Sigurnosni aspekti računovodstvenih sustava u oblaku

Drglin, Mateo

Sveučilište Jurja Dobrile u Puli

Mateo Drglin

Sigurnosni aspekti računovodstvenih sustava u oblaku

Završni rad

Pula, kolovoz 2024.

Sveučilište Jurja Dobrile u Puli

Mateo Drglin

Sigurnosni aspekti računovodstvenih sustava u oblaku

Završni rad

JMBAG: 0303088413, redovan student

Studijski smjer: Sveučilišni preddiplomski studij Informatika

Predmet: Poslovni informacijski sustavi

Znanstveno područje: Društvene znanosti

Znanstveno polje: Informatika

Znanstvena grana: Informatika i Računovodstvo

Mentor: izv. prof. dr. sc. Darko Etinger, sumentor: prof. dr. sc. Lorena Mošnja Škare

Pula, kolovoz 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Mateo Drglin, kandidat za prvostupnika smjera Informatika ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljeni način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

U Puli, 28.8.2024

IZJAVA O KORIŠTENJU AUTORSKOGA DJELA

Ja, Mateo Drglin dajem odobrenje Sveučilištu Jurja Dobrile u Puli, nositelju prava korištenja, da moj završni rad pod nazivom „Sigurnosni aspekti računovodstvenih sustava u oblaku“ upotrijebi da tako navedeno autorsko djelo objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te preslika u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

Potpis

_____

U Puli, 28.8.2024

Sadržaj:

1. UVOD

Računovodstvo je jedna od bitnih disciplina u današnjem poslovnom svijetu, koja prati i proučava poslovanje, odnosno planira, evidentira, kontrolira, analizira poslovne promjene i priprema računovodstvene informacije. Napretkom tehnologije i prilagođavajući se potrebama suvremenog poslovanja, dolazimo i do računovodstva u oblaku, koje koristi udaljene servere i softver dostupan preko interneta, što omogućuje mobilnost, povećanu efikasnost, povećanu kvalitetu poslovanja i smanjenu cijenu održavanja računovodstvenih servisa. Da bi oblak bio dostupan potrebna je internetska veza. Računovodstvo u oblaku je povećalo efikasnost, povećalo kvalitetu poslovanja i smanjilo cijenu održavanja računovodstvenih servisa.ponovljeno U tradicionalnom računovodstvu, koristio se lokalno instalirani računovodstveni softver na računalima tvrtke za vođenje administrativnih poslova[14] ili vlastite računovodstvene službe. Međutim, taj pristup je imao svoje nedostatke, uključujući i činjenicu da su svi bitni podaci bili pohranjeni na tim računalima, što je nosilo rizik od gubitka ili oštećenja podataka. Računovodstvo u oblaku je računovodstvo kod kojeg se koristi računovodstveni softver na udaljenom serveru koji nije u vlasništvu neke tvrtke.

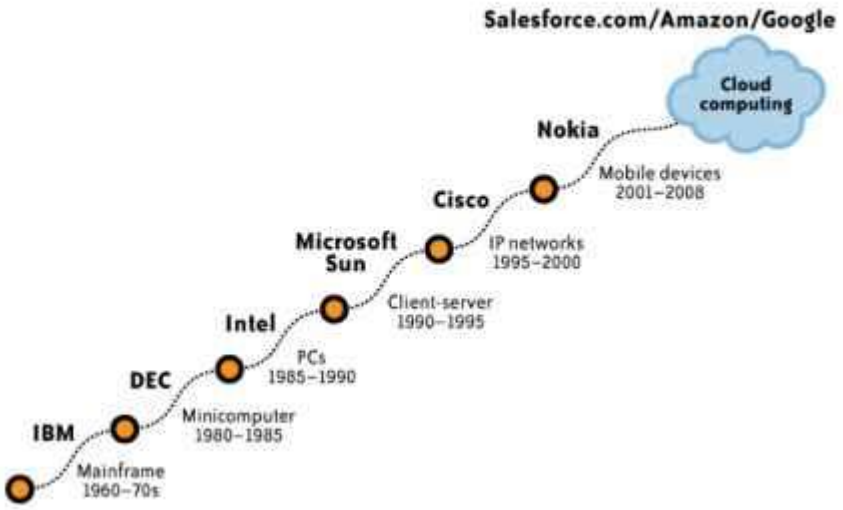
Pojam računovodstva u cloudu će se dodatno objasniti u nastavku.

Cilj ovog istraživanja je upoznati se dublje s konceptom računovodstva u oblaku, istražiti kako se oblak koristi kao tehnološka platforma za vođenje računovodstva te razumjeti prednosti i izazove koje donosi. Posebna pažnja biti će posvećena analizi sigurnosnih aspekata povezanih s korištenjem računovodstva u oblaku, Kroz ovo istraživanje, planiram stvoriti cjelovit uvid u kako oblak utječe na računovodstvo te identificirati najbolje prakse koje će omogućiti sigurno i učinkovito korištenje oblaka u poslovnom okruženju.

Ovaj diplomski rad sastoji se od 7 poglavlja, uključujući uvod i zaključak. U prvom dijelu obrađuje se povijest, definicije i karakteristike računovodstva u oblaku. Treće poglavlje detaljno opisuje računovodstvo u oblaku, prikazat će prednosti i nedostatke korištenja oblak servisa naspram tradicionalnog računovodstva. Četvrto poglavlje detaljno opisuje probleme sigurnosti oblaka kao što su prijetnje i koje se mjere trebaju poduzeti da bi se oblak osigurao.

2. Povijest razvoja računovodstvenog oblaka

Razumijevanje računalstva u oblaku zahtijeva razumijevanje njegove evolucijske putanje. Kao što je istaknuto u poznatom djelu Alvina Tofflera, "Treći val" (Bantam, 1980.), ljudski napredak je napredovao u fazama. On ih kategorizira u tri glavna vala: poljoprivredna društva, industrijsko doba i sadašnje informacijsko doba. Svaki od ovih valova sadrži značajne podvalove[30]. tijek informacijskog doba prikazan je na slici 1-1, započeto je s glavnim računalima, pa se prešlo na miniračunala i osobna računala, a trenutno smo na vrhu računalstva u oblaku.



slika 1: Podvalovi tijek.

izvor: Mather, T. Kumaraswamy, S. Latif, S., Cloud security and privacy: an enterprise perspective on risks and compliance. O' Reily, str. 312.

Time dolazimo i do računovodstva u oblaku. Pojam "računovodstvo u oblaku" prvi su iznijeli Ping i Xuefeng 2011 godine, a definirano je kao: „računalstvo u oblaku plus računovodstvo jednako je računovodstvo u oblaku."[1].

Prema Michael Cusmanu povijest računovodstvenog oblaka možemo pratiti još u 1990-ima kada se počeo pojavljivati popularni model za softverske aplikacije SaaS (Software as a Service). SaaS je model računalstva u oblaku koji omogućuje korisnicima pristup softverskim aplikacijama putem interneta, bez potrebe za instalacijom i održavanjem softvera na lokalnom računalu[15].

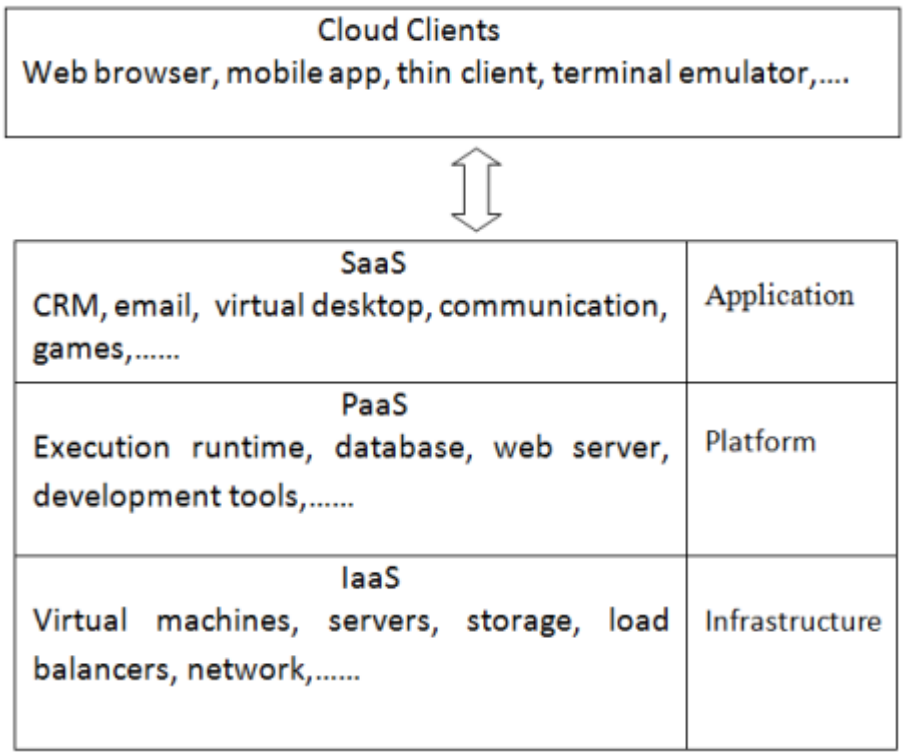
Korisnici mogu pristupiti aplikacijama putem web preglednika, što pojednostavljuje održavanje i podršku softvera jer se te zadatke obavlja na strani pružatelja usluga. SaaS se ponekad i naziva „softver na zahtjev", a Microsoft ga je ranije nazivao "softver plus usluge"[23]. Kako bi korisnici dobili pristup, potrebno je najčešće plaćati pretplatu nekom pružatelju usluga.

Sredinom 2000-ih do kasnih 2010-ih pružatelji usluga oblaka usredotočili su se na poboljšanje sigurnosti i povjerljivosti podataka. Počeli su sa uvođenjem sigurnosnih standarda i naprednih tehnologija, nakon implementacije bolje sigurnosti, povećalo se i povjerenje korisnika tih usluga oblaka[15].

Prema Bruce A. Phillipsu u zadnjem desetljeću računovodstvo u oblaku počelo se širiti sve više i više, te dobiva nove funkcionalnosti kao što su automatizacija procesa, analitika podataka i integracija s drugim poslovnim alatima[16].

Trenutačno računovodstvo u oblaku je postalo jako zastupljeno, mnoge tvrtke su već preuzele taj model u njihovom poslovanju jer nudi niže troškove, skalabilnost, mobilnost i poboljšanu sigurnost podataka.

Osim SaaS postoje PaaS (Platform as a Service) i IaaS (Infrastructure as a service)



Slika 2: prezentacija oblak usluga

Izvor: Khanom, Musammat Tahmina. (2017). Cloud Accounting: A Theoretical Overview. IOSR Journal of Business and Management. 19. 31-38. 10.9790/487X-1906053138.

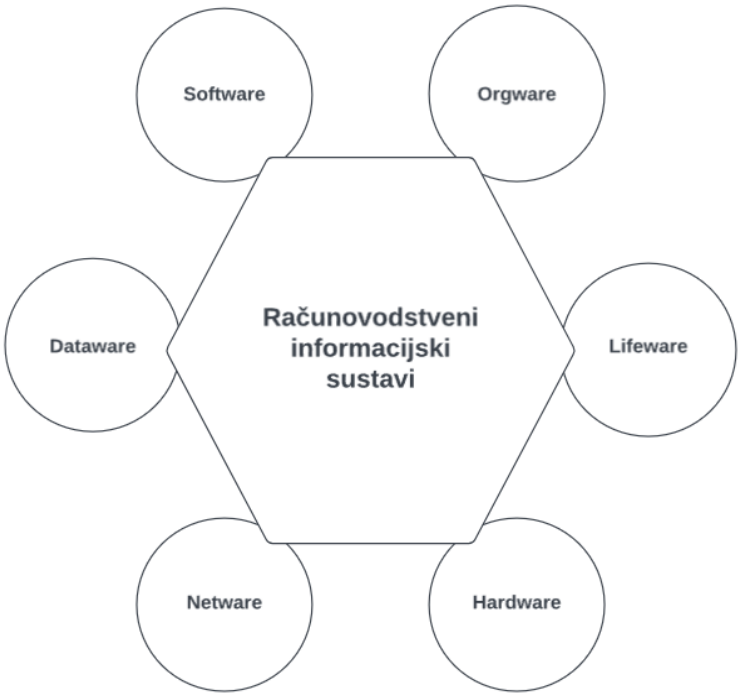
3. Računovodstveni sustav u oblaku

3.1 Računovodstveni informacijski sustav

Računovodstveni informacijski sustav predstavlja dio ukupnog informacijskog sustava u kojem se proizvode informacije neophodne za poslovno odlučivanje[2].

Računovodstveni informacijski sustav je sada dio svakog računovodstvenog poslovanja bez kojeg poslovanje nije moguće, RIS možemo definirati kao sveukupnost ljudi (lifever), opreme (hardver), računalnih programa (softver), pohranjenih podataka, načina i metoda njihove organizacije (dataver), komunikacijskih i mrežnih veza (netver) te organizacijskih postupaka (orgware), koji su ključni za prikupljanje, obradu i skladištenje financijskih podataka koji su potrebni za vođenje računovodstva[3]. Za lifever možemo uvrstiti sve ljudske resurse koji imaju neke uloge u informacijskom sustavu, to su najčešće programeri i administratori. Isto tako kao što u lifever uvrštavamo ljudske resurse u netveru ubrajamo svu komunikacijsku opremu i podršku. Hardver predstavlja fizičke odnosno materijalne dijelove računala, to se odnosi na komponente i opremu koje sačinjavaju računalo. Dok hardver predstavlja opipljivi ili fizički dio računala softver upravlja hardverom, te jedan bez drugog ne bi mogli postojati. Softver je po definiciji je skup podataka ili računarskih instrukcija koje računaru govore kako treba da radi. Dataver se odnosi na organizaciju podatkovnih baza i ostalih podataka, bitno je da se napravi dobra baza podataka za kvalitetno, brzo i jednostavno poslovanje. Za orgware možemo reći da je to skup informacijskih sustava koji služe za upravljanje internim procesima i operacijama organizacije.

Slikom 3 prikazani su elementi računovodstvenog informacijskog sustava i njihova povezanost



Slika 3: elementi RIS-A

Izvor: autor

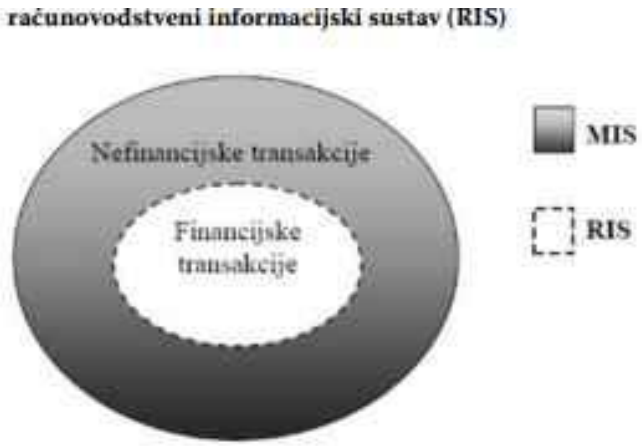
Računovodstvo kao informacijski sustav ima tri elementa [3]:

1. mjerenje ili kvantificiranje poslovnih događaja u novčanom izrazu te njihovo evidentiranje na kontima (input),
2. procesiranje ili obrada podataka u poslovnim knjigama i izrada financijskih izvještaja (računovodstveni proces) i
3. objavljivanje financijskih izvještaja, kojim računovodstvo komunicira s vanjskim i unutarnjim korisnicima financijskih izvještaja pružajući im informacije potrebne za poslovno odlučivanje (output).

Najčešće se susrećemo sa dva informacijska sustava a to su (upravljački) informacijski sustav i računovodstveni informacijski sustav.

Prema Robertu Zenzeroviću razlika između management (upravljačkog) informacijskog sustava i računovodstvenog informacijskog sustava jest u činjenici što su predmet ulaza u management informacijski sustav i nefinancijske transakcije, dok kod računovodstvenog informacijskog sustava to nije slučaj. Računovodstveni informacijski sustav bavi se isključivo financijskim transakcijama koje su ujedno zanimljive i za management informacijski sustav[19].

Dakle, unatoč njihovim razlikama, nefinancijske informacije u upravljačkom informacijskom sustavu i financijske informacije u računovodstveno informacijskom sustavu mogu biti međusobno povezane za korist nekog poslovanja. Integracijom ovih sustava možemo pružiti bolju sliku i razumijevanje za poboljšanje poslovanja.



Izvor: Zenzerović, R.: Računovodstveni informacijski sustavi, Pula, 2007., pg. 30

Slika 4: Upravljački i informacijski sustav

Izvor: Zenzerović, R.: Računovodstveni informacijski sustavi, Pula, 2007

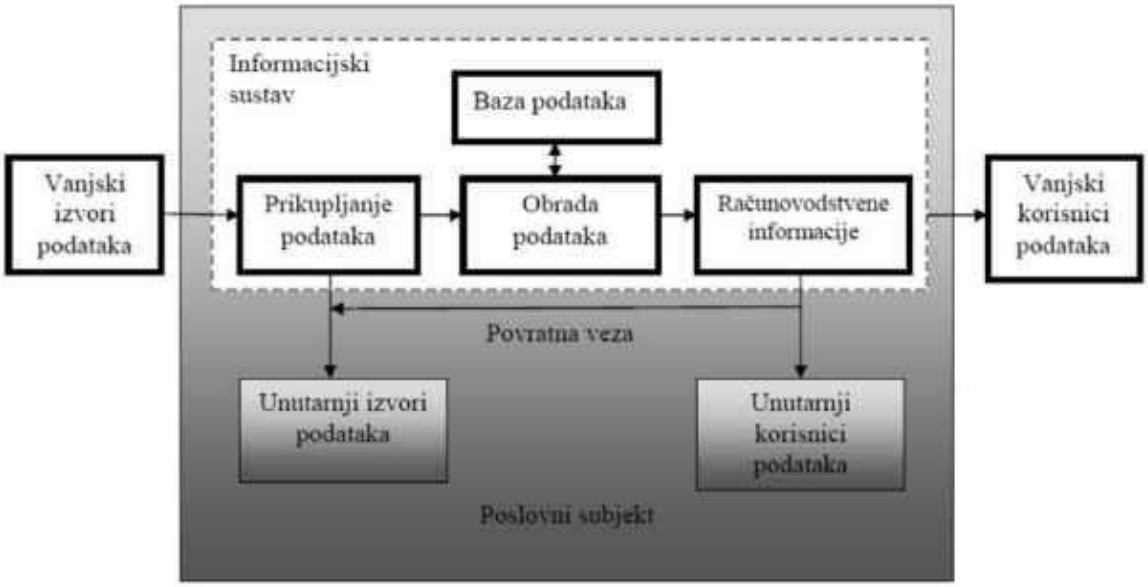
Danas računovodstveni informacijski sustavi prodaju se kao već izrađeni i spremni za korištenje softverski paketi od strane velikih dobavljača poput Microsoft, Oracle, Amazon, IBM gdje su konfigurirani i prilagođeni tako da odgovaraju svim poslovnim procesima organizacije. Računovodstveni informacijskih sustav je podsustav informacijskog sustava, iako je to podsustava računovodstvo je isto samostalni sustav sa svim potrebnim elementima – inputom, procesom i outputom, koji čine jedan sustav.

Tri ključna elementa sustava računovodstva su[3]:

1. mjerenje ili kvantificiranje poslovnih događaja, izraženo u novcu, te evidencija istih na kontima (input),

2. procesiranje, odnosno obrada podataka u poslovnim knjigama i izrada financijskih izvještaja (računovodstveni proces) ,

3. objavljivanje financijskih izvještaja (output).



Slika 5: Model računovodstveno informacijskih sustava

izvor: Gulin, D.: Računovodstvo. Hrvatska zajednica računovođa i financijskih djelatnika, Zagreb, 2003, str. 204.

Danas su računovodstveni informacijski sustavi zasnovani na oblaku sve popularniji i za mala i srednja poduzeća i za velike organizacije zbog nižih troškova, jednostavnosti i fleksibilnosti. Da bi računovodstveni sustav bio kvalitetan, potrebno je da ima djelotvornu zaštitu računalne opreme, programa i podataka, zatim točno, brzo i cjelovito procesiranje transakcija, izvještaja i drugih evidencija, efikasan način identifikacije i eliminacije netočnih izvora podataka, točne i cjelovite baze podataka[25].

-- Vezano za „Detaljnija razrada – v. Katarina Žager je pisala o RIS-u“ nažalost nisam uspio pronaći knjigu online a da nije potrebno kupiti

3.2 Računovodstvo u oblaku

Računovodstvo u oblaku odnosi se na korištenje računalnih resursa i softvera dostupnih putem interneta za vođenje knjigovodstvenih evidencija i izvješćivanje. Ta tehnologija omogućava organizacijama da pristupe svojim financijskim podacima putem interneta, bez potrebe za vlastitim IT infrastrukturama. Računovodstvo u oblaku je metoda kojom kompanije upravljaju i koriste svoje računovodstvene podatke. Tradicionalno, računovodstveni podaci bili su pohranjeni na lokalnim serverima i pristupa im se putem lokalno instaliranih računovodstvenih programa. No, trend se dramatično promijenio s porastom usvajanja računalstva u oblaku. Kada govorimo o računovodstvu u oblaku, mislimo na praksu korištenja virtualnih računovodstvenih sustava putem internetske veze. U ovom slučaju, softver i podaci se pohranjuju na serverima pružatelja usluga[14]. Korisnici pristupaju tim serverima putem interneta, omogućujući im da pregledavaju, mijenjaju i analiziraju financijske podatke s bilo kojeg mjesta koje ima internetsku vezu. Ključni aspekt računovodstva u oblaku je mogućnost korisnika da surađuju na dokumentima u stvarnom vremenu. To znači da se više korisnika može prijaviti u sustav i raditi na istom dokumentu ili skupu podataka istodobno. To poboljšava produktivnost, učinkovitost i točnost računovodstvenih procesa [8].

3.2.1 Servisni modeli

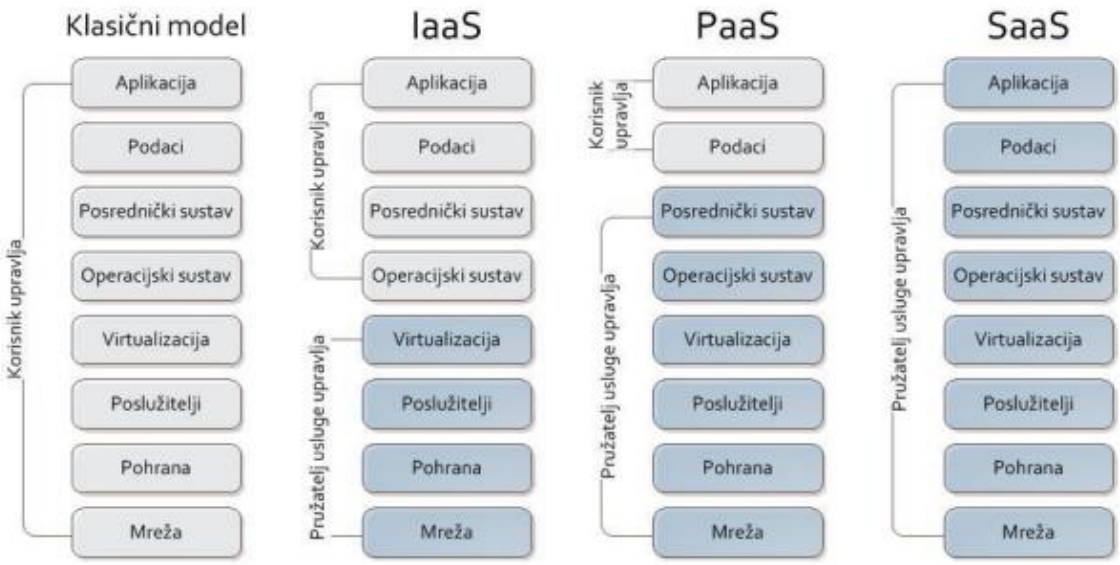
Oblak se sastoji od različitih modela usluga a to su Softver kao usluga(SaaS), Platforma kao usluga(PaaS) i Infrastruktura kao usluga(IaaS).

Softver kao usluga (SaaS - eng.Software as a service) jest softver koji se licencira na pretplatnoj osnovi i koji se nalazi na centralnoj lokaciji (kao npr. na serveru pružatelja usluga)[22]. Glavna prednost SaaS računovodstvenog pristupa je u tome što omogućuje online korištenje računovodstvenog programa bez potrebe za lokalnom instalacijom softvera. Sa prednostima postoje i nedostaci, a jedan od ključnih nedostataka SaaS usluga jest da se podaci korisnika čuvaju kod pružatelja usluga u oblaku, zbog čega bi korisnici mogli biti zabrinuti za privatnost i sigurnost svojih podataka. Kako bi se riješili ti problemi, pružatelji usluga osiguravaju svoje korisnike pružajući niz sigurnosnih metoda, kao što su enkripcija podataka, sigurnosne kopije i stroge kontrole pristupa usluzi u oblaku.

Platforma kao usluga (PaaS - eng.Platform as a service) je softver u kojem se nudi cijela platforma, ona uključuje resurse poput operativnog sustava, programskog jezika, baze podataka, web poslužitelja koji se automatski skalira kako bi zadovoljio zahtjeve aplikacije[24]. U PaaS-u pružatelj usluga pruža usluge za servere, pohranu, bazu podataka i mrežu, ukratko, pružatelj usluga pruža korisnicima sve usluge koje su im potrebne. PaaS isto tako pojednostavljuje i olakšava lakoću korištenja aplikacije, te smanjuje troškove upravljanja aplikacijom.

Infrastruktura kao usluga (IaaS - eng.Infrastructure as a Service) je softver pri kojem se osnovna računalna infrastruktura poslužitelja, softvera i mrežne opreme pruža kao usluga na zahtjev na kojoj se može razviti platforma i uspostaviti izvršavanje aplikacija. Njegova glavna svrha je izbjegavanje kupnje, smještaja i upravljanja osnovnim

hardverom i softverom infrastrukturne komponente i umjesto toga korištenje tih resursa kao virtualiziranih objekata kojima se može upravljati putem njegovog sučelja.[10].

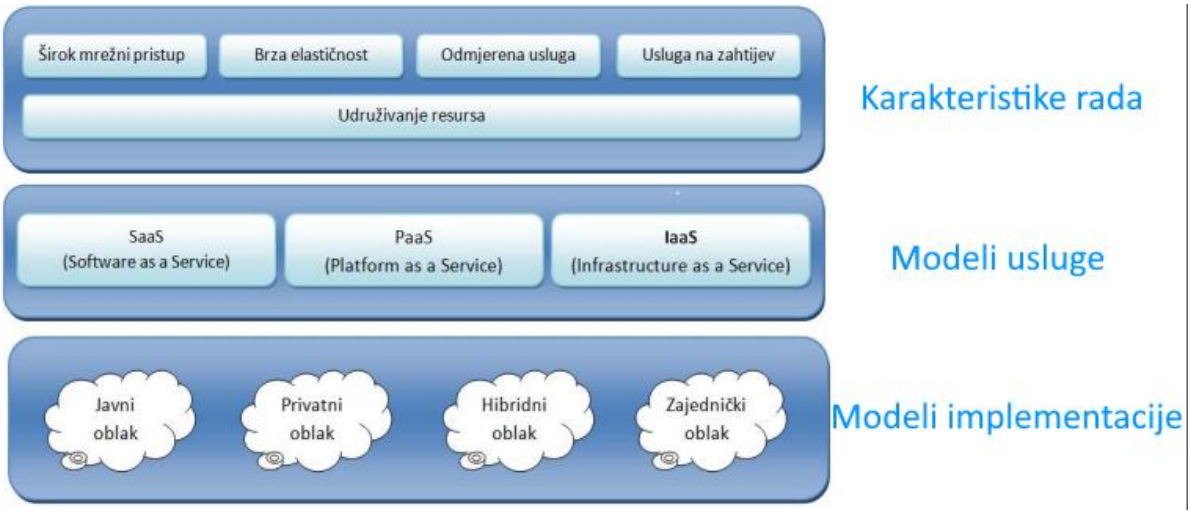


Slika 6: Modeli računarstva u oblaku

izvor: NCERT-PUBDOC-2010-03-293 dostupno na:
https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf

3.2.2 Modeli implementacije

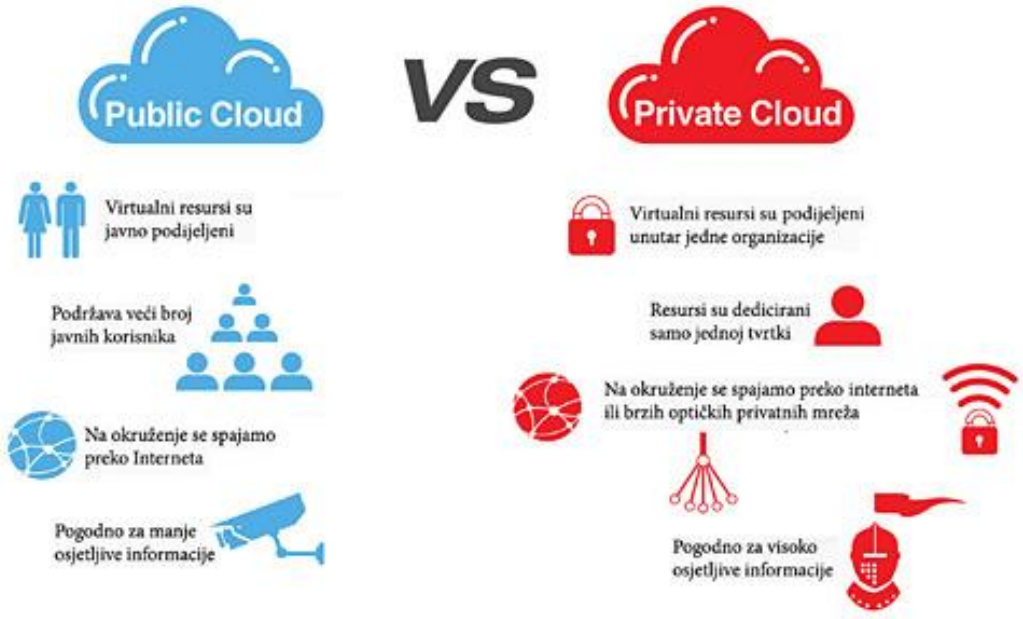
Osim što imamo servisne modele usluga, imamo i 4 različita modela implementacije tih usluga, a to su javni, privatni, hibridni i zajednički oblak.



slika 7. Karakteristike, modeli i implementacije usluge oblaka

izvor: NCERT-PUBDOC-2010-03-293 dostupno na:
https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-03-293.pdf

Javni oblak (eng. Public Cloud) - cloud computing platforma dostupna i otvorena za javnost, neovisno o tome radi li se o pojedincima ili organizacijama. U vlasništvu je tvrtke koja prodaje cloud computing usluge, aplikacije različitih korisnika često se nalaze na istim poslužiteljima, sustavima za pohranjivanje i mrežama[5]. Javni oblak omogućuje korisnicima lagani pristup za relativno malu cijenu i bez ikakve potrebe za održavanjem. Neki od problema kod javnog oblaka su što hakeri mogu pristupiti podacima, zato što podaci nisu unutar tvrtke nego su kod poslužitelja usluge. Neke od pretnja su krađe identiteta, slaba autentifikacija, manjak enkripcije i unutrašnji napad od strane zaposlenika, administratora ili slično.
Privatni oblak predviđen je isključivo za upotrebu od jedne organizacije i nitko drugi, te se cijeli oblak nalazi u privatnoj mreži koja ima svoj hardver i softver. Organizacija koja koristi privatni oblak ima oblak samo unutar organizacije, te mogu samostalno upravljati vlastitim oblakom bez potrebe, to im daje bolju fleksibilnost i kontrolu. Iako su privatni oblaci cijenovno dosta skupi uspoređujući javni oblak, oni nude mnoge prednosti kao što su visoka sigurnost, kontrola samog oblaka i fleksibilnost.

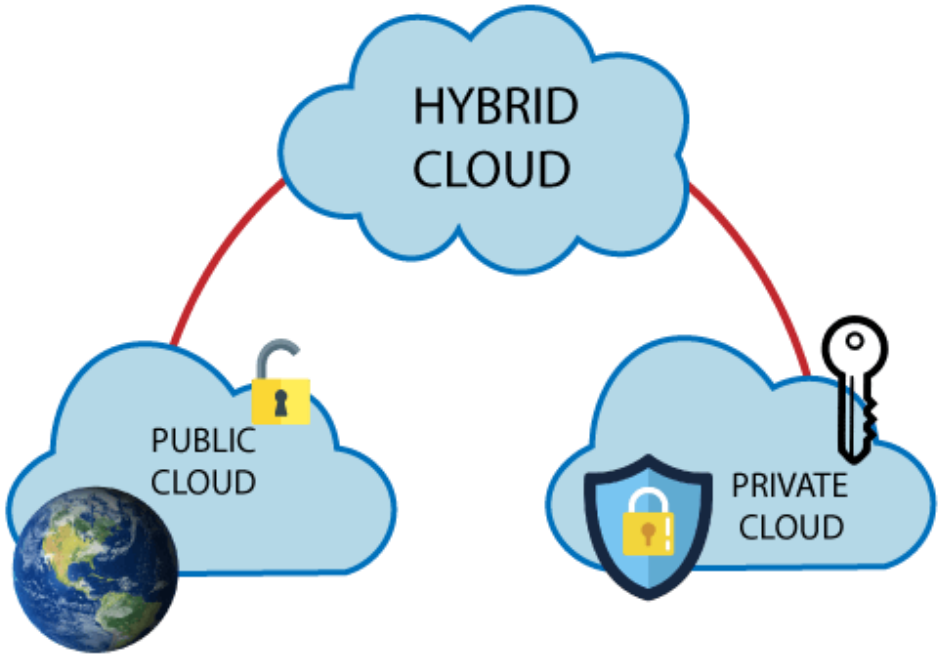


Slika 8: Javni i privatni oblak

Izvor: Info trend (2018) Privatni oblak – skupa autonomija. Dostupno na: http://www.infotrend.hr/clanak/2015/9/privatni-oblak---skupa-autonomija,86,1197.html (15.08.2018.)

Ako poduzeće koristi elemente javnog i privatnog oblaka radi fleksibilnosti za to postoji oblak koji se naziva hibridni oblak. Taj model uzima najbolje što privatni i javni oblak nude. Organizacija ima mogućnost spremanja bitnih podataka u privatni oblak koji nudi sigurnost, te kada organizacija treba dodatnog prostora ili spremanju sigurnosnih kopija koje nisu jako kritične za tvrtku.

Prema Microsoftu prednosti hibridnog oblaka uključuju dodatnu, jedinstvenu funkcionalnost poznatu kao "Cloud bursting". To je kada aplikacija ili resurs koji se izvodi unutar privatnog oblaka doživi skok upotrebe, uzrokujući da se probije u javni oblak kako bi iskoristio prednosti dodatnih alata[7]. Statistički gledano hibridni oblak ima vidljivo najveću korištenost naspram ostalim oblacima[6].

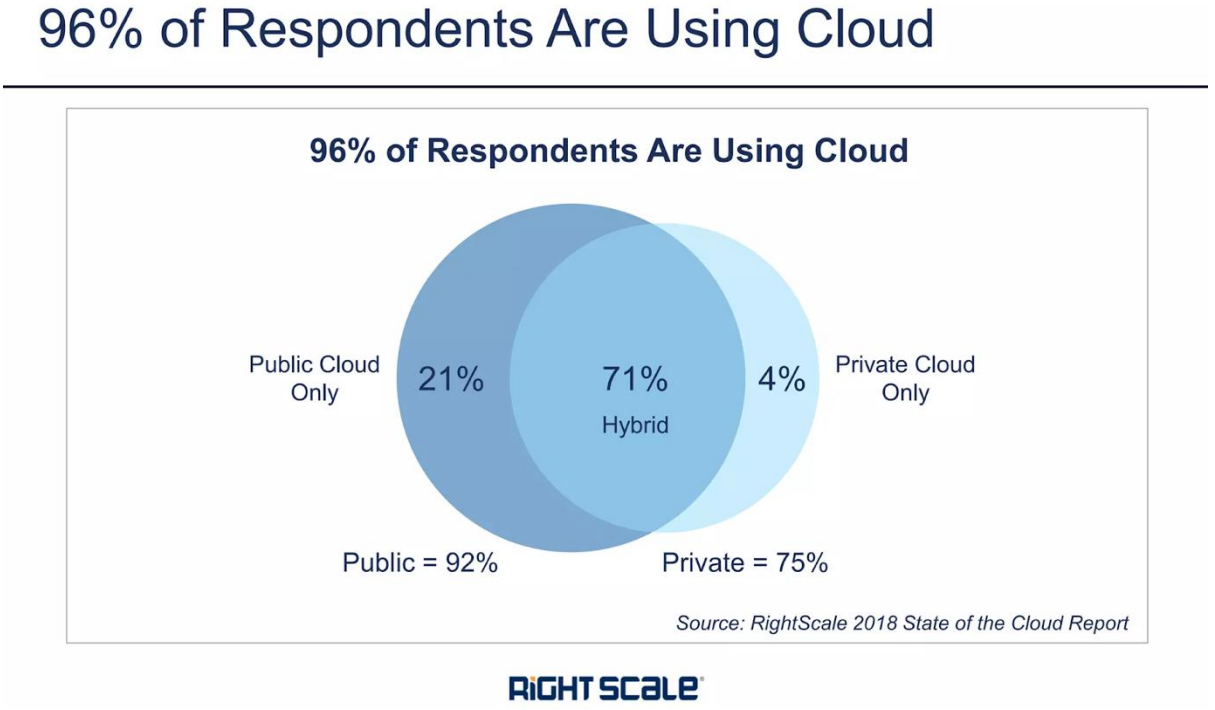


Slika 9: Hibridni oblak

Izvor: https://www.javatpoint.com/hybrid-cloud

Glavne prednosti hibridnog oblaka[7]:

1. Kontrola: organizacija može održavati privatnu infrastrukturu za osjetljivu imovinu ili radna opterećenja koja zahtijevaju nisku latenciju.
2. Fleksibilnost: mogu se iskoristiti dodatni resursi u javnom oblaku kada trebaju.
3. Isplativost: mogućnost skaliranja na javni oblak, dodatnu računalnu snaga plaća se samo kada je potrebna.
4. Lakoća : prijelaz na oblak ne mora biti naporan jer se može migrirati postupno dodajući radna opterećenja tijekom vremena.

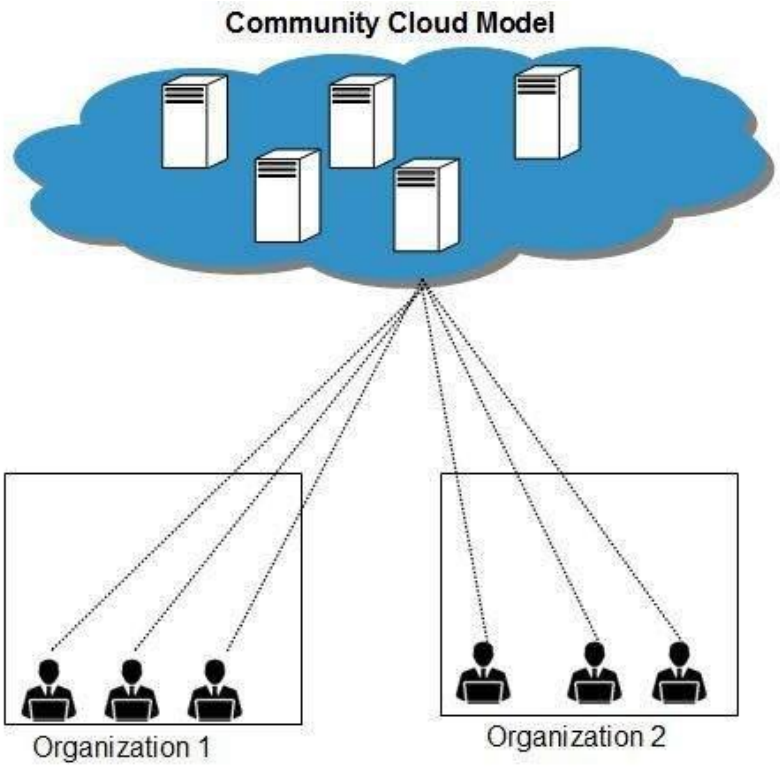


Slika 10: Statistika korištenja cloud usluga

Izvor: RightScale 2018 State of the Cloud Report

Osim privatnog, javnog i hibridnog oblaka postoji i zajednički oblak. U tome oblaku više organizacija dijele infrastrukturu, resurse i usluge toga oblaka. Oblak je namijenjen korisnicima koji imaju zajedničke interese ili brige(npr. misija, sigurnosni zahtjevi, politika i razmatranja sukladnosti). Njime mogu upravljati organizacije ili treća strana i može postojati u prostorijama ili izvan njih[17].

Međutim, zajednički oblak postavlja i različite izazove kao što su privatnosti i sigurnosti oblaka. Budući da više korisnika dijeli istu infrastrukturu, postoji potencijalni sukob interesa i rizik od neovlaštenog pristupa podacima drugih korisnika oblaka. Kako bi se očuvala sigurnost i privatnost podataka, davatelji usluga oblaka moraju implementirati odgovarajuće sigurnosne mjere, kao što su stroga segmentacija mreža, enkripcija podataka i pravilno upravljanje pristupom.



Slika 11: zajednički oblak

Izvor: tutorialspoint, cloud computing community cloud model, dostupno na: https://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm

3.2.1 prednosti

Računovodstvo koje se temelji na oblaku jest jedan od najvećih napredaka koji se pojavio u računovodstvenom informacijskom sustavu. Ovaj model nudi niz prednosti koje pojednostavljuju, ubrzavaju i poboljšavaju računovodstvene postupke. Korištenje računovodstva u oblaku također olakšava rad u timovima zato što računovodstvo nije vezano za samo jedno lokalno računalo. Budući da svi u timu mogu pristupiti istim podacima odjednom, više nema potrebe za čestim ažuriranjem i usklađivanjem među različitim korisnicima ili odjelima.

Uvođenjem računovodstva u oblaku možemo značajno smanjiti operativne troškove. Korištenjem tog modela eliminira se potreba za velikim kapitalnim investicijama u hardver i softver, jer korisnici plaćaju samo ono što koriste, isto tako jedno od važnijih prednosti je da računovodstvo u oblaku omogućuje korisnicima mogućnost pristupa financijskim podacima u stvarnom vremenu, što olakšava pravovremeno izvještavanje i brže donošenje odluka.

Kada je u pitanju sigurnosno kopiranje podataka i restauracija podataka, računovodstvo u oblaku ima veliku prednost naspram tradicionalnom računovodstvu zato što automatski radi sigurnosne kopije. Prije je bilo potrebno posvetiti se pripremama sigurnosnih kopija što se trebalo obavljati u radnom tjednu. Trebalo je

ručno napraviti sigurnosnu kopiju nedavnih računovodstvenih podataka. Računovodstvo u oblaku omogućuje automatsku izradu sigurnosnih kopija podataka, uklanjajući mogućnost da se to zaboravi učiniti i smanjuje se mogućnost pravljenja ljudskih pogrešaka.

Računovodstveni podaci automatski se sigurnosno kopiraju i spremaju na neko drugo mjesto. To pomaže u zaštiti informacija u slučaju provale, požara ili drugih incidenata kojima bi se moglo izgubiti osjetljive i važne informacije. Ukoliko tvrtka iskusi jedan od ovih incidenata, pružatelj usluga temeljen na oblaku može pomoći u vraćanju podataka, ponovnim uspostavljanjem poslovanja može minimizirati negativan utjecaj i neugodnosti za kupce[9].

3.2.2 Nedostaci

Prema Nabil Sultanu s rastućom prevalencijom digitalizacije poslovnih procesa, računovodstvo oblaku se ističe kao vodeća inovacija koja obećava povećanje efikasnosti, fleksibilnosti i smanjenje operativnih troškova. Međutim, iako ima očite prednosti, računovodstvo u oblaku suočava se s nizom nedostataka i izazova, uključujući sigurnosne izazove, nedostatak kontrole, probleme s pouzdanošću, potencijal za tehničke probleme i nedostatak prilagodbe[12].

Ključne prepreke u prihvaćanju računovodstva u oblaku je sigurnost podataka, što se odnosi na probleme kao što su hakiranje, gubitak ili curenje podataka i slično. Iako pružatelji usluga u oblaku uvijek nastoje ojačati sigurnosne protokole, ovi problemi još uvijek sprječavaju potpuno preuzimanje ove tehnologije.

Hakerski napadi su jedan od glavnih sigurnosnih izazova sa kojima se suočava računovodstvo u oblaku. Poduzeća koja prelaze na cloud računovodstvo prenose svoje osjetljive financijske podatke na servere treće strane, čime se povećava rizik od hakerskih napada [20]. Iako većina pružatelja usluga u oblaku ima robusne sigurnosne protokole, nijedan sustav nije potpuno imun na napade. Osim toga, može doći i do zlouporabe podataka od strane neovlaštenih korisnika unutar ili izvan neke organizacije.

Neovlašteni pristup ili curenje podataka mogu dovesti do financijskih gubitaka, kršenja odredbi o privatnosti podataka i narušavanja reputacije. Još jedan od izazova je nedostatak kontrole, prenošenjem podataka poduzeća na servere pružatelja usluga. Korisnici oblaka nemaju pristup niti fizičku kontrolu nad hardverom i drugim resursima koji pohranjuju i obrađuju njihove podatke i informacije[11]. Tehnički problemi, poput hardverskih kvarova ili prekida mreže mogu dovesti do nedostupnosti usluga ili čak mogućeg gubitka podataka čime može doći do ozbiljnih problema za poduzeće. Međutim, oblak usluge su sve više zastupljenije i razvijaju se, te pružatelji usluga nastoje učiniti oblak usluge sve pristupačnijima i sigurnijima za buduće korisnike.

4. Sigurnosti u cloudu

U današnje vrijeme sigurnost u oblaku predstavlja ključnu brigu za pojedine korisnike i za organizacije koje koriste računalstvo u oblaku. Sigurnost u oblaku odnosi se na zaštitu podataka, resursa i aplikacija koje se nalaze na udaljenim serverima koje kontroliraju pružatelji usluga oblaka. Sigurnost u oblaku nije samo odgovornost pružatelja usluga, već i krajnjih korisnika koji moraju razumjeti svoje uloge i odgovornosti u zaštiti svojih podataka i resursa.[13]. U sigurnosti u oblaku svako ima svoju odgovornost, one se razlikuju ovisno koji model usluge koriste. Usluge koje se koriste su Infrastruktura kao usluga (IaaS), Platforma kao usluga (PaaS) ili softver kao usluga (SaaS).

slika 12: Bitni aspekti sigurnosti u oblaku

izvor: https://www.mieuxtechnologies.com/cloud-security-services/

4.1 Prijetnje u cloudu

4.1.1 Gubitak i curenje podataka

Gubitak podataka predstavlja neželjeni ili nenamjerni gubitak ili uništenje informacija koje su pohranjene na digitalnim medijima. Prijetnje podacima radnje su koje mogu utjecati na cjelovitost, povjerljivost ili dostupnost podataka tvrtke ili ustanove, a curenje podataka povjerljive podatke izlaže danim okruženjima. Prijetnje koje su zastupljene na oblaku su računalni napadi, zlonamjerni softveri, interni rizici, krađe identiteta, nehotično izlaganje i ucjenjivački softveri, Da bi se podaci osigurali od mogućih prijetnji primjenjuju se razne metode zaštite. Prevencija gubitka podataka odnosi se na strategiju koja pomaže organizacijama u otkrivanju i sprječavanju neovlaštenog prijenosa ili otkrivanja osjetljivih informacija. To može uključivati tehnologije, alate i postupke koji nadziru, upravljaju i štite podatke koji se koriste, obrađuju ili pohranjuju

unutar organizacije. Rješenja za sprječavanje gubitka podataka (Data Loss Prevention - DLP) nude niz prednosti koje omogućuju organizacijama da zaštite svoje osjetljive i povjerljive informacije. prednosti DLP alata za sprječavanje gubitka podataka su[28]:

1. Klasifikacija i Nadzor Povjerljivih Podataka: Prepoznavanje i primjena pravila na osjetljive podatke omogućuje bolju zaštitu i usklađenost s politikama sigurnosti.
2. Otkrivanje i Blokiranje Sumnjivih Aktivnosti: DLP rješenja prate podatke koji protječu kroz mrežu i mogu blokirati neovlašteno slanje ili kopiranje, poput e-maila ili USB pogona.
3. Automatizacija Klasifikacije Podataka: Automatsko prikupljanje informacija o dokumentima, poput njihovog stvaranja, pohrane i dijeljenja, poboljšava kvalitetu klasifikacije i primjenu pravila za sprječavanje gubitka podataka.
4. Održavanje Usklađenosti s Propisima: DLP omogućuje izvješćivanje koje olakšava usklađenost s regulativama kao što su HIPAA, SOX i FISMA, uključujući planove zadržavanja podataka i programe obuke za zaposlenike.
5. Nadzor nad Pristupom Podacima i Njihovim Korištenjem: Kontrola pristupa temeljena na ulogama i upravljanje digitalnim identitetima omogućuje bolje praćenje tko ima pristup čemu, time se spriječavaju interna kršenja i prijevare.
6. Poboljšanje Vidljivosti i Kontrole: DLP pruža uvid u tko možda šalje povjerljive podatke neovlaštenim korisnicima i omogućuje dodatne analize i prilagodbe za jačanje mjera računalne sigurnosti.

4.1.2 Privatnost i povjerljivost podataka

Iako se pojmovi "zaštita podataka" i "privatnost podataka" ponekad koriste kao sinonimi, postoji značajna razlika između njih dvoje. Dok zaštita podataka nudi alate i propise za stvarno ograničavanje pristupa podacima, privatnost podataka određuje tko ima pristup podacima. Od tvrtki se traži da poduzmu korake za zaštitu osjetljivih korisničkih podataka, a zahtjevi usklađenosti pomažu osigurati da tvrtke poštuju zahtjeve korisnika za privatnošću[27]. Zaštita podataka je ključan aspekt u upravljanju informacijama i odnosi se na prakse i mjere koje se primjenjuju kako bi se osiguralo da su podaci zaštićeni od neovlaštenog pristupa i oštećenja. Za razliku od zaštite podataka, koja se fokusira na tehničke i proceduralne aspekte osiguravanja podataka, privatnost podataka je više usmjerena na etičke i pravne obveze vezane uz informacije koje se odnose na pojedinca.

4.1.3 Zlouporaba oblak usluga

Zlouporaba i neželjena upotreba oblak usluga predstavljaju ozbiljne sigurnosne izazove s kojima se suočavaju korisnici i pružatelji usluga oblaka. Kako se tehnologija razvija, tako i metode zlouporabe postaju naprednije. Zlouporaba oblak usluga postaje sve složenija i promjenjiva. Loša implementacija oblaka, lažne prijave na oblak usluge su neki od primjera zlouporabe oblak usluga. Pružatelji usluga moraju pružiti korisnicima moguća rješenja koja se mogu primijeniti u slučaju neke prijetnje, također korisnici trebaju imati opciju prijave incidenata.

4.1.4 Krađa identiteta

Krađa identiteta ozbiljan je zločin koji uključuje neovlašteno korištenje tuđeg identiteta, često s namjerom da se postigne financijska dobit ili da se izbjegne odgovornost. Phishing je jedna od metoda koju kriminalci često koriste, to su lažne e-mail usluge i web stranice koje izgledaju kao legitimne usluge kako bi od korisnika izvukli osjetljive informacije npr (lažni facebook email koji obavještava korisnika o sumnjivim aktivnostima te ga traži da promjeni šifru. Isto tako postoje spyware i malware oni su zlonamjerni softveri koji mogu biti instalirani na uređaju žrtve, te tako neopaženo prikuplja njihove informacije.[21].

4.2 Osiguranja u cloudu

4.2.1 Fizičko čuvanje podataka

Fizičko čuvanje podataka odnosi se na korištenje fizičkih uređaja i medija, kao što su tvrdi diskovi, magnetne trake, CD-ovi, DVD-ovi i drugi oblici medija za pohranu, za spremanje digitalnih informacija. Fizičko čuvanje više nije toliko potrebno od kad je došao oblak, s obzirom na sve veću dostupnost i pouzdanost digitalnih sistema za skladištenje podataka koji omogućavaju pristup informacijama iz bilo kojeg dijela svijeta i olakšavaju dijeljenje resursa među korisnicima.

4.2.2 Automatsko sigurnosno korištenje (backup)

Zaštita podataka važan je aspekt koji se temelji na sigurnosnom kopiranju naših podataka. U slučaju gubitka ili oštećenja podataka, redovite sigurnosne kopije osiguravaju da možemo brzo dohvatiti svoje podatke. Dobra praksa je često raditi sigurnosne kopije lokalno i na oblaku, u slučaju da se nešto desi uvijek možemo vratiti podatke uz minimalne ili nikakve štete. Osim odabira prave sigurnosne kopije, trebali biste također uzeti u obzir vrstu sigurnosne kopije koju izvodite. Inkrementalne sigurnosne kopije spremaju samo promjene napravljene od zadnje sigurnosne kopije, dok pune sigurnosne kopije stvaraju potpunu kopiju vaših podataka. Kombinacija obje vrste može pomoći u postizanju prave ravnoteže između prostora za pohranu i vremena oporavka[27].

4.2.3 Enkripcija podataka

Podaci se procesom enkripcije pretvaraju se u šifru koju mogu čitati samo ovlaštene osobe. Upotrebom te tehnologije može se spriječiti krađa podataka i neovlašteni pristup, to čini enkripciju ključnim dijelom zaštite podataka[27]. Za enkripciju možemo reći da je kao pisanje tajnog pisma koje samo željena osoba može pročitati, koristeći posebne ključeve i algoritme za kodiranje i dekodiranje. Koristi se za zaštitu osjetljivih informacija kao što su lozinke, kreditne kartice i osobni podaci.

4.2.4 Ostale sigurnosne mjere

Timovi za sigurnost neprestano su fokusirani na nove prijetnje i rade na jačanju konfiguracija resursa u oblaku direktno u kodu kako bi smanjili broj problema sa sigurnošću koji dospijevaju u produkcijska okruženja. Važno je objediniti vidljivost stanja sigurnosti za DevOps te minimizirati mrtve kutove kroz uvide u stanje sigurnosti na različitim DevOps platformama. Da bi se postigla veća sigurnost, potrebno je pomicati fokus na sigurnost u ranijim fazama procesa, omogućavajući timovima za sigurnost i razvoj da usko surađuju. Na taj način, sigurnost se integrira direktno u kod, osiguravajući da su nativne aplikacije u oblaku sigurne od samog početka[29].

5. Sigurnosni aspekti

5.1 Identifikacija i autentifikacija korisnika

Autentifikacija je testiranje ili usklađivanje dokaza identiteta korisnika da bi se osiguralo da korisnik dokaže da je to zapravo on. Na primjer korisnik se pokušava prijaviti na neku stranicu i korisnik onda treba predati svoj email i šifru da se prijavi. Postoje različite vrste autentifikacija kao što su[33]:

1. Korisničko ime i lozinka: To je najčešća metoda autentifikacije koja zahtijeva unos korisničkog imena i lozinke. Kada se korisnik prijavi, sustav uspoređuje unesene podatke s pohranjenim vjerodajnicama u bazi podataka kako bi provjerio korisnikov identitet.
2. Višefaktorska autentifikacija: Ovo je napredna metoda koja zahtijeva više od jednog načina provjere identiteta. Obično uključuje nešto što korisnik zna (lozinka), najčešće se koristi (npr. mobilni uređaj) i biometrijski podaci kao dokaz da je to zaista on.
3. Biometrijska autentifikacija: Ova metoda koristi fizičke karakteristike korisnika za provjeru identiteta, kao što su otisak prsta, prepoznavanje lica, skeniranje šarenice ili prepoznavanje glasa.
4. Kartična autentifikacija: Korisnici koriste kartice ili pametne kartice koje sadrže identifikacijske podatke za pristup sustavu.
5. Certifikati i ključevi: Koristi se kod digitalnih potpisa i SSL/TLS certifikata za provjeru autentičnosti i integriteta podataka.
6. Javni i privatni ključevi: Metoda kriptografske autentifikacije koja koristi javni ključ za enkripciju i privatni ključ za dekripciju podataka.

U brojnim poduzećima gdje se odvija mnogo poslovnih procesa koji koriste podatke iz nekoliko autorizacijskih razina, potrebno je mnogo aplikacija koje su ih sposobne obrađivati, s time da svaka od njih ima specifične funkcionalnosti koje ne trebaju biti dostupne svim zaposlenicima. Tako je osmišljen sustavi jednostruke prijave čija filozofija rada se može realizirati na dva načina:[26]

1. putem dupliciranja korisničkih imena i lozinki koji se stavljaju u bazu podataka za svaku aplikaciju
2. tijekom prijave korisnika podatke proslijediti svim aplikacijama koje zaposlenik ima pravo koristiti na temelju svoje uloge u poduzeću.

5.2 Upravljanje pristupom i ovlaštenjima

Svrha upravljanja pristupom i ovlaštenja je odbijanje pristupa računalnim resursima koji pokušavaju pristupiti nelegitimnim putem. Dodatni problemi koje treba riješiti uključuju pokušaje upada zlonamjernih entiteta za kontrolu, uništavanje ili oštećenje računalnih resursa. Dok se dostupnost čuva, isto tako potrebno je održavati povjerljivost i integritet. Zahtjevi za ovu kategoriju trebaju imati rješenje kako osigurati da su računalni resursi dostupni ovlaštenim korisnicima kada je to potrebno[17].

Ovlaštenje ili autorizacija je proces nakon uspješne autentifikacije koji određuje ovlaštenja korisnika. Ovlaštenje se odnosi na prava i dozvole koje su dodijeljene ovlaštenim korisnicima kako bi pristupili određenim resursima ili izvršavali određene akcije unutar sustava.

5.3 Monitoriranje i detekcija sigurnosnih prijetnji

Prema IETF-u prijetnja je potencijal za kršenje sigurnosti, koji postoji kada postoji entitet, okolnost, sposobnost, radnja ili događaj koji bi mogli uzrokovati štetu[18]. Za prijetnju ne možemo reći da je sigurnosni problem, zato što ne postoji u implementaciji, nego to je nešto što može narušiti sigurnost. Osiguranje od prijetnji obuhvaća identificiranje prijetnja i izazova koje treba riješiti sa odgovarajućim protumjerama, tako se implementiraju različite sigurnosne metode s funkcionalnim i operativnim zahtjevima informacijskih sustava[20]. Aktivno nadziranje i upravljanje pristupom je vrlo bitno za kontrolu i otkrivanje neovlaštenih pristupa, tako administratori mogu lakše pronaći neovlaštene korisničke pristupe. Isto tako jako je korisno redovito testirati sistem za ranjivosti u organizaciji, to omogućuje veću sigurnost u slučaju napada. Korištenjem naprednih alata indentificiraju se sumnjive aktivnosti i potencijalne prijetnje koje se mogu pojaviti u oblaku, time se smanjuje mogućnost za ljudske greške i brže se reagira na prijetnje.

5.4 Sigurnosna politika i procedura

Sigurnosna politika je okvir za učinkovito i djelotvorno upravljanje sigurnošću poslovnih sustava, osiguravajući da se primijene odgovarajuće strategije, protokoli i tehnologije kako bi se zaštitili osjetljivi podaci i resursi. Ova politika usmjerava procese identificiranja, procjene i ublažavanja rizika, postavljanje jasnih smjernica za pravilno korištenje informacija te osigurava da zaposlenici, partneri i korisnici budu svjesni svojih uloga u održavanju visokih standarda sigurnosti. Kroz kontinuirano praćenje i ažuriranje, sigurnosna politika osigurava da organizacija ostane otporna na promjenjive prijetnje i izazove u digitalnom okruženju[26].

5.5 Kontinuitet poslovanja i oporavak od katastrofe

Kontinuitet poslovanja i oporavak od katastrofe uključuju pripreme, testiranje i akcije potrebne za zaštitu kritičnih poslovnih procesa od kvarova glavnog sustava i mrežnih kvarova[17]. Ti aspekti se bave nadzorom i otkrivanjem potencijalnih prijetnji i sigurnosnih incidenata u informacijskim sustavima, te imaju ključnu ulogu u zaštiti organizacija od hakerskih napada ili zlonamjernih aktivnosti. Glavni cilj oporavljanja od katastrofe je napraviti dobar plan koji implementira bitne procese u određenom vremenu koji minimaliziraju gubitak organizacije. Katastrofe mogu uključivati prirodne katastrofe kao što su potresi, poplava, a mogu biti i hakerski napadi, kvarovi i slično. Plan oporavka se sastoji od niza koraka kao što su na primjer ocjenjivanje rizika i identifikacija ključnih rizika, izrada planova oporavak, obuka osoblja, kontinuirano praćenje procesa oporavka. Ti procesi omogućuju organizaciji brži oporavak i smanjenje dodatne štete.

Katastrofa nije gotova dok se sve operacije ne vrate u normalan položaj i funkciju. Postoji vrlo velik prozor ranjivosti kada se obrada transakcije vrati s alternativne sigurnosne kopije na izvornu proizvodnju mjesto. Ako resursi računalstva u oblaku pružaju veliki dio sigurnosne kopije za organizaciju, sve moguće ranjivosti bit će ublažene. Katastrofa se može službeno proglasiti završenim tek kada se sva područja poduzeća vrate u normalu, a svi su podaci potvrđeni kao točni[17].

6. Računovodstveni sustavi u oblaku na primjeru Konta d.o.o Varaždin

Tvrtka Konto d.o.o osnovana je početkom 1993. godine, a već od 1994. godine aktivno se bavi projektiranjem, razvojem i održavanjem informacijskih sustava. Svoje poslovanje proširila je otvaranjem ureda u Varaždinu u ožujku 1996. godine. Osnovna djelatnost usmjerena je na projektiranje, razvoj i održavanje informacijskih sustava. Njihova ponuda obuhvaća cjelovita poslovna rješenja i aplikacije dizajnirane za pojedinačne poslovne procese. Ove aplikacije su međusobno povezane i modularne, omogućavajući optimalnu prilagodbu korisniku u njihovom svakodnevnom radu[31]. Kod 99% slučajeva koristi se usluga privatnog oblaka iz sigurnosnih razloga. Takav model organizaciji daje svu kontrolu nad infrastrukturom u privatnom oblaku i sama njome upravlja i administrira i to je najčešće:

1. Vlastita serverska infrastruktura (IaaS)

2. CDU – Centar dijeljenih usluga

   Centar dijeljenih usluga ili kako se još naziva „Državni oblak“ jedan je od ključnih projekata Središnjeg državnog ureda za razvoj i digitalnog društva u kojemu će se spojiti državna informacijska infrastruktura i omogućiti zajedničko korištenje informacijskih i komunikacijskih tehnologija te istih aplikativnih rješenja u svrhu racionalizacije[32].

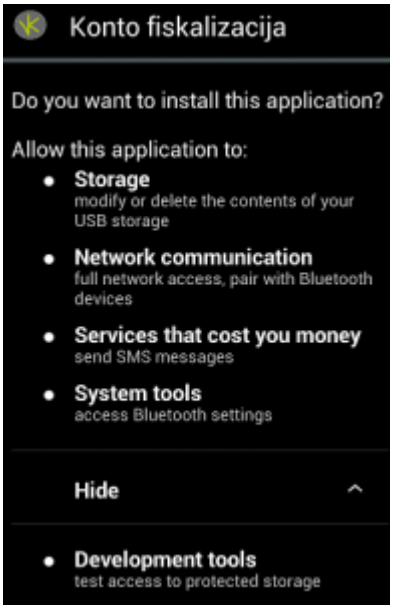
Konto d.o.o instalira, konfiguira i održava aplikacijski dio sustava i bazu podataka. Aplikacijski sustav u Kontu je visoko integriran kroz različite tehnologije desktop programa, web aplikacija, specijaliziranih mobilnih aplikacija, web servisa i slično. Oblak se uvijek nalazi unutar sigurnosne VPN mreže i nije izložen prema internetu iz sigurnosnih razloga. Svi korisnici aplikacija dobivaju različite osobne razine sigurnosti kao što su osobni VPN pristup prema oblaku od strane organizacije. Isto tako Konto d.o.o kao dodatnu sigurnost koristi aplikacijsku autentifikaciju i autorizaciju korisnika.

6.2 Primjer korištenja fiskalne mobilne kase u oblaku

Konto d.o.o nudi besplatno korištenje fiskalne mobilne kase. Aplikacija se preuzima na google play trgovini aplikacija. Cilj mobilne kase je da korisnicima olakšava rad, sve što je potrebno je putem USB-a ili bluetooth-a spojiti se na pisač.

6.2.1 Instalacija

Aplikaciju korisnik može preuzeti putem maila ili se može preuzeti sa interneta. Prilikom instaliranja aplikacije operacijski sustav pitat će ako smo sigurni da želimo preuzeti aplikaciju i pojavit će se potrebne dozvole koje aplikacija treba za rad.



Slika 13: popis dozvola koje program koristi

Izvor: konto.hr

Za normalni rad aplikacije potrebno je prihvatiti sve dozvole ili aplikacija neće korektno raditi.

6.2.2 Pokretanje i rad aplikacije

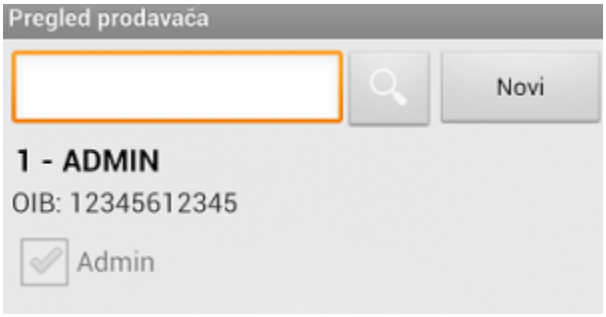
Pri ulazu u aplikaciju korisnik se mora prijaviti, no pri prvom pokretanju korisnik mora upisati ADMIN kao korisničko ime, te lozinku ostaviti praznu[34].

Nakon uspješne prijave korisnik mora podesiti program za budući rad. Korisnik se treba navigirati na evidencije, te na prodavači i onda nakon toga treba dodati novog korisnika.

Slika 14: glavni izbornik

Izvor: konto.hr

Prilikom navigiranja na prodavači pojavit će se ekran kao na sljedećoj slici.



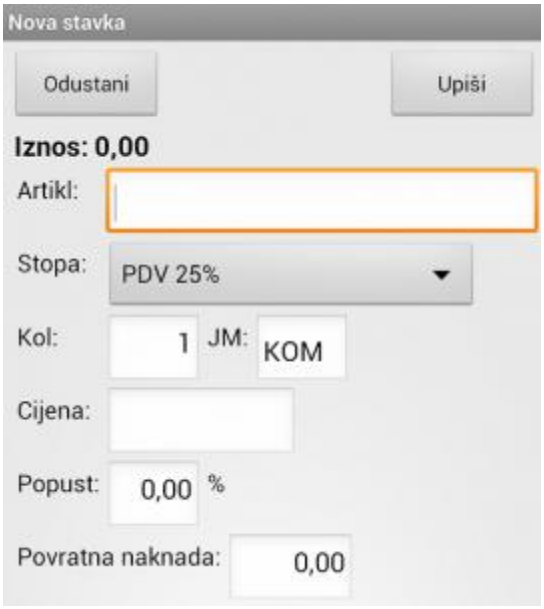
Slika 15: dodavanje novog prodavača

Izvor: konto.hr

Nakon dodavanja novog prodavača i davanja ovlasti istima, potrebno je restartirati aplikaciju za provjeru ako prodavač može pristupiti aplikaciji.

6.2.3 Dodavanje i uklanjanje stavki računa

Aplikacija ima jednostavno dodavanje stavke, kako bi dodali stavku potrebno je navigirati se u kasu, te kliknuti novi račun kao što je vidljivo na slici 16.



Slika 16: dodavanje nove stavke

Izvor: konto.hr

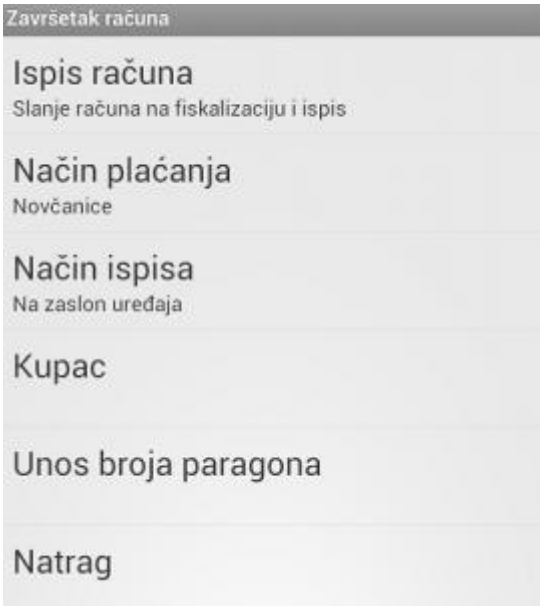
Nakon što se nova stavka(artikl) spreme u aplikaciju moguće ih je koristiti bez ponovnog upisa podataka, ako artikl ne postoji u evidenciji potrebno ga je manualno dodati.

Kako bismo izbrisali stavku potrebno je pritisnuti na crveni križić kao što je na slici 17.

Slika 17: brisanje stavke

Izvor: konto.hr

Nakon unosa svih potrebnih stavki korisnik mora kliknuti „završi račun“. Pritiskom na „završi račun“ pojavljuje se sljedeći ekran.



Slika 18: završetak računa

Izvor: konto.hr

Kao što je prikazano na slici 18, potrebno je odabrati način plaćanja i način ispisa. Nakon uspješno ispisanog računa, program se vraća na unos novog računa.

6.2.4 Backup aplikacije

Backup ili sigurnosna kopija se nalazi na glavnom izborniku pod „backup.“ U toj stavci korisnik može napraviti backup ili restore (vraćanje stare kopije). Korisniku se nudi opcija gdje želi da mu se sprema backup, nakon odabira aplikacija radi backup direktorij. Nakon izrade backup-a preporučljivo je datoteku prebaciti na cloud uslugu kao što su Google Drive, Microsoft OneDrive, Dropbox ili drugi.

Google Drive

Jedan je od najpopularnijih oblaka za pohranu podataka na cloud, nudi najviše besplatnog mjesta za skladištenje podataka. Google Drive koristi TLS i 256-bit AES enkripciju za čuvanje protoka podataka između računala i oblaka, isto tako koristi i višefaktorsku autorizaciju[35].

Microsoft OneDrive

OneDrive nudi samo 2gb slobodnog prostora u besplatnoj verziji, no ako je kupljen Microsoft 365 za poslovanje, onda se dobije premium verzija usluge koju je isto tako moguće dijeliti sa drugim osobama. OneDrive koristi SSL i TLS za čuvanje podataka i isto nudi višefaktorsku autorizaciju za očuvanje korisničkog računa, s time da samo premium verzija nudi enkripciju podataka, čime je veća mogućnost da se dogodi curenje podataka za besplatnu verziju[36].

Dropbox

Dropbox isto kao i Microsoft OneDrive nudi samo 2gb slobodnog prosotra za besplatne korisnike te nudi različite pakete za privatne i poslovne svrhe. Isto kao Google Drive i Microsoftov OneDrive, Dropbox nudi višefaktorsku autorizaciju i enkripciju i dodatno koristi sigurnosni ključ[37].

7. Zaključak

Razvoj računovodstvenog oblaka predstavlja značajan korak u evoluciji računovodstvenih sustava, pružajući organizacijama mogućnost da optimiziraju svoje poslovanje kroz fleksibilnost i pristupačnost podataka. U ovom radu detaljno sam istražio različite aspekte računovodstvenog sustava u oblaku, počevši od općih informacija o računovodstvenim informacijskim sustavima do specifičnosti modela implementacije i servisnih modela u oblaku. Proučavajući prednosti i nedostatke računovodstva u oblaku saznali smo da donosi brojne prednosti poput skalabilnosti i smanjenja troškova, no isto tako postoje i izazovi kao sigurnost oblaka. Analizirali smo različite prijetnje u oblaku uključujući gubitak podataka, prijetnje privatnosti i zlouporaba usluga. Isto tako istaknute su ključne mjere osiguranja koje organizacije mogu primijeniti kako bi smanjili te prijetnje. U segmentu sigurnosnih aspekata, istražio sam ključne elemente kao što su identifikacija i autentifikacija korisnika, upravljanje pristupom i ovlaštenjima, monitoriranje i detekcija sigurnosnih prijetnji, sigurnosna politika i procedura te kontinuitet poslovanja i oporavak od katastrofe. Svi ovi aspekti su od suštinskog značaja za održavanje integriteta, povjerljivosti i dostupnosti podataka u računovodstvenom sustavu u oblaku. Unatoč izazovima sigurnosti, računovodstvo u oblaku predstavlja ključan resurs za suvremene organizacije koje teže efikasnosti, fleksibilnosti i inovacijama. Implementacija adekvatnih sigurnosnih mjera i pridržavanje najboljih praksi u području računovodstva u oblaku ključni su elementi uspješne integracije ovog tehnološkog rješenja u poslovne procese.

Literatura:

1. Cheng Ping, he Xuefeng. Application of "Cloud Accounting" in Accounting Informatization of Small and Medium-sized Enterprises Journal of Chongqing University of Technology (Social Sciences),2011

2. Vitasović, M. (2012). ANALIZA STANJA I DOPRINOSA RAČUNOVODSTVENOGA INFORMACIJSKOG SUSTAVA I SUSTAVA UPRAVLJANJA FINANCIJAMA U SEGMENTU RAZVOJA PRORAČUNSKOG SUSTAVA LOKALNIH JEDINICA. *Ekonomska misao i praksa, 21* (2), 563-594.

Str 32

3. Tokić, M., Proklin, M. (2011): Značajke računovodstvenoga informacijskog sustava poduzetnika, Ekonomski vjesnik : Review of Contemporary Entrepreneurship, Business, and Economic Issues, Vol. XXIV No. 2, str. 294 – 300

(u tekst reference)

4. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4-5), 372-386.

5. CERT, LS&S, L. za sustave i signale: Cloud Computing, NCERT-PUBDOC-2010-03-293, 2010

6. 2018 Cloud Trends: RightScale State of the Cloud Report

7. “what are private public hybrid clouds”, Microsoft, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds

8. Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management, 34*(2), 177-184.

9.”benefits of cloud over traditional accounting” , Paychex,

https://www.paychex.com/articles/finance/benefits-of-cloud-over-traditional-accounting/

10. Khanom, Musammat Tahmina. (2017). Cloud Accounting: A Theoretical Overview. IOSR Journal of Business and Management. 19. 31-38. 10.9790/487X-1906053138.

str 34

11. Wilshusen, G. C. (2010). Information security federal guidance needed to address control issues with implementing cloud computing. GAO Reports, preceding, 1–48.

12. Sultan, N. (2011). Reaching for the “cloud”: How SMEs can manage. *International Journal of Information Management, 31*(3), 272-278.

13. “What is Cloud security”, Checkpoint, https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

14. O. Dimitriu and M. Matei, Cloud accounting: A new business model in a challenging context, Procedia Economics and Finance, 32,2015, 665-671.

15. Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53(4), 27. doi:10.1145/1721654.1721667

16. “How cloud computing will change accounting forever”, Bruce A. Phillips (2012)

17. L. Krutz, R., Dean Vines, R. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing str.384

18. Shirey, R. (2007). Internet Security Glossary,

https://datatracker.ietf.org/doc/html/rfc4949

19. Zenzerović, R (2007). Računovodstveni informacijski sustavi, 17-336

20. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.

21. “Identity Theft: Trends and Issues” (2014). Congressional Research Service

https://crsreports.congress.gov/product/pdf/R/R40599/18

22. Panker, Jon; Lewis, Mark; Fahey, Evan; Vasquez, Melvin Jafet (august 2007). "How do you pronounce IT?". *TechTarget*.

23. "Microsoft describes software plus services". InfoWorld. 26. 7. 2007.

24. Naren.J, & Sowmya, S.K. & Deepika, P.. (2014). Layers of Cloud – IaaS, PaaS and SaaS: A Survey. International Journal of Computer Science and Information Technology. Vol. 5 (3). 4477 - 4480.

25. Oluić, A.: “Kvaliteta računovodstvenih informacijskih sustava u Republici Hrvatskoj”, Zbornik Ekonomskog fakulteta u Zagrebu, Vol. 6, No. 1, 2008., prema: Romney, M. B., Steinbart, P. J., Cushing, B. E.: Accounting Information System, Addison-Wesley Publishing Company 1997., str. 543.

26. “Autentifikacija, autorizacija i bilježenje”, (2013). Fakultet organizacije i informatike u Varaždinu

27. “What is Data Protection and Privacy?”, Cloudian, https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

28. “what is data loss prevention DLP”, Microsoft,

https://www.microsoft.com/hr-hr/security/business/security-101/what-is-data-loss-prevention-dlp

29. “what is cloud security”, Microsoft,

https://www.microsoft.com/hr-hr/security/business/security-101/what-is-cloud-security

30. Mather, T. Kumaraswamy, S. Latif, S., Cloud security and privacy: an enterprise perspective on risks and compliance. O’ Reily, str. 312.

31. „ o nama“, Konto d.o.o, https://www.konto.hr/o-nama/

32. „Uspostava Centra dijeljenih usluga“, https://rdd.gov.hr/projekti-i-eu-projekti/eu-projekti/uspostava-centra-dijeljenih-usluga/1596?lang=hr

33. Autentifikacija i autorizacija korisnika na jednom mjestu
https://bib.irb.hr/datoteka/299708.06_ISS_1043.pdf

34. Konto hrvatska „https://www.konto.hr“

35. Google Drive „https://www.google.com/drive/“

36. Microsoft OneDrive „https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage“

37. Dropbox „https://www.dropbox.com/features/security“