiti podataka“, dostupno na: https://europa.eu/ (6. travanj 2021.)

[18] ISACA, „ISACA International“ dostupno na: https://www.isaca.hr (25. ožujak 2021.)

[19] CARNet CERT, „COBIT metodologija“, dostupno na: https://www.cis.hr/ (5. ožujka 2021.)

10. PRILOZI

10.1. Popis slika

10.2. Popis tablica