Upravljanje sigurnošću kod implementacije programskih rješenja u računalnom oblaku

Tirić, Ivan

SVEUČILIŠTE U ZAGREBU
FAKULTET STROJARSTVA I BRODOGRADNJE

DIPLOMSKI RAD

Ivan Tirić

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET STROJARSTVA I BRODOGRADNJE

DIPLOMSKI RAD

Mentor:
Doc. dr. sc. Tomislav Stipančić

Student:
Ivan Tirić

Zagreb, 2022.

Izjavljujem da sam ovaj rad izradio samostalno koristeći znanja stečena tijekom studija i navedenu literaturu.

Zahvaljujem mentoru doc. dr. sc. Tomislavu Stipančiću na svoj pruženoj pomoći i savjetovanju prilikom izrade ovoga rada.

Zahvaljujem prijateljima, kolegama, a najviše roditeljima i bratu na pruženoj podršci tijekom studiranja.

Ivan Tirić

SVEUČILIŠTE U ZAGREBU
FAKULTET STROJARSTVA I BRODOGRADNJE
Središnje povjerenstvo za završne i diplomske ispite
Povjerenstvo za diplomske radove studija strojarstva za smjerove:
proizvodno inženjerstvo, računalno inženjerstvo, industrijsko inženjerstvo i menadžment, inženjerstvo materijala te mehatronika i robotika

Sveučilište u Zagrebu Fakultet strojarstva i brodogradnje	
Datum:	Prilog:
Klasa: 602-14/22-6/1	
Ur. broj: 15-1703-22-	

DIPLOMSKI ZADATAK

Student: **IVAN TIRIĆ** Mat. br.: 0108062554

Naslov rada na hrvatskom jeziku: **Upravljanje sigurnošću kod implementacije programskih rješenja u računalnom oblaku**

Naslov rada na engleskom jeziku: **Security management in the implementation of software solutions in the cloud**

Opis zadatka:

U današnje vrijeme gotovo da i ne postoji poduzeće koje ne koristi neko od programskih rješenja u računalnom oblaku kao što su Twitter, Facebook, Office 365 i Salesforce. Također, prilikom poslovanja kompanije se često oslanjaju na mnoštvo drugih programskih rješenja dostupnih putem računalstva u oblaku. Računalna sigurnost stoga predstavlja važnu stavku i prioritet za širu primjenu te tehnologije. Mnoge organizacije žele unaprijediti ili proširiti svoje poslovanje korištenjem aplikacija u oblaku, ali se istovremeno s razvojem tehnologije pojavljuju novi sigurnosni zahtjevi vezani uz transparentnost korištenja, zaštitu podataka, upravljanje identitetima te zaštitu od napada s mreže.

U radu je potrebno napraviti sljedeće:
1. Objasniti ključne aspekte i referentnu arhitekturu računalstva u oblaku.
2. Opisati osnovne sigurnosne zahtjeve korištenja aplikacija u oblaku te model podijeljene odgovornosti.
3. Istražiti sigurnosna rješenja s posebnim naglaskom na rješenja tipa "Cloud Access Security Broker (CASB)".
4. Analizirati dostupna CASB rješenja i detaljnije objasniti jedno od njih.
5. Na jednom realnom primjeru prikazati primjenu odabranog rješenja.

U radu je potrebno navesti korištenu literaturu i eventualno dobivenu pomoć.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
29. rujna 2022.	1. prosinca 2022.	12. prosinca do 16. prosinca 2022.

Zadatak zadao: doc. dr. sc. Tomislav Stipančić

Predsjednica Povjerenstva: prof. dr. sc. Biserka Runje

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

POPIS AKRONIMA I KRATICA

APAC azijsko-pacifička regija (*eng. Asia-Pacific Region*)

API programsko sučelje aplikacije (*eng. Application Programming Interface*)

CASB brokeri za pristup i sigurnost u računalnom oblaku (*eng. Cloud Access and Security Brokers)*

CDN mreža za isporuku sadržaja (*eng. content delivery network*)

CSA (*eng. Cloud Security Alliance*) (organizacija)

DLP sprječavanje gubitka podataka (eng. Data Loss Prevention)

DNS distribuirani hijerarhijski sastav (eng. Domain Name System)

DRP mogućnosti planiranja oporavka od katastrofe (*eng. Disaster Recovery Planning*)

EMEA regija Europa, Bliski Istok, Afrika (*eng. Europe, Middle East, and Africa Region*)

ERP planiranje resursa poduzeća (eng. *Enterprise Resource Planning)*

HTTP/2 (*eng. Hypertext Transfer Protocol/2)* (protokol)

IaaS računalna infrastruktura kao usluga (*eng. Infrastructure as a Service*)

IDS sustav za otkrivanje upada (*eng. Intrusion Detection Systems)*

IPS sustav za sprječavanje upada (*eng. Intrusion Prevention Systems*)

IR plan odgovora na incidente (*eng. Incident Response*)

IRM upravljanje pravima na informacije (*eng. Information rights management*)

MFA multifaktorska autentifikacija (*eng. Multi-factor Authentication*)

NAC kontrola pristupa mreži (eng. network access control)

NIST Nacionalni institut za standarde i tehnologiju (*eng. National Institute of Standards and Technology*)

PaaS platforma kao usluga (*eng. Platform as a Service)*

PII podaci koji su povezani sa identitetom osobe (*eng. personally identifiable information*)

SaaS softver kao usluga (*eng. Software as a Service)*

SAML 2.0 *(eng. Security Assertion Markup Language 2.0)* (standard)

SCIM *(eng. System for Cross-domain Identity Management)* (standard)

SDK pribor za razvijanje softvera (*eng. Software Development Kit*)

SIEM upravljanjem sigurnosnim informacijama i događajima (eng. Security Information and Event Management)

SSE usluge sigurnosti na (računalnim) rubovima (*eng. Security Service Edge*)

SSL sigurnosni sloj priključka *(eng. Secure Sockets Layer)*

SSO jedinstvena (jednostruka) prijava (*eng. Single Sign On*)

TDE transparentna enkripcija baze podataka (*eng. Transparent Database Encryption*)

URL ujednačeni ili usklađeni lokator sadržaja (resursa) (eng. Uniform Resource Locators)

***XACML** (eng. eXtensible Access Control Markup Language)* (standard)

XML jezik za označavanje podataka (eng. EXtensible Markup Language)

SAŽETAK

Korištenje računalstva u oblaku je u značajnom porastu, sve više organizacija se odlučuje na korištenje te tehnologije. S tim korištenjem dolaze i pitanja o sigurnosti vezane na računalstvo u oblaku. Sigurnost u računalstvu u oblaku je drugačija od tradicionalne IT sigurnosti, model podijeljene odgovornosti to prikazuje jer su oba dionika, i korisnik usluga i pružatelj usluga, odgovorni za sigurnost. U prvom dijelu ovog rada, opisano je računalstvo u oblaku, NIST referentna arhitektura računalstva u oblaku, sigurnosni zahtjevi korištenja aplikacija u računalnom oblaku te Cloud Access Security Broker - CASB. U drugom dijelu rada prikazan je realni primjer primjene sigurnosnih tehnologija u računalstvu u oblaku.

Ključne riječi: računalstvo u oblaku, sigurnost, SSO, CASB.

SUMMARY

The use of cloud services is on the rise, more and more enterprises are deciding to use this technology. With the use of cloud services come questions about cloud security. Security in the cloud is different from traditional IT security, the shared responsibility model depicts this because the cloud actors together - cloud consumer and cloud provider – are responsible for cloud security. The first part of this paper describes cloud computing, the NIST cloud computing reference architecture, security requirements for the use of cloud applications and Cloud Access Security Brokers (CASBs). In the second part of this paper is a presentation of the application of a cloud security solution.

Key words: cloud computing, security, SSO, CASB

1. UVOD

Sve više organizacija se odlučuje za rješenja u računalnom oblaku. Veličina globalnog tržišta računalstva u oblaku je 369 milijardi američkih dolara (u 2021. godini). Projekcije pokazuju da bi to tržište trebalo imati prosječnu kumulativnu godišnju stopu rasta od skoro 16% i to od 2022. do 2030. godine [1]. Zbog toga je razumijevanje računalstva u oblaku dobilo na značenju. Za to razumijevanje veliku ulogu imaju razne publikacije kao što su publikacije od NIST-a gdje su, među ostalim, definirani osnovni pojmovi računalstva u oblaku (kao što su temeljne karakteristike računalstva u oblaku, modeli usluga te modeli implementacije), akteri u okruženju računalstva u oblaku, opseg kontrole tih aktera nad resursima računalstva u oblaku ili referentne arhitekture koje se mogu uzeti kao temelj za izradu vlastitih rješenja računalstva u oblaku. Značajan dio tržišta računalstva u oblaku su SaaS usluge, gdje pružatelj usluge nudi aplikaciju na korištenje korisniku usluge. U tom modelu pružatelj usluga je zadužen za većinu zadaća oko administracije i sigurnosti aplikacije, no korisnik usluga ne može pretpostavljati da nema nikakve zadaće oko sigurnosti aplikacije. Što se više koristi računalstvo u oblaku to fokus sve više pada na sigurnost. Zbog toga je razvijen model podijeljene odgovornosti za sigurnost u računalnom oblaku. Svaki model usluga računalstva u oblaku ima drugačiju podjelu odgovornosti između korisnika usluga računalstva u oblaku i pružatelja usluga računalstva u oblaku. Korisnici IaaS usluga računalstva u oblaku imaju najveću odgovornost za sigurnost (u odnosu na druge korisnike usluga računalstva u oblaku) od sva tri modela usluga računalstva u oblaku dok korisnici SaaS usluga u tom modelu su odgovorni za ovlaštenja i prava pristupa aplikaciji (što bi bio najuži spektar odgovornosti za sigurnost što korisnik može imati).

Povećanjem tržišta računalstva u oblaku, povećava se i broj aplikacija u računalnom oblaku koje organizacije koriste. Kako bi se zadržao zadovoljavajući pregled nad tim, sve više rastućim, aplikacijskim krajolikom te kako bi se upravljalo identitetima i pristupom tim aplikacijama koriste se CASB i SSO rješenja. Zaposlenici/korisnici u organizacijama čak koriste i aplikacije koje nisu odobrene od strane organizacije. Za vidljivost tih aplikacija te dosljedno isključivanje iz uporabe se također koriste CASB rješenja. Odluke i politike o stupnju osjetljivosti podataka i dopuštenjima za dijeljene podataka te provođenje tih odluka i politika je isto područje za CASB. Od kritične važnosti za poslovanje organizacije je zaštita aplikacija u računalnom oblaku kao što su ERP sustavi (npr. SAP) ili CRM sustavi (npr. Salesforce) te podataka koje te aplikacije sadrže.

2. NIST DEFINICIJA RAČUNALSTVA U OBLAKU

NIST je akronim za *eng. National Institute of Standards and Technology* (pri *eng. U.S. Department of Commerce*). Publikacije tog instituta predstavljaju temeljne dokumente arhitekture i sigurnosti računalstva u oblaku unutar Sjedinjenih Američkih Država, a u ostatku svijeta se primjenjuju kao najbolje prakse, standardi za izgradnju i uspostavu sigurnosti u računalstvu u oblaku. Najvažniji NIST dokumenti vezani za računalstvo u oblaku su:

- NIST SP 800-145 The NIST Definition of Cloud Computing
- NIST SP 500-292 NIST Cloud Computing Reference Architecture

Računalstvo u oblaku je model koji omogućava univerzalan, jednostavan mrežni pristup na zahtjev dijeljenom skupu konfigurabilnih računalnih resursa (npr. mreži, poslužiteljima, pohrani podataka, aplikacijama i uslugama) koje je moguće gotovo u realnom vremenu pribaviti i pustiti u uporabu uz minimalan upravljački napor ili interakciju s pružateljem usluga računalstva u oblaku. Referentni model računalstva u oblaku sačinjava: pet temeljnih karakteristika računalstva u oblaku, tri modela pružanja usluga i četiri modela implementacije [2]. Temeljne karakteristike računalstva u oblaku su [2]:

- Samouslуživanje na zahtjev *eng. on-demand self-service*. Korisnik usluga može jednostrano aktivirati računalne resurse, kao što je vrijeme korištenja poslužitelja i mrežna pohrana podataka, sukladno vlastitoj potrebi i potpuno automatski bez ljudske interakcije s pružateljem usluge računalstva u oblaku.
- Vrlo visoki kapacitet pristupa mreži *eng. broad network access*. Računalni resursi su dostupni putem mreže, a pristup je omogućen putem standardnih mehanizama koji promiču korištenje heterogenih laganih ili teških klijentskih platformi (npr. mobilnih telefona, tableta, prijenosnih računala i radnih stanica).
- Objedinjavanje resursa *eng. resource pooling*. Računalni resursi pružatelja usluga računalstva u oblaku su objedinjeni kako bi istovremeno mogli opsluživati više korisnika usluga računalstva u oblaku koristeći model dijeljenja resursa, pri kojem se različiti fizički i virtualni resursi dinamički dodjeljuju i preraspodjeljuju ovisno o potražnji. Na taj način se stvara osjećaj lokacijske neovisnosti, jer korisnik usluga računalstva u oblaku uglavnom nema kontrolu niti znanje o točnoj lokaciji ustupljenih resursa, ali zato korisnik usluga računalstva u oblaku ima mogućnost odrediti lokaciju na višoj razini apstrakcije (npr. nacija, savezna država/pokrajina ili podatkovni centar). Primjeri dijeljenih resursa uključuju pohranu (računalna memorija), obradu (procesiranje), radnu memoriju i propusnost mreže.
- Visoka (praktično trenutna) elastičnost *eng. rapid elasticity*. Računalni resursi se mogu elastično dodjeljivati i razduživati, a u nekim slučajevima potpuno automatski, tj. brza ekspanzija ili smanjenje proporcionalno potražnji. Korisnicima usluga računalstva u oblaku se dostupni računalni resursi često čine neograničenima uz osjećaj da se mogu koristiti u bilo kojoj količini i aktivirati u bilo kojem trenutku.

- Mjerena (obračunata) usluga *eng. measured service*. Sustavi računalstva u oblaku automatski kontroliraju i optimiraju korištenje resursa oslanjajući se na mogućnost mjerenja na razini apstrakcije koja odgovara vrsti usluge (npr. količina pohrane podataka, obim obrade podataka, propusnost mreže ili aktivni korisnički računi). Mogućnost nadzora, kontrole i izrade detaljnih i izvještaja o korištenju računalnih resursa pruža veliku transparentnost kako za pružatelja usluga računalstva u oblaku tako i za korisnika usluga računalstva u oblaku.

Modeli usluga [2]:

- Softver kao usluga *eng. Software as a Service* (SaaS). Računalni resursi koji se pružaju korisniku usluga računalstva u oblaku omogućavaju korištenje aplikacija koje se izvode na infrastrukturi računalstva u oblaku u vlasništvu pružatelja usluga. Aplikacijama je moguće pristupiti s različitih klijentskih uređaja, na primjer putem korisničkog sučelja na laganom klijentu (kao što je web preglednik) ili aplikativnog programskog sučelja (*eng. Application Programming Interface* - API). Korisnik usluga računalstva u oblaku ne upravlja temeljnom infrastrukturom računalstva u oblaka kao što su mrežni resursi, poslužitelji, operativni sustavi, sustavi za pohranu podataka ili uz moguću iznimku ograničenih postavki konfiguracije aplikacija s kojima specifično upravlja korisnik.
- Platforma kao usluga *eng. Platform as a Service (PaaS)*. Računalni resursi koji se pružaju korisniku usluga računalstva u oblaku predstavljaju implementaciju aplikacija na infrastrukturu pružatelja usluga računalstva u oblaku. Aplikacije su kreirane od strane korisnika usluga računalstva u oblaku ili od trećih strana, ali pomoću programskih jezika, razvojnih okvira, usluga i alata koje podržava pružatelj usluga računalstva u oblaku. Korisnik usluga ne upravlja niti nadzire temeljnu infrastrukturu u oblaku uključujući mrežne resurse, poslužitelje, operativne sustave ili sustave za pohranu podataka, ali ima kontrolu nad postavljenim aplikacijama i eventualno konfiguracijskim postavkama platforme za upogonjenje aplikacija.
- Računalna infrastruktura kao usluga eng. Infrastructure as a Service (IaaS). Računalni resursi koji se pružaju korisniku usluge računalstva u oblaku predstavljaju obradu (procesiranje) podataka, pohranu podataka, mrežne resurse i druge temeljne računalne resurse na kojima korisnik može implementirati i pokrenuti proizvoljan softver, koji može uključivati operativne sustave i aplikacije. Korisnik usluga računalstva u oblaku ne upravlja temeljnom infrastrukturom računalnog oblaka, ali ima kontrolu nad operativnim sustavima, pohranom i postavljenim aplikacijama te eventualno ograničenu kontrolu odabranih mrežnih komponenti (npr. vatrozid računala domaćina)

Modeli implementacije *eng. Deployment model* [2]:

- Privatni model računalstva u oblaku *eng. Private cloud*. Infrastruktura računalstva u oblaku predviđena je za isključivu upotrebu jedne organizacije koja se sastoji od više potrošača (npr. poslovnih jedinica). Može biti u vlasništvu, upravljana te pogonjena od strane organizacije, treće strane ili kombinacije prethodno navedenih aktera. Privatni oblak može biti smješten na lokaciji u vlasništvu korisnika ili izvan njega.
- Zajednički model računalstva u oblaku *eng. Community cloud*. Infrastruktura računalstva u oblaku predviđena je za ekskluzivnu upotrebu od strane određene

zajednice korisnika iz organizacija koje imaju zajedničke interese (npr. misija, sigurnosni zahtjevi, politika i razmatranja sukladnosti *eng. compliance*). Može biti u vlasništvu, upravljana te pogonjena od jednog ili više članova (organizacija) zajednice, treće strane ili kombinacije prethodno navedenih aktera. Može biti smještena u prostorima nekog od aktera (ili svih aktera) ili izvan njega.

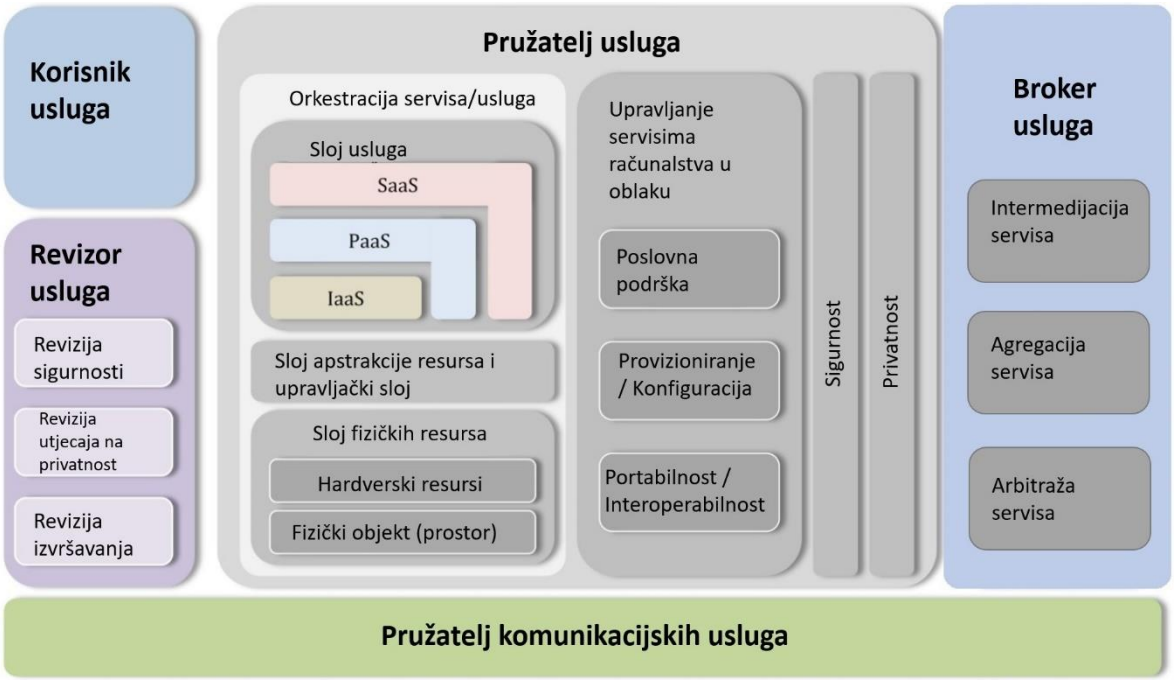
- Javni model računalstva u oblaku *eng. Public cloud*. Infrastruktura računalstva u oblaku predviđena je za otvorenu upotrebu od strane šire javnosti. Može biti u vlasništvu, upravljana te pogonjena od strane trgovačkog društva, akademske organizacije, javne/državne organizacije ili kombinacije prethodno navedenih aktera. Javni računalni oblak je smješten u prostorima pružatelju usluga računalstva u oblaku.
- Hibridni model računalstva u oblaku *eng. Hybrid cloud*. Infrastruktura računalnog oblaka sastavljena je od dviju ili više različitih modela računalstva u oblaku (privatni, zajednički, javni) koji ostaju samostalne cjeline, ali su međusobno povezane standardiziranom ili vlastitom tehnologijom koja omogućuje prenosivost podataka i aplikacija (npr. tehnika rasprsnuća oblaka *eng. cloud bursting* koja se koristi za dinamičko uravnoteživanje opterećenja između računalnih oblaka).

3. NIST REFERENTNA ARHITEKTURA RAČUNALSTVA U OBLAKU

NIST referentna arhitektura računalstva u oblaku predstavljena u dokumentu [3] NIST SP 500-292 i predstavlja logičko proširenje NIST definicije računalstva u oblaku. To je generički konceptualni model visoke razine apstrakcije koji služi kao vrlo učinkovit alat za analizu zahtjeva, izradu arhitekture i planiranje operacija računalstva u oblaku. Model nije vezan ni za jednog specifičnog dobavljača, uslugu ili referentnu implementaciju, niti definira preskriptivna rješenja koja sprječavaju inovacije. Model definira skup aktera, aktivnosti i funkcija koje se mogu koristiti u procesu razvoja arhitektura računalstva u oblaku i u vezi je sa popratnom taksonomijom računalstva u oblaku. Referentna arhitektura sadrži skup pogleda i opisa koji su osnova za raspravu o karakteristikama, upotrebi i standardima za računalstvo u oblaku. Ovaj model temeljen na akterima (ulogama) namijenjen je ispunjavanju očekivanja sudionika omogućavajući im da razumiju cjelokupni pogled na uloge i odgovornosti kako bi procijenili i raspodijelili rizik. NIST referentna arhitektura računalstva u oblaku usredotočuje se na zahtjeve "što" usluge u oblaku pružaju, a ne "kako" dizajnirati rješenje i implementaciju. Referentna arhitektura ima za cilj olakšati razumijevanje operativnih zamršenosti/složenosti u računalstvu u oblaku. Ona ne predstavlja arhitekturu određenog sustava računalstva u oblaku, umjesto toga je alat za opisivanje, analizu i razvoj arhitekture za specifičan sustav koristeći zajednički referentni okvir [3].

3.1. Prikaz referentne arhitekture

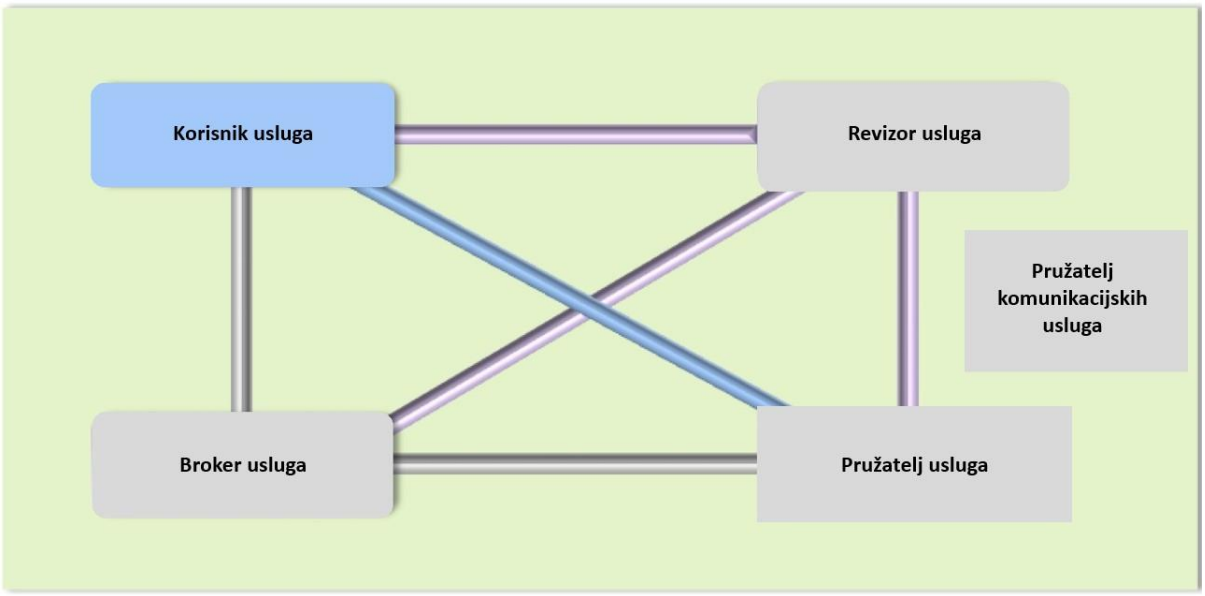
Slika 1. prikazuje NIST referentnu arhitekturu računalstva u oblaku. Ta arhitektura identificira glavne aktere, te njihove aktivnosti i funkcije u računlrstvu u oblaku. Dijagram prikazuje generičku arhitekturu visoke razine apstrakcije i namijenjen je olakšavanju razumijevanja zahtjeva, upotrebe, karakteristika i standarda računalstva u oblaku. Kao što je prikazano na slici 1., NIST referentna arhitektura računalstva u oblaku definira pet glavnih aktera: korisnik usluga računalstva u oblaku, pružatelj usluga računalstva u oblaku, pružatelj komunikacijskih usluga za računalstvo u oblaku, revizor usluga računalstva u oblaku i broker usluga računalstva u oblaku. Svaki akter je entitet (osoba ili organizacija) koji sudjeluje u transakciji ili procesu i/ili obavlja zadatke u računalstvu u oblaku [3]. Na slici 2. su prikazane interakcije između aktera u računalstvu u oblaku.



Slika 1. Prikaz referentne arhitekture [3]

Definicije glavnih aktera [3]:

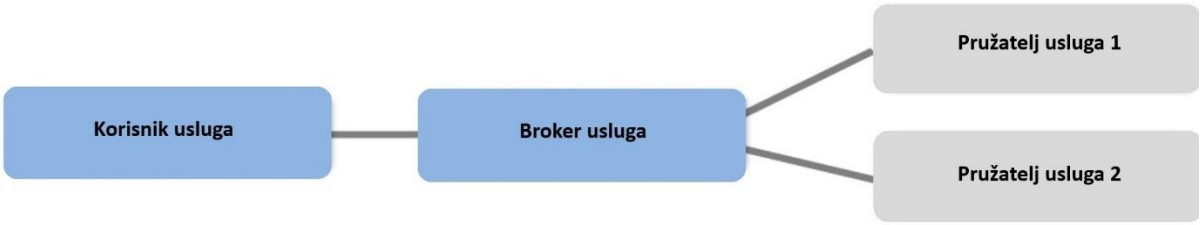
- Korisnik usluga računalstva u oblaku *eng. Cloud Consumer* (u daljnjem tekstu će se koristiti izraz korisnik usluga) je osoba ili organizacija koja održava poslovni odnos s pružateljima usluga računalstva u oblaku i koristi ih.
- Pružatelj usluga računalstva u oblaku *eng. Cloud Provider* (u daljnjem tekstu će se koristiti izraz pružatelj usluga) je osoba, organizacija ili entitet odgovoran za stavljanje usluge na raspolaganje zainteresiranim stranama.
- Revizor usluga računalstva u oblaku *eng. Cloud Auditor* (u daljnjem tekstu će se koristiti izraz revizor usluga) je strana koja može provesti neovisnu procjenu usluga računalstva u oblaku, rada informacijskog sustava, performansi i sigurnosti implementacije računalstva u oblaku.
- Broker usluga računalstva u oblaku *eng.* Cloud Broker (u daljnjem tekstu će se koristiti izraz broker usluga) je subjekt koji upravlja korištenjem, izvedbom i isporukom usluga računalstva u oblaku te posreduje u odnosima između pružatelja usluga računalstva u oblaku i korisnika usluga računalstva u oblaka.
- Pružatelj komunikacijskih usluga za računalstvo u oblaku *eng.* Cloud Carrier (u daljnjem tekstu će se koristiti izraz pružatelj komunikacijskih usluga) je posrednik koji pruža povezanost i prijenos usluga računalstva u oblaku od pružatelja usluga oblaka do korisnika usluga računalstva u oblaku.



Slika 2. Interakcije između aktera [3]

U referentnoj arhitekturi se navode i tri scenarija upotrebe računalstva u oblaku [3]:

- Scenarij 1: Korisnik usluga može zatražiti usluge od brokera usluga umjesto da izravno kontaktira pružatelja usluga. Broker usluga može stvoriti novu uslugu kombiniranjem više usluga ili poboljšanjem postojeće usluge. U ovom primjeru, stvarni pružatelji usluga su nevidljivi korisniku usluga, a korisnik usluga izravno komunicira s brokerom usluga. Ovaj scenarij je prikazan na slici 3.



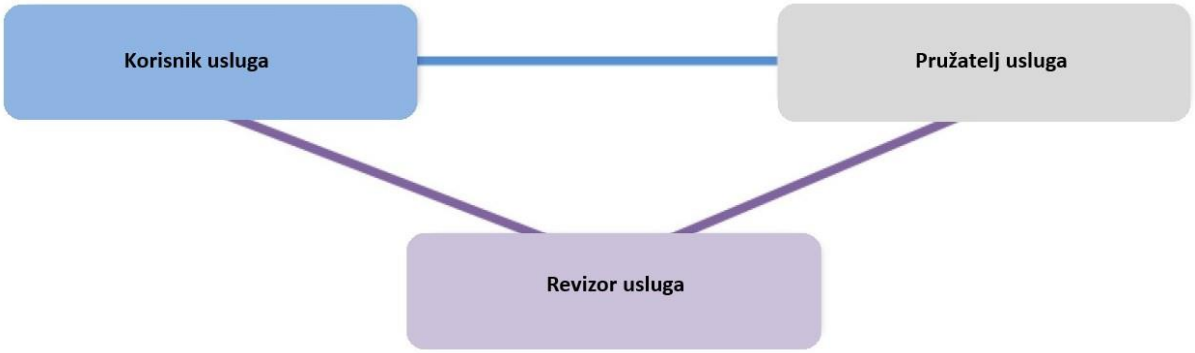
Slika 3. Scenarij za brokere usluga [3]

- Scenarij 2: Pružatelji komunikacijskih usluga omogućavaju povezivost i prijenos usluga računalstva u oblaku od pružatelja usluga do korisnika usluga. Kao što je prikazano na slici 4. pružatelj usluga i dogovara dva jedinstvena ugovora o razini usluge (*eng. Service Level Agreements* - SLA), jedan s pružateljem komunikacijskih usluga (npr. SLA2) i jedan s korisnikom usluga (npr. SLA1). Pružatelj usluga dogovara ugovore o razini usluge (SLA) s pružateljem komunikacijskih usluga i može zahtijevati namjenske i kriptirane veze kako bi osigurao da se usluge u oblaku koriste na

odgovarajućoj razini u skladu s ugovornim obvezama s korisnicima usluga. U tom slučaju, pružatelj usluga može navesti svoje zahtjeve o računalnim resursima i kapacitetima, fleksibilnosti i funkcionalnosti u SLA2 kako bi pružio uslugu sukladno zahtjevima u SLA1.

Slika 4. Scenarij za pružatelje komunikacijskih usluga [3]

- Scenarij 3: Za uslugu u oblaku, revizor usluga provodi neovisne procjene rada i sigurnosti implementacije. Revizija može uključivati interakcije s korisnikom usluga i pružateljem usluga. Slika 5. prikazuje scenarij 3.



Slika 5. Scenarij za revizore usluga [3]

3.2. Akteri u okruženju računalstva u oblaku

Korisnik usluga glavni je dionik usluge računalstva u oblaku. Korisnik usluga predstavlja osobu ili organizaciju koja održava i koristi poslovni odnos s pružateljem usluga. Korisnik usluga pregledava katalog usluga od pružatelja usluga, naručuje odgovarajuću uslugu, sklapa potrebne ugovore s pružateljem usluga za odabranu uslugu i koristi uslugu. Korisnik usluga može dobiti fakture za korištenu uslugu i obvezan je u skladu s tim organizirati plaćanja [3]. Korisnici usluga trebaju ugovore o razini usluge kako bi odredili zahtjeve tehničke izvedbe koje ispunjava pružatelj usluga. Ugovori o razini usluge mogu pokrivati uvjete koji se odnose na kvalitetu usluge, sigurnost, te mjere za greške tijekom rada. Pružatelj usluga također može navesti u ugovoru o razini usluge skup mogućnosti koja nisu izričito dostupne korisnicima usluga, tj. ograničenja i obveze koje korisnici usluga moraju prihvatiti. Korisnici usluga mogu

slobodno odabrati pružatelja usluga s nižom cijenom i povoljnijim uvjetima. U pravilu se ne može pregovarati o cjenovnoj politici pružatelja usluga i o ugovoru o razini usluge, osim u slučaju kada korisnik usluga očekuje povećanu upotrebu računalnih resursa i u tom slučaju bi mogao pregovarati za bolje uvjete [4].

Pružatelj usluge je osoba ili organizacija tj. to je subjekt odgovoran za stavljanje usluge na raspolaganje zainteresiranim stranama. Aktivnosti pružatelja usluga računalstva u oblaku mogu se podijeliti u pet glavnih područja: implementacija usluga, orkestracija usluga, upravljanje uslugama računalnog oblaka, sigurnost i privatnost. Pružatelj usluga stječe i upravlja računalnom infrastrukturom potrebnom za pružanje usluga, pokreće softver u računalnom oblaku koji omogućava te usluge i dogovara isporuku usluga korisnicima usluga putem mrežnog pristupa. Za model SaaS pružatelj usluga implementira, konfigurira, održava i ažurira rad softverskih aplikacija na infrastrukturi u oblaku tako da se korisnicima usluga pružaju usluge na očekivanim razinama. Pružatelj SaaS usluge preuzima većinu odgovornosti upravljanja aplikacijama i infrastrukturom, dok korisnici SaaS usluga imaju ograničenu administrativnu kontrolu nad aplikacijama [3].

Pružatelj PaaS usluge upravlja računalnom infrastrukturom za platformu i pokreće softver u oblaku koji pruža komponente platforme, kao što je okruženje za pokretanje softvera (*eng. runtime software execution stack*), baze podataka i druge međuprogramske komponente (*eng.* middleware). Pružatelj PaaS usluge obično podržava proces razvoja, implementacije za korisnika PaaS usluga i to tako što pruža alate kao što su integrirana razvojna okruženja *eng. integrated development environments*, programske pakete za razvoj softvera *eng. software development kits* te alate za implementaciju i upravljanje. Korisnik PaaS usluge ima kontrolu nad aplikacijama i djelomično na nekim postavkama hosting okruženja, ali nema (ili ima ograničen) pristup infrastrukturi koja je u osnovi platforme kao što su mreža, poslužitelji, operativni sustavi ili pohrana [3].

Za model IaaS, pružatelj usluge pribavlja fizičke računalne resurse koji kasnije postaju dio osnovne usluge, uključujući poslužitelje, mrežne komponente, sustave za pohranu podataka i hosting infrastrukturu. Pružatelj usluga pokreće softver u računalnom oblaku koji je neophodan kako bi računalni resursi bili dostupni korisniku IaaS usluga putem skupa servisnih sučelja i apstrakcije računalnih resursa, kao što su virtualni strojevi i virtualna mrežna sučelja. Korisnik IaaS usluga koristi računalne resurse, kao što je virtualno računalo, za svoje temeljne računalne potrebe. U usporedbi s korisnicima SaaS i PaaS usluga, korisnik IaaS usluga ima pristup

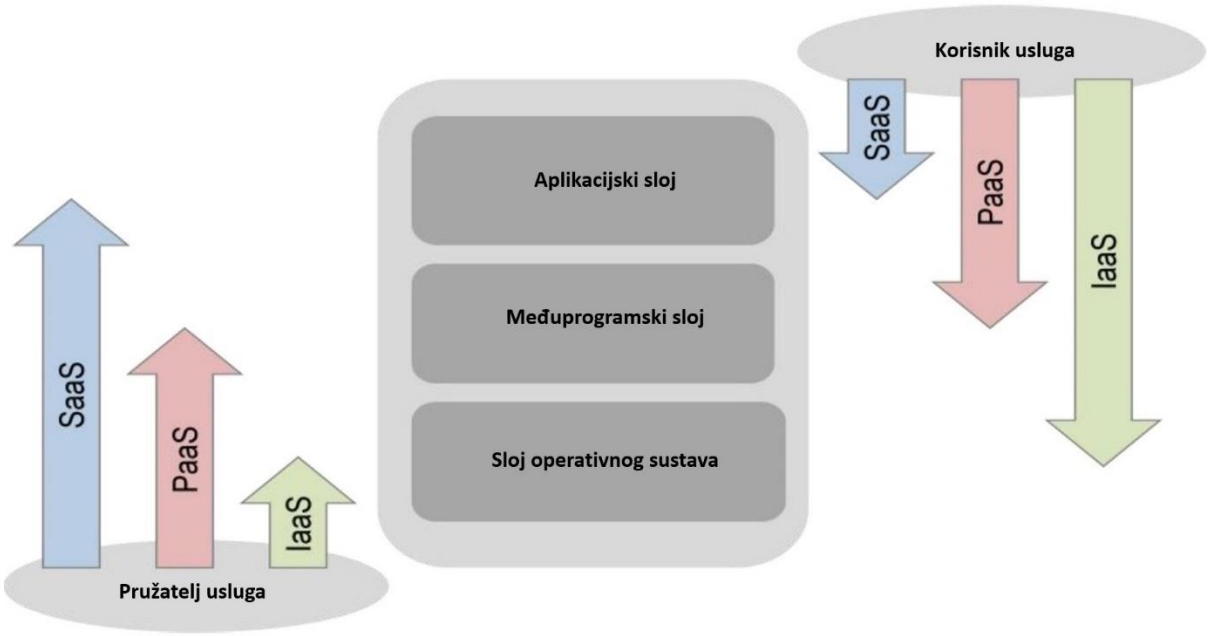
fundamentalnijim oblicima računalnih resursa i stoga ima veću kontrolu nad komponentama u aplikacijskom stogu (*eng. stack*), uključujući operacijski sustav i mrežu. S druge strane, pružatelj IaaS usluge ima kontrolu nad fizičkim hardverom i softverom u računalnom oblaku koji omogućuje pružanje ovih infrastrukturnih usluga, na primjer, fizičkih poslužitelja, mrežne opreme, uređaja za pohranu podataka, operacijskog sustava računala domaćina i hipervizora za virtualizaciju [3].

Revizor oblaka je akter koji može obaviti neovisno ispitivanje upravljanja uslugama računalnog oblaka s namjerom vrednovanja i izrade odgovarajućih izvještaja o tome. Revizije se provode kako bi se provjerila usklađenost sa standardima kroz pregled objektivnih dokaza. Revizor oblaka može procijeniti usluge pružatelja usluga u smislu sigurnosnih mjera, utjecaja na privatnost, performansi itd. [3].

Korisnik usluga može zatražiti usluge računalstva u oblaku direktno od pružatelja usluga ali i od brokera usluga. Broker usluga je akter koji upravlja upotrebom, izvedbom i isporukom usluga računalstva u oblaku te pregovara o odnosima između pružatelja usluga i korisnika usluga. Aktivnosti brokera usluga se mogu podijeliti u 3 kategorije: posredovanje u vezi s uslugama, agregacija usluga, arbitraža usluga [3].

Pružatelj komunikacijskih usluga djeluje kao posrednik koji osigurava povezanost i prijenos usluga računalnog oblaka između korisnika usluga i pružatelja usluga. Oni omogućuju pristup korisnicima usluga putem mrežnih, telekomunikacijskih i drugih pristupnih uređaja. Distribuciju usluga u računalnom oblaku obično pružaju mrežni i telekomunikacijski operateri [3].

Kontrola nad resursima računalstva u oblaku je podijeljena između korisnika usluga i pružatelja usluga. Opseg kontrole aktera nad resursima ovisi o modelu usluga (Saas, PaaS, IaaS). Na slici 5. je prikazano kako se opseg kontrole korisnika usluga i pružatelja usluga mijenja u ovisnosti o odabranom modelu usluga. S različitim opsegom kontrole su i različite odgovornosti pri upravljanju aplikacijama u računalnom oblaku [3].

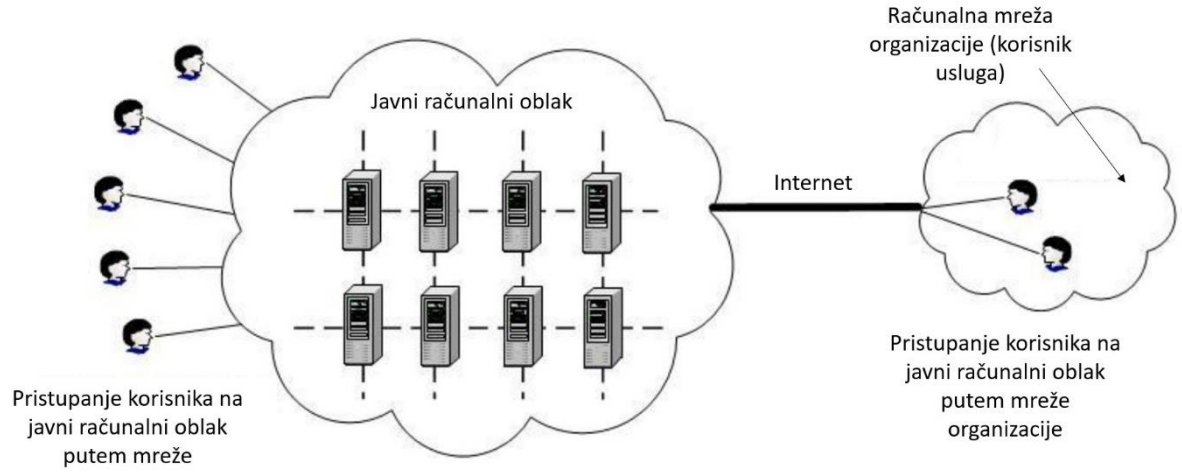


Slika 6. Opseg kontrole aktera nad resursima računalnog oblaka [3]

3.3. Arhitekturne komponente referentne arhitekture računalstva u oblaku

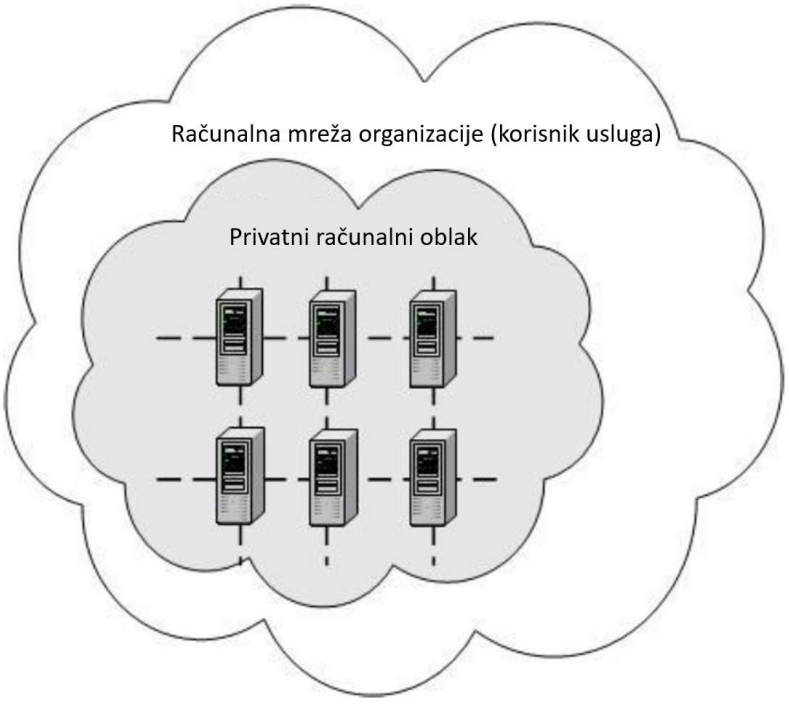
Kao što je navedeno u NIST-ovoj definiciji računalstva u oblaku, infrastruktura u oblaku može biti implementirana kao jedan od slijedećih modela: javni model računalstva u oblaku, privatni model računalstva u oblaku, zajednički model računalstva u oblaku te hibridni model računalstva u oblaku. Razlike se temelje na tome koliko su računalni resursi ekskluzivni za korisnika usluga [3].

Javni model računalstva u oblaku je onaj u kojem su infrastruktura oblaka i računalni resursi dostupni široj javnosti putem javne mreže. Javni računalni oblak u vlasništvu je organizacije koja prodaje usluge u računalnom oblaku i služi raznolikoj skupini klijenata. Slika 8. predstavlja jednostavan prikaz javnog računalnog oblaka i njegovih korisnika [3].

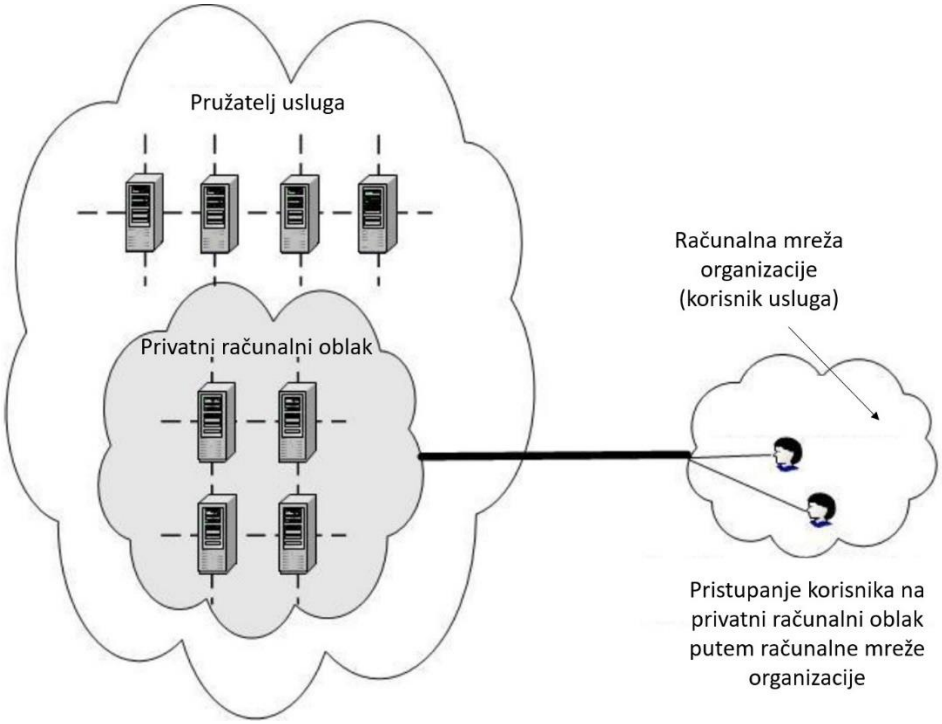


Slika 7. Javni računalni oblak [3]

Kod privatnog modela računalstva u oblaku jedna organizacija (korisnik usluga) ima ekskluzivan pristup infrastrukturi i računalnim resursima. Njima može upravljati ili ta organizacija ili treća strana, a može se nalaziti u prostorima organizacije (tj. interni privatni računalni oblak) ili biti prepušteni tvrtki koja pruža usluge hostinga (tj. eksterni privatni računalni oblak). Slika 8. i slika 9. prikazuju interni i eksterni privatni računalni oblak [3].

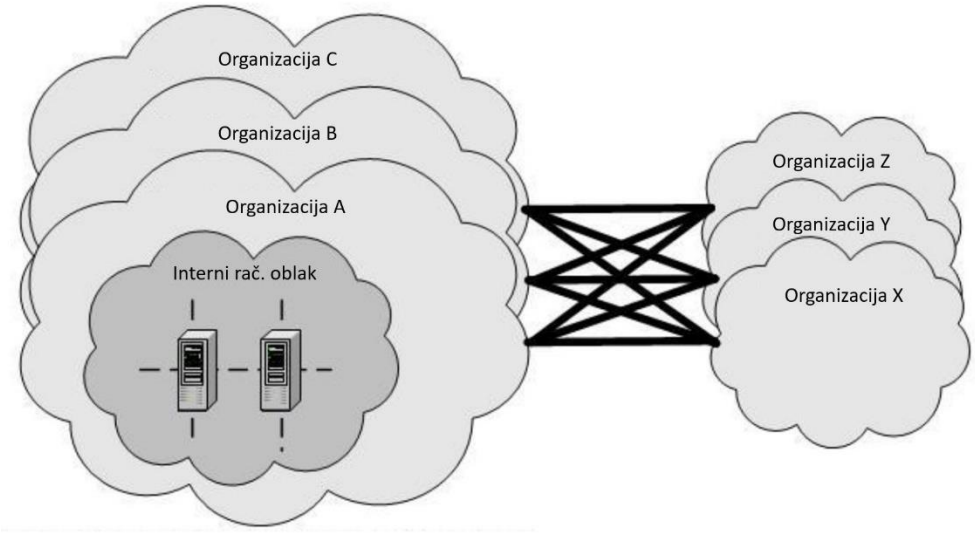


Slika 8. Interni privatni računalni oblak [3]



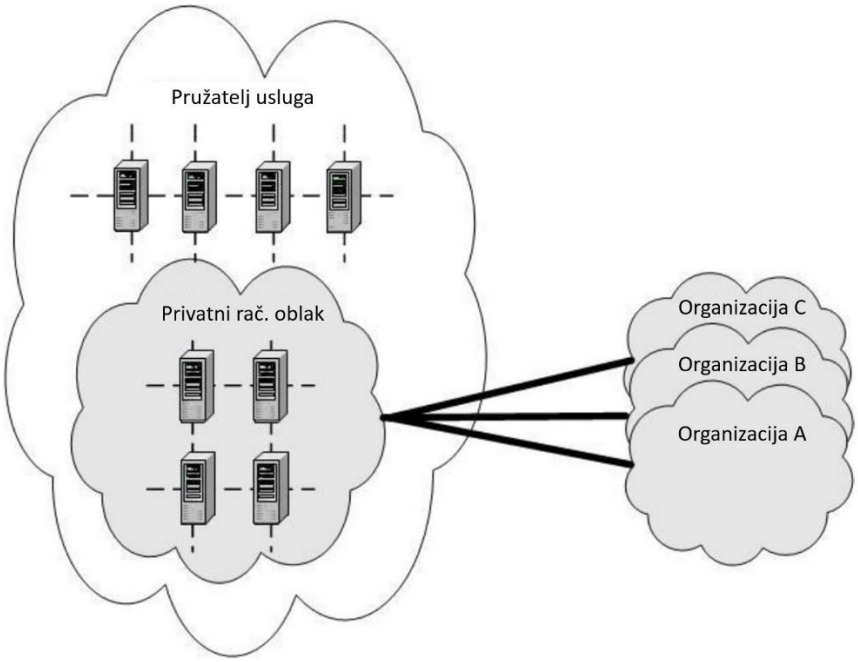
Slika 9. Eksterni privatni računalni oblak [3]

Zajednički model računalstva u oblaku služi grupi korisnika usluga koji imaju zajedničke interese kao što su ciljevi misije društva, sigurnost, privatnost i politika sukladnosti *(eng. compliance policy)*, umjesto da služi jednoj organizaciji kao što to čini privatni računalni oblak. Slično privatnim računalnim oblacima, računalnim oblakom zajednice mogu upravljati te organizacije ili treća strana, a može se implementirati u prostorima organizacija (tj. interni oblak zajednice) ili prepustiti tvrtki koja pruža usluge hostinga (tj. eksterni oblak zajednice). Slika 10. prikazuje interni računalni oblak koji se sastoji od niza organizacija sudionica. Korisnik usluga može pristupiti lokalnim resursima oblaka, kao i resursima drugih organizacija koje sudjeluju putem veza između pridruženih organizacija [3].



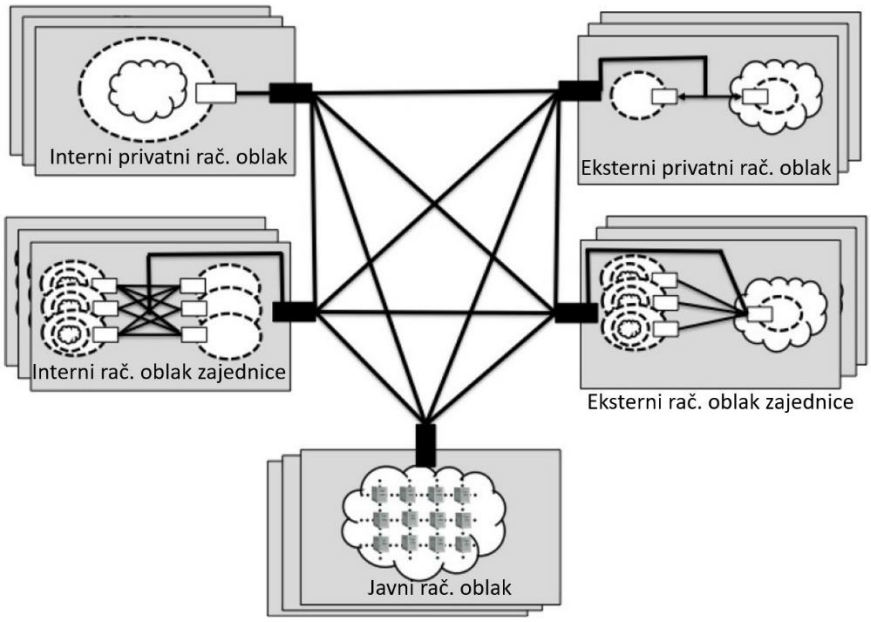
Slika 10. Interni računalni oblak zajednice [3]

Slika 11. prikazuje eksterni računalni oblak zajednice, gdje je poslužiteljska strana prepuštena tvrtki koja pruža usluge hostinga. U ovom slučaju je infrastruktura eksternog računalnog oblaka zajednice izvan prostora organizacija i služi skupu organizacija koje traže i koriste usluge oblaka [3].



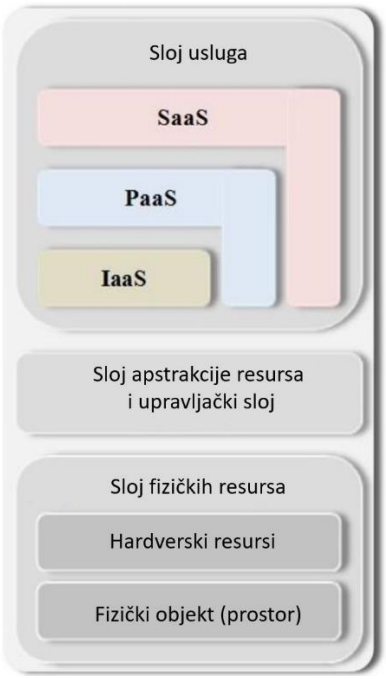
Slika 11. Eksterni računalni oblak zajednice [3]

Hibridni računalni oblak je sastavljen od dvije ili više vrsta računalnih oblaka (interni privatni računalni oblak, interni računalni oblak zajednice, eksterni privatni računalni oblak, eksterni računalni oblak zajednice ili javni računalni oblak) koji ostaju kao različiti entiteti, ali su povezani standardiziranom ili vlastitom tehnologijom koja omogućuje prenosivost podataka i aplikacija [3]. Na slici 12. je prikazan hibridni računalni oblak.



Slika 12. Hibridni računalni oblak [3]

Orkestracija usluga odnosi se na skup komponenti sustava za podršku pružatelju usluga u aktivnostima aranžiranja, koordinacije i upravljanja računalnim resursima u svrhu pružanja usluga računalstva u oblaku korisnicima usluga. Slika 13. prikazuje generički dijagram ovog skupa komponenti koji je temelj pružanja usluga računalstva u oblaku [3].

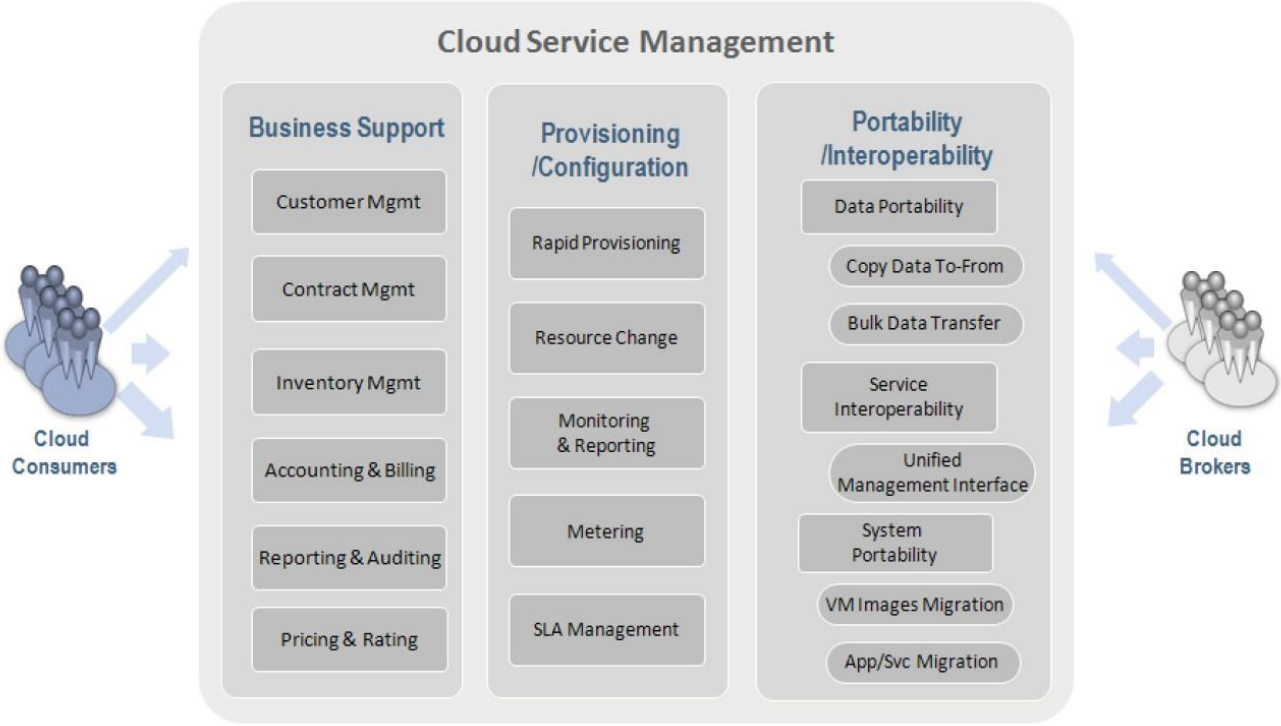


Slika 13. Skup komponenti nužnih za orkestraciju usluga [3]

U ovom se prikazu koristi troslojni model koji predstavlja grupiranje tri vrste komponenti sustava koje pružatelji usluga trebaju sastaviti za isporuku svojih usluga. U modelu prikazanom na slici 13., gornji sloj je sloj usluga, tu pružatelji usluga definiraju sučelja za korisnike usluga za pristup računalnim uslugama. Pristupna sučelja svakog od tri modela usluga nalaze se u ovom sloju. Moguće je, iako nije nužno, da se SaaS aplikacije mogu graditi na PaaS komponentama, a PaaS komponente mogu se graditi na IaaS komponentama. Neobavezni odnosi ovisnosti između komponenti SaaS, PaaS i IaaS predstavljeni su grafički kao komponente naslagane jedna na drugu; dok pravi kut komponenti predstavlja da svaka komponenta usluge može postojati sama za sebe bez ovisnosti o druge dvije komponente. Na primjer, SaaS aplikacija može se implementirati i hostirati na virtualnim strojevima iz IaaS oblaka ili se može implementirati izravno na resurse računalnog oblaka bez korištenja IaaS virtualnih strojeva. Srednji sloj u modelu je sloj apstrakcije resursa i upravljački sloj. Ovaj sloj sadrži komponente sustava koje pružatelji usluga koriste za upravljanje pristupom i pružanje pristupa fizičkim računalnim resursima putem softverske apstrakcije. Primjeri komponenti apstrakcije resursa uključuju softverske elemente kao što su hipervizori, virtualni strojevi, virtualna pohrana podataka i druge apstrakcije računalnih resursa. Apstrakcija resursa mora osigurati učinkovito, sigurno i pouzdano korištenje temeljnih fizičkih resursa. Iako se tehnologija virtualnog stroja obično koristi na ovom sloju, moguća su i druga sredstva za pružanje potrebnih softverskih apstrakcija. Upravljački aspekt ovog sloja odnosi se na softverske komponente koje su odgovorne za dodjelu resursa, kontrolu pristupa i praćenje

korištenja. Ovo softverska struktura povezuje brojne temeljne fizičke resurse i njihove softverske apstrakcije kako bi se omogućilo udruživanje resursa, dinamička dodjela i mjerena (obračunata) usluga. Različiti softveri otvorenog koda i vlastiti softver za računalstvo u oblaku primjeri su ove vrste međuprograma. Najniži sloj u stogu (*eng. stack*) je sloj fizičkih resursa, koji uključuje sve fizičke računalne resurse. Ovaj sloj uključuje hardverske resurse, kao što su računala (CPU i memorija), mrežne komponente (usmjerivači, vatrozidi, preklopnici, mrežne veze i sučelja), komponente za pohranu podataka (tvrdi diskovi) i drugi elementi fizičke računalne infrastrukture. Također uključuje resurse objekta, kao što su grijanje, ventilacija i klimatizacija, napajanje, komunikacije i drugi aspekti fizičkog postrojenja. Slijedeći konvencije o arhitekturi sustava, vodoravno pozicioniranje, tj. slojevitost, u modelu predstavlja odnose ovisnosti – komponente gornjeg sloja ovise o funkcioniranju susjednog nižeg sloja. Sloj apstrakcije resursa i upravljanja resursima, koji se nalazi povrh sloja fizičkih resursa, izlaže virtualne resurse računalnog oblaka i podržava sloj usluga čija su sučelja usluga računalnog oblaka izložena korisnicima usluga, ali korisnici usluga nemaju izravan pristup fizičkim resursima [3].

Upravljanje uslugama/servisima računalstva u oblaku uključuje sve funkcije povezane s uslugama koje su potrebne za upravljanje i rad onih usluga koje zahtijevaju ili potražuju korisnici usluga. Kao što je ilustrirano na slici 14., upravljanje uslugama računalstva u oblaku može se opisati iz perspektive poslovne podrške, pružanja i konfiguracije usluga te iz perspektive zahtjeva prenosivosti i interoperabilnosti [3].



Slika 14. Upravljanje uslugama/servisima računalstva u oblaku [3]

Poslovna podrška uključuje skup usluga povezanih s poslovanjem koje se bave klijentima i procesima podrške. Ona uključuje komponente koje se koriste za pokretanje poslovnih operacija koje su okrenute klijentu. Perspektiva pružanja i konfiguracije usluga uključuje: brzo aktiviranje usluga (automatsko postavljanje sustava u računalnom oblaku na temelju tražene usluge/resursa/mogućnosti i kapaciteta), promjena resursa (prilagodba konfiguracije/dodjele resursa zbog popravaka, nadogradnji i pridruživanja novih čvorova u računalni oblak), praćenje i izvješćivanje, mjerenje isporučene usluge, te upravljanje SLA ugovorima. Prihvatljivost računalstva u oblaku uvelike ovisi o tome kako računalni oblak može odgovoriti na zahtjeve korisnika o sigurnosti, prenosivosti i interoperabilnosti. Što se tiče prenosivosti, potencijalne kupce zanima mogu li premjestiti svoje podatke ili aplikacije u više okruženja računalnih oblaka po niskoj cijeni i uz minimalne smetnje. Iz perspektive interoperabilnosti, korisnici zahtijevaju mogućnost komunikacije između višestrukih računalnih oblaka [3].

Sigurnost je predstavljena kao poprečni presjek koji se proteže kroz sve slojeve referentnog modela računalstva u oblaku od fizičke sigurnosti do sigurnosti aplikacija. Stoga briga o sigurnosti u arhitekturi računalstva u oblaku nije isključivo u djelokrugu pružatelja usluga, već i korisnika oblaka i drugih relevantnih aktera. Sustavi koji se temelje na računalnom oblaku i dalje moraju ispunjavati sigurnosne zahtjeve kao što su autentifikacija, autorizacija, dostupnost, povjerljivost, upravljanje identitetom, integritet, revizija, nadzor sigurnosti,

odgovor na incidente i upravljanje sigurnosnom politikom. Tri modela usluga koja su određena NIST definicijom računalstva u oblaku, tj. SaaS, PaaS i IaaS, predstavljaju korisnicima usluga različite vrste upravljanja uslugama i omogućavaju različite ulazne točke sustava u računalnom oblaku, što stvara različite površine za napad koje napadači potencijalno mogu iskoristiti. Važno je razmotriti utjecaj modela usluga i njihove različite probleme u sigurnosnom dizajnu i implementaciji. Na primjer, SaaS pruža korisnicima pristup uslugama u računalnom oblaku pomoću mrežne veze, obično preko interneta i putem web preglednika [3]. Naglasak je na sigurnosti web preglednika u razmatranjima sigurnosti SaaS sustava u oblaku [4]. Korisnici IaaS usluga koriste virtualne strojeve koji se izvršavaju na hipervizorima na računalima domaćinima pružatelja usluga. Stoga je sigurnost hipervizora u svrhu implementacije izolacije virtualnih strojeva opsežno analizirana od strane pružatelje IaaS usluga koji koriste tehnologije virtualizacije. Varijacije modela implementacije računalstva u oblaku također imaju važne sigurnosne implikacije. Jedan od načina analize sigurnosnih implikacija iz perspektive modela implementacije je različita razina ekskluzivnosti korisnika usluga u modelu implementacije. Privatni računalni oblak namijenjen je jednoj organizaciji, a javni računalni oblak može imati nepredvidive stanare koji koegzistiraju jedni s drugima, stoga je izolacija radnog okruženja manji sigurnosni problem u privatnom oblaku nego u javnom oblaku [3].

Drugi način za analizu sigurnosnog utjecaja modela implementacije računalstva u oblaku je korištenje koncepta granica pristupa *eng. concept of access boundaries*. Na primjer, interni privatni oblak može ali i ne mora imati dodatne sigurnosne mjere na granici računalnog oblaka jer se interni privatni oblak nalazi u prostorima korisnika usluga unutar mrežne granice organizacije (korisnika usluga), dok eksterni privatni oblak obično zahtijeva uspostavljanje perimetralne zaštite na granici računalnog oblaka. Korisnik usluge i pružatelj usluge imaju različite stupnjeve kontrole nad računalnim resursima u sustavu računalstva u oblaku [3].

U usporedbi s tradicionalnim IT sustavima, gdje jedna organizacija ima kontrolu nad kompletnim računalnim resursima i cijelim životnim ciklusom sustava, pružatelji usluga i korisnici usluga zajednički dizajniraju, grade, postavljaju i upravljaju sustavima temeljenim na računalnom oblaku. Podjela kontrole znači da obje strane sada dijele odgovornosti u pružanju odgovarajuće zaštite za sustave temeljene na računalstvu u oblaku. Sigurnost je zajednička odgovornost. Sigurnosne mjere koje se koriste za pružanje zaštite, potrebno je analizirati kako bi se utvrdilo koja strana je u boljoj poziciji za provedbu. Ova analiza treba uključiti razmatranja iz perspektive modela usluge, pri čemu različiti modeli usluga podrazumijevaju različite stupnjeve kontrole između pružatelja usluga i korisnika usluga. Na primjer, sigurnosne mjere upravljanja računom za početne privilegirane korisnike sustava u IaaS scenarijima

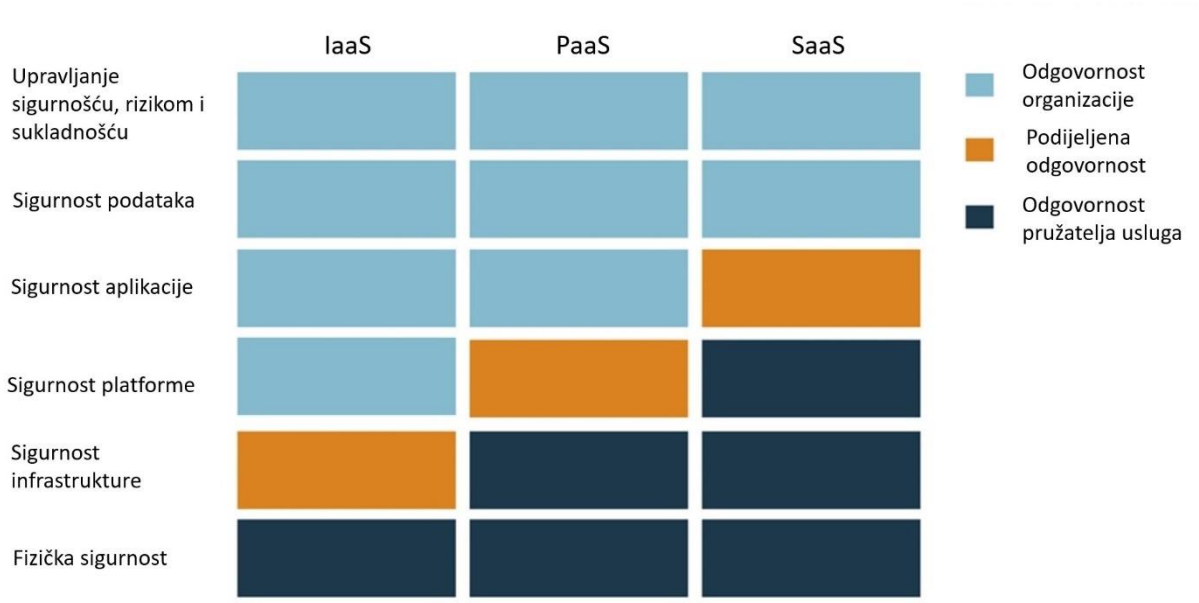
obično izvodi pružatelj IaaS usluge, dok upravljanje korisničkim računom aplikacije za aplikaciju postavljenu u IaaS okruženju obično nije odgovornost pružatelja usluga. Pružatelji usluga trebali bi zaštititi sigurno, ispravno i dosljedno prikupljanje, obradu, komunikaciju, korištenje i raspolaganje osobnim podacima i podacima koji su povezani sa identitetom osobe *eng. personally identifiable information* (PII). Ključni poslovni imperativ morao bi biti osigurati privatnost prikupljenih podataka koji su povezani sa identitetom osobe. To su podaci koji se mogu koristiti za razlikovanje ili praćenje identiteta pojedinca, kao što su njegovo ime, broj socijalnog osiguranja (u Hrvatskoj npr. OIB), biometrijski podaci itd. sami ili u kombinaciji s drugim osobnim ili identifikacijskim podacima koji su povezani ili se mogu povezati s određenim osobama, kao što su datum i mjesto rođenja, majčino djevojačko prezime itd. Iako računalstvo u oblaku pruža fleksibilno rješenje za zajedničke resurse, softver i informacije, ono također predstavlja dodatne izazove u vezi s privatnošću za korisnike koji koriste računalne oblake [3].

4. SIGURNOSNI ZAHTJEVI KORIŠTENJA APLIKACIJA U RAČUNALNOM OBLAKU

Sigurnost i sukladnost (*eng. compliance*) u računalnom oblaku uključuje sve što je dosada bilo obuhvaćeno u sigurnosnoj arhitekturi kompleksnih računalnih sustava, samo u računalnom oblaku. Sve tradicionalne sigurnosne domene ostaju, ali se priroda rizika, uloge i odgovornosti te provedba sigurnosnih mjera radikalno mijenjaju. Iako se cjelokupni opseg sigurnosti i sukladnosti ne mijenja, dijelovi za koje je svaki akter u računalnom oblaku odgovoran svakako se mijenjaju. Računalstvo u oblaku zajednički je tehnološki model gdje su različite organizacije često odgovorne za implementaciju i upravljanje različitim dijelovima stoga (*eng. stack*). Kao rezultat toga, odgovornosti za sigurnost također su raspoređene po cijelom stogu, a time i po uključenim organizacijama. To se uobičajeno naziva model podijeljene odgovornosti. On se može predstaviti kao matrica odgovornosti koja ovisi o određenom pružatelju usluga računalstva u oblaku i značajki/proizvodu, modelu usluge i modelu implementacije [5]. Na visokoj razini apstrakcije, odgovornost za sigurnost preslikava se na stupanj kontrole koji bilo koji akter ima nad arhitekturom stoga [5]:

- Softver kao usluga: pružatelj usluge odgovoran je za gotovo cjelokupni sigurnost, korisnik usluge može upravljati samo vlastitom upotrebom aplikacije i ne može promijeniti način na koji aplikacija radi. Pružatelj SaaS usluga odgovoran je za sigurnost perimetra, bilježenje, praćenje, reviziju te sigurnost aplikacije, dok korisnik usluge može samo upravljati ovlaštenjima i pravima pristupa u aplikaciji.
- Platforma kao usluga: pružatelj usluga odgovoran je za sigurnost platforme, dok je korisnik usluge odgovoran za sve što implementira na platformi, uključujući način na koji konfigurira sve ponuđene sigurnosne značajke. Odgovornosti su tako ravnomjernije podijeljene. Na primjer, kada se koristi baza podataka kao usluga, pružatelj usluge upravlja temeljnom sigurnošću, zakrpama i konfiguracijom jezgre, dok je korisnik usluge odgovoran za sve ostalo, uključujući koje sigurnosne značajke baze podataka koristiti, upravljanje računima ili čak metodama autentifikacije.
- Infrastruktura kao usluga: baš kao i PaaS, pružatelj usluge je odgovoran za temeljnu sigurnost, dok je korisnik usluge odgovoran za sve što gradi na infrastrukturi. Za razliku od PaaS-a, ovo stavlja daleko veću odgovornost na korisnika usluge. Na primjer, pružatelj IaaS usluge će vjerojatno nadzirati svoj perimetar kako bi prepoznao napade, ali korisnik je u potpunosti odgovoran za to kako definira i implementira sigurnost svoje virtualne mreže, na temelju alata dostupnih na usluzi.

Na slici 15. je prikazana podjela odgovornosti za sigurnost između korisnika usluga i pružatelja usluga u ovisnosti o odabranom modelu usluga.



Slika 15. Podjela odgovornosti za sigurnost [6]

Kompleksnost podjele odgovornosti se povećava kada se koriste brokeri usluga ili drugi posrednici i partneri [5]. CSA (Cloud Security Alliance) daje dvije preporuke zbog podijeljene odgovornosti za sigurnost [5]:

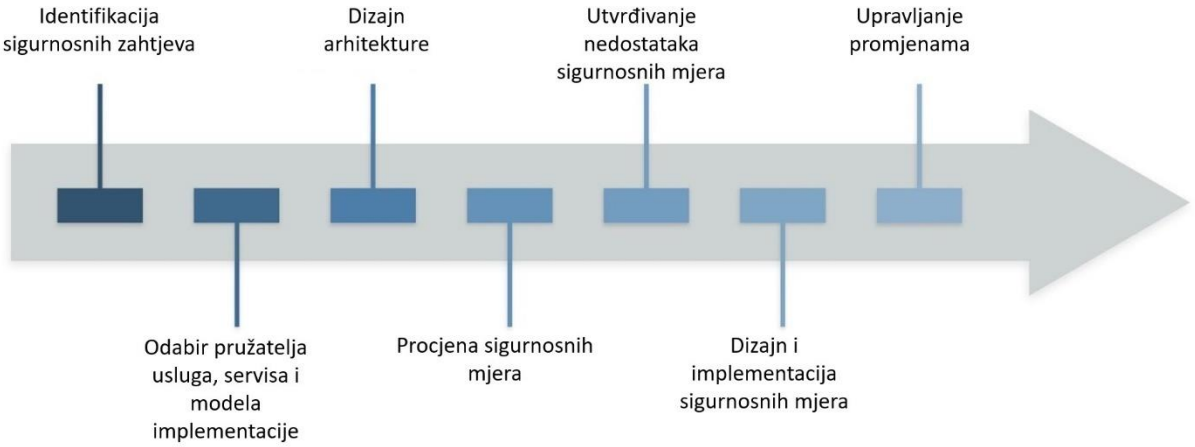
- Pružatelji usluga trebali bi jasno dokumentirati svoje interne sigurnosne mjere i sigurnosne značajke za korisnike kako bi korisnik usluge mogao donijeti odgovarajuću odluku. Pružatelji usluga bi također trebali pravilno dizajnirati i implementirati te sigurnosne mjere.
- Korisnici usluga trebali bi za bilo koji projekt u domeni računalstva u oblaku izraditi matricu odgovornosti kako bi dokumentirali tko implementira koje sigurnosne mjere i kako. To bi također trebalo biti usklađeno sa svim potrebnim standardima sukladnosti *(eng. compliance)*.

Ovisno o pojedinom projektu koji se temelji na računalstvu u oblaku detalji implementacije, potrebne sigurnosne mjere, specifični procesi, razne referentne arhitekture i modeli dizajna uvelike se razlikuju [5]. Zbog toga je u literaturi [5] predstavljen jednostavan model sigurnosnog procesa u računalnom oblaku. Model je prikazan na slici 16. Koraci tog modela su [5]:

- Identifikacija potrebnih sigurnosnih zahtjeva, zahtjeva sukladnosti te svih postojećih sigurnosnih mjera.
- Odabir pružatelja usluga, usluge koje će se upotrebljavati i model implementacije.
- Dizajn arhitekture.
- Procjena sigurnosnih mjera.
- Utvrđivanje nedostataka sigurnosnih mjera.

- Dizajn i implementacija sigurnosnih mjera u svrhu popunjavanja praznina/nedostataka.
- Upravljanje promjenama.

Budući da će različiti projekti temeljeni na računalstvu u oblaku, čak i kad se koriste usluge samo jednog pružatelja usluga, vjerojatno koristiti potpuno različite skupove konfiguracija i tehnologija, svaki projekt treba evaluirati kao samostalnu cjelinu. Na primjer, sigurnosne mjere za aplikaciju postavljenu samo na IaaS uslugama jednog pružatelja usluga mogu izgledati podosta drugačije od sličnog projekta koji umjesto toga koristi više PaaS usluga od istog pružatelja usluga. Ključno je identificirati zahtjeve, dizajnirati arhitekturu i zatim identificirati nedostatke koji proizlaze iz mogućnosti i kapaciteta temeljne platforme računalstva u oblaku [5].



Slika 16. Prikaz modela sigurnosnog procesa [5]

4.1. Upravljanje podacima/informacijama

Definicija upravljanja informacijama/podacima je: Osiguravanje korištenja podataka i informacija u skladu s organizacijskim politikama, standardima i strategijom — uključujući regulatorne, ugovorne i poslovne ciljeve [5]. Primarni cilj informacijske sigurnosti je zaštititi temeljne podatke koji pokreću naše sustave i aplikacije. Kako tvrtke prelaze na računalstvo u oblaku, tradicionalne metode osiguranja podataka dovode se u pitanje zbog implementacije novih arhitektura koje su razvijene za računalstvo u oblaku. Elastičnost (računalnog oblaka), multiklijentski model, nove fizičke i logičke arhitekture te apstraktne mjere sigurnosti zahtijevaju nove strategije za sigurnost podataka. Upravljanje informacijama u eri računalstva u oblaku zastrašujući je izazov koji utječe na sve organizacije i zahtijeva ne samo nove tehničke

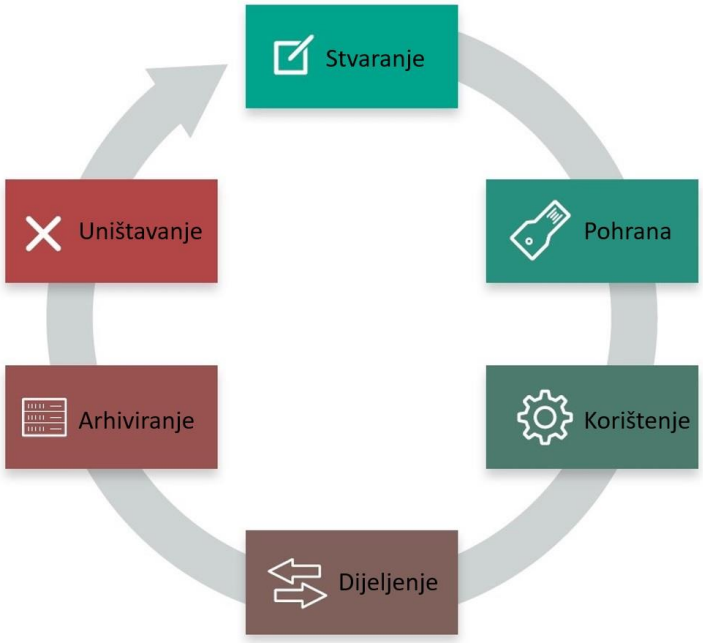
zaštite već i nove pristupe temeljnom upravljanju. Iako računalstvo u oblaku ima barem neki učinak na sva područja upravljanja informacijama, ono posebno utječe na sukladnost, privatnost i poslovne politike zbog povećane složenosti u radu s trećim stranama i upravljanju granicama nadležnosti. Brojni su aspekti pohranjivanja podataka u računalnom oblaku koji utječu na zahtjeve upravljanja informacijama i podacima. Jedan od tih aspekata je multiklijenstki način rada, on unosi kompleksne sigurnosne implikacije u funkcioniranje sustava. Kada se podaci pohranjuju u javnom računalnom oblaku, pohranjuju se na zajedničkoj infrastrukturi s trećim, nepouzdanim stranama (korisnicima usluga). Čak i pri korištenju privatnog računalnog oblaka, podaci se pohranjuju i njima se upravlja na infrastrukturi koju dijele različite poslovne jedinice, koje vjerojatno imaju različite potrebe za upravljanje podacima. Zbog sve većeg dijeljenja računalnih okruženja rastu i zajedničke sigurnosne odgovonosti. Postaje sve vjerojatnije da će podatke posjedovati i njima upravljati različiti timovi ili čak organizacije. Dakle, važno je razlikovati između povjereništva nad podacima i vlasništva nad podacima. Vlasništvo se odnosi na to tko posjeduje podatke. Nije uvijek savršeno jasno tko posjeduje podatke. Korisnik usluga može pružiti podatke, a pružatelj usluga onda posjedovati te podatke ili ih korisnik usluga još uvijek može zakonski posjedovati, sve ovisi o zakonu, ugovorima i poslovnim politikama organizacija. Ako se podaci hostiraju na javnom pružatelju usluga, trebao bi ih posjedovati korisnih usluga, ali i to opet može ovisiti o ugovorima. Povjereništvo nad podacima se odnosi na to tko upravlja podacima. Ako korisnik usluga daje svoje osobne podatke, a pružatelj usluga nema prava vlasništva nad tim podacima onda je pružatelj usluga samo povjerenik nad tim podacima. To znači da pružatelj usluga može te podatke koristiti samo na odobrene načine. Ako korisnik usluge koristi usluge pružatelja usluga kroz javni model implementacije računalnog oblaka, pružatelj usluge postaje povjerenik nad podacima no i korisnik usluge vjerojatno ima odgovornost nad podacima, barem djelomičnu, ovisno o mjerama koje korisnik usluge implentira i s kojima upravlja. Korištenjem usluga pružatelja usluga, korisnik usluga se ne oslobađa odgovornosti za podatke. U osnovi, vlasnik podataka definira pravila (ponekad neizravno, kroz regulaciju), a povjerenik podataka provodi ta pravila. Na uloge i granice uloga vlasnika podataka i povjerenika podataka utječe i infrastruktura računalnog oblaka, osobito u slučaju javnog modela računalstva u oblaka. Smještanjem klijentskih podataka u računalni oblak, uvodi se pružatelj usluga kao nova strana u model upravljanja. Zbog toga što računalstvo u oblaku omogućuje smještanje podataka na više lokacija (jurisdikcija) potrebne su dodatne mjere kako bi se podaci ograničili na odgovarajuće lokacije. Računalstvo u oblaku ima utjecaj na sukladnost, propise i pravila o privatnosti. Ugovor korisnika usluga s (njegovim) klijentom može sprječavati dijeljenje ili

upotrebu podataka na infrastrukturi pružatelja usluga ili mogu postojati sigurnosni zahtjevi kao na primjer enkripcija podatka. Uništavanje i uklanjanje podataka je povezano s tehničkim mogućnostima platforme računalstva u oblaku, neophodno je osigurati uništavanje i uklanjanje podataka u skladu sa poslovnom politikom organizacije [5].

Domene upravljanja podacima na koje računalstvo u oblaku ima velik utjecaj su [5]:

- Klasifikacija podataka. Često je povezano sa sukladnošću *(eng. compliance)* i utječe na destinacije u računalnom oblaku te zahtjevima u pogledu postupanja. Nije nužno da svaka organizacija ima program za klasifikaciji podataka, no ako ga ima onda se i on mora prilagoditi za računalstvo u oblaku.
- Politike upravljanja informacijama. Te politike su povezane s klasifikacijom i dio o računalstvu u oblaku je potrebno dodati u te politike. Također bi trebale pokriti različite modele usluga računalstva u oblaku, budući da se slanje podataka pružatelju SaaS usluge odnosno izrada vlastite aplikacije na infrastrukturi pružatelja IaaS usluge značajno razlikuje.
- Politike lokacije i nadležnosti. Ove politike imaju izravne implikacije u računalstvu u oblaku. Svaki eksterni hosting mora biti u skladu s lokacijskim i pravnim zahtjevima. Interne politike se mogu promijeniti, ali je nužno pridržavati se zakonskih zahtjeva. Postoji i mogućnost da internacionalni sporazumi i nacionalni zakoni stvore konflikte u postupanju.
- Ovlaštenja. Računalstvo u oblaku zahtijeva minimalne promjene kod autorizacija.
- Vlasništvo. Organizacija je uvijek odgovorna za podatke i informacije i te odgovornosti se ne mogu odbaciti prelaskom na računalstvo u oblaku.
- Povjereništvo. Pružatelj usluga može postati povjerenik nad podacima. Hostirani podaci ali ispravno enkriptirani su još uvijek pod povjereništvom organizacije.
- Privatnost. Privatnost je zbroj regulatornih zahtjeva, ugovornih obveza i obveza prema kupcima (npr. javne izjave). Mora se razumjeti sve zahtjeve i osigurati usklađenost upravljanja informacijama i sigurnosnih politika.
- Ugovorne kontrolne mjere. Ovo je pravni alat koji se koristi za postavljanje upravljačkih zahtjeva na treće strane kao što je pružatelj usluga.
- Sigurnosne mjere. Sigurnosne mjere su alat za implementaciju procesa/domene upravljanja podacima. Ove mjere se značajno mijenjaju u računalstvu u oblaku naspram klasičnih modela računalstva.

Alat za modeliranje i evaluaciju sigurnosti podataka pogledom s visoke razine te postavljanja fokusnih točaka jest sigurnosni ciklus podataka *eng. Data Security Lifecycle*. Taj ciklus sadrži šest faza, od stvaranja do uništenja. Na Slici 17. je prikazan sa linearnim (slijednim) procesom. No unatoč tome podaci mogu nakon što su stvoreni bez ograničenja prelaziti između faza te ne moraju nužno proći kroz sve faze [5].

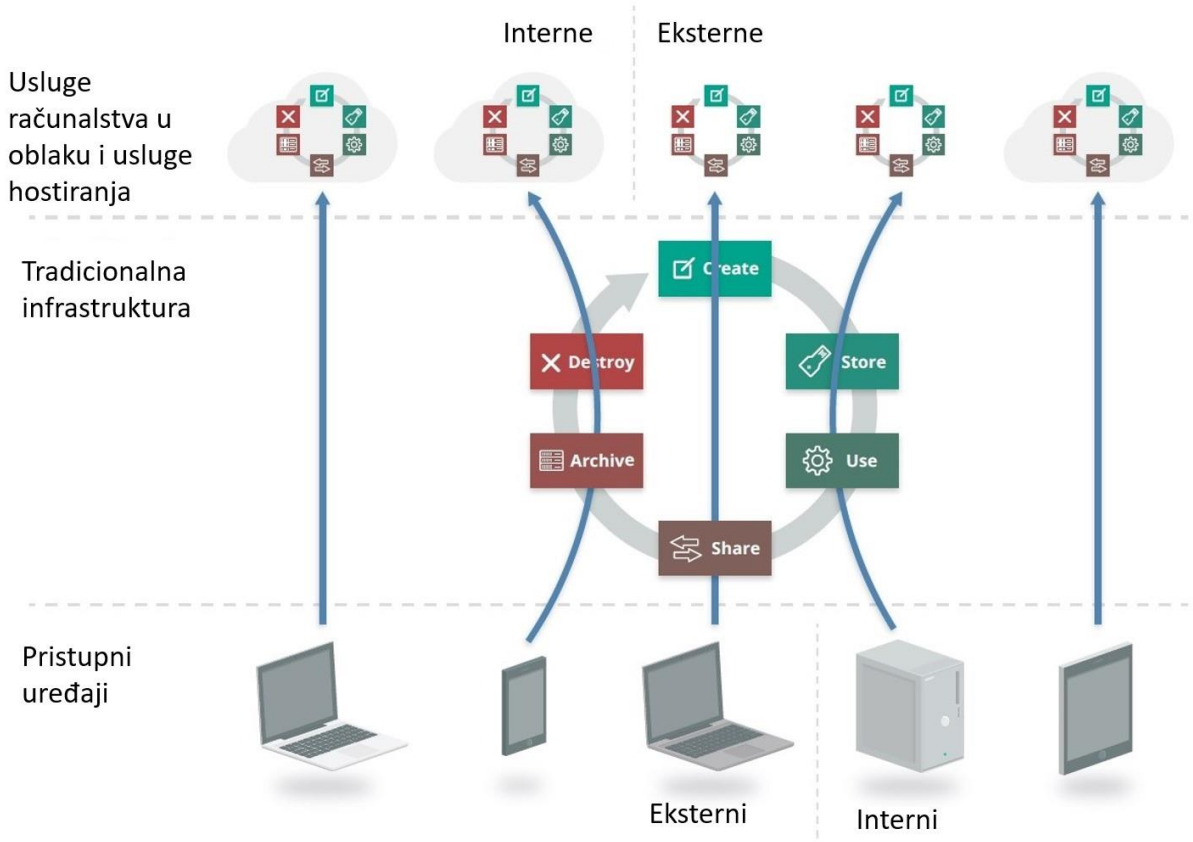


Slika 17. Ciklus sigurnosti podataka [5]

Šest faza tog ciklusa su [5]:

- Stvaranje. Ova faza ciklusa je stvaranje novog digitalnog sadržaja ili izmjena/ažuriranje/modificiranje postojećeg sadržaja.
- Pohranjivanje. Ova faza ciklusa je čin obvezivanja/predaje digitalnih podataka u neku vrstu spremišta za pohranu podataka i obično se događa istovremeno sa fazom stvaranja.
- Korištenje. U ovoj fazi ciklusa se podaci pregledavaju, obrađuju ili se koriste na neki drugi način u nekoj vrsti aktivnosti (ne uključujući modificiranje).
- Dijeljenje. Informacije su dostupne drugima, primjerice između korisnika, kupaca i partnera.
- Arhiviranje. Podaci napuštaju aktivnu uporabu i ulaze u dugoročnu pohranu.
- Uništavanje. Podaci se trajno uništavaju korištenjem fizičkih ili digitalnih sredstava (npr. kripto uništavanje *eng. cryptoshredding*).

Ciklus predstavlja faze kroz koje informacija prolazi, ali se ne bavi njezinom lokacijom ili načinom na koji joj se pristupa. Važnost lokacija podatka najbolje se može ilustrirati kad se ciklus predstavi, ne kao jedan linearni proces, već kao skup više ciklusa koji se odvijaju paralelno u različitim okruženjima. U gotovo bilo kojoj fazi podaci se mogu kretati u, iz ili između tih okruženja. Podacima se pristupa i pohranjuju se na više lokacija, a svaka ima svoj životni ciklus [5]. To je ilustrirano na slici 18.



Slika 18. Lokacije i način pristupa podacima [5]

Zbog svih potencijalnih regulatornih, ugovornih i drugih pitanja vezanih uz nadležnost, izuzetno je važno razumjeti i logičku i fizičku lokaciju podataka. Još jedna bitna stvar su prava korisnika (*eng. entitlements*). Nakon što su definirane lokacije i kretanja podataka mora se definirati tko i kako pristupa podacima. Podacima se danas pristupa pomoću raznih uređaja. Ovi uređaji imaju različite sigurnosne karakteristike i mogu koristiti različite aplikacije ili klijente [5]. Postoje tri aktivnosti koje se mogu vršiti s danim podatkom, tj. tri funkcije [5]:

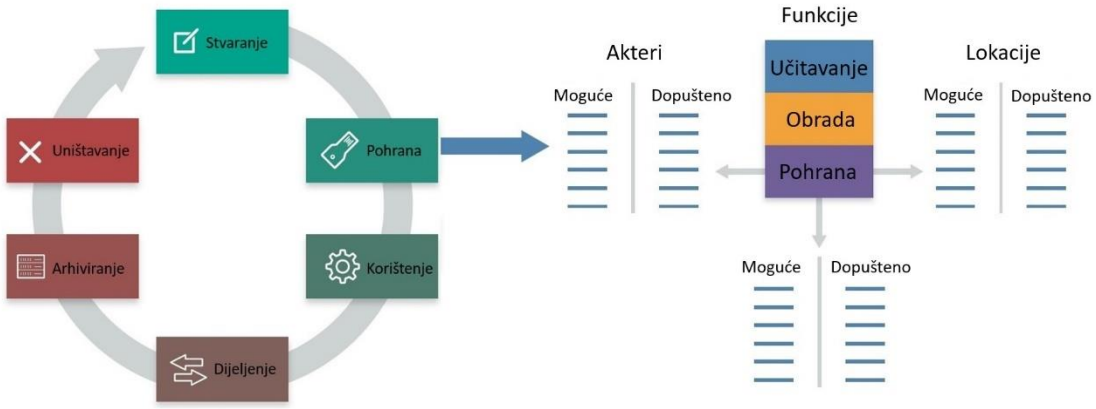
- Učitati. Pregledavanje/učitavanje podatka, uključujući stvaranje, kopiranje, prijenos datoteka, slanje/širenje i ostale razmjene podataka.
- Procesiranje/obrada. To je izvršenje transakcije na podacima, ažuriranje podataka ili korištenje poslovnoj obradi/transakciji itd.
- Pohranjivanje. Čuvanje podataka (u datoteci, bazi podataka itd.).

Tablica 1. prikazuje mapiranje ove 3 funkcije nad ciklusom sigurnosti podatka [5].

Tablica 1. Mapiranje funkcija [5]

	Stvaranje	Pohranjivanje	Korištenje	Dijeljenje	Arhiviranje	Uništavanje
Učitavanje	**X**	**X**	**X**	**X**	**X**	**X**
Obrada	**X**		**X**			
Pohranjivanje		**X**			**X**	

Akter (osoba, aplikacija ili sustav/proces, za razliku od pristupnog uređaja) obavlja svaku funkciju na nekoj lokaciji. Sigurnosne mjere onda ograničavaju moguće radnje aktera na dopuštene radnje [5]. Tako se osigurava da samo akteri sa dovoljnim pravima izvršavaju funkcije dopuštene funkcije nad podacima i to na dozvoljenim lokacijama, što je ilustrirano na slici 19.



Slika 19. Mapiranje funkcija i sigurnosnih mjera [5]

4.2. Sigurnost i enkripcija podataka

Sigurnost podataka je ključni alat za provedbu politika upravljanja informacijama i podacima. To vrijedi za sigurnost podataka općenito, neovisno da li uključeno računalstvo u oblaku ili ne. Mnoge organizacije nemaju iskustvo povjeravanja velike količine svojih osjetljivih podataka, ako ne i sve, trećoj strani ili miješati sve svoje interne podatke u zajednički skup resursa (računalni oblak). Zbog toga organizacije znaju postaviti opću sigurnosnu politiku za sve što se nalazi u računalnom oblaku umjesto da se drže daleko sigurnijeg i isplativijeg pristupa temeljenog na analizi rizika. Ako organizacija koja koristi SaaS model računalstva u oblaku sve kriptira jer nema povjerenja u tog pružatelja usluga, to vjerojatno znači da ne bi

trebala koristi usluge tog pružatelja usluga. Problem takvog postupka jest što enkripcija svega kao rješenje može dovesti do lažnog osjećaja sigurnosti npr. enkripcija podatkovnog prometa bez osiguravanja sigurnosti samih uređaja. Mjere za sigurnost podataka se obično dijele u tri skupine [5]. A to su [5]:

- Kontroliranje podataka koji idu računalni oblak (i gdje idu).
- Zaštita i upravljanje podacima u računalnom oblaku. Ključne mjere i procesi su:
  - Sigurnosne mjere pristupa.
  - Enkripcija.
  - Arhitektura.
  - Praćenje/upozoravanje (upotrebe, konfiguracije, stanja ciklusa itd.).
  - Dodatne sigurnosne mjere uključujući one koje se odnose na određeni proizvod/uslugu/platformu pružatelja usluga, sprječavanje gubitka podataka itd.
- Provedba mjera sigurnosti tijekom informacijskog ciklusa.
  - Upravljanje podacima o lokaciji/rezidenciji.
  - Osiguravanje sukladnosti, uključujući revizijske artefakte kao što su logovi (dnevnici) i konfiguracije.
  - Sigurnosne kopije i kontinuitet poslovanja.

Budući je pohranjivanje u računalnom oblaku virtualizirano, to obično zahtijeva drugačije vrste pohrane podataka od onih koje se koriste u tradicionalnim tehnologijama pohranjivanja. Ispod virtualizacijskog sloja se mogu koristiti standardni ili tradicionalni mehanizmi za pohranjivanje, ali tehnologije virtualizacije pohranjivanja podataka u računalnom oblaku kojima korisnici pristupaju bit će drugačije [5]. Najčešće tehnologije pohranjivanja podataka kojima će korisnici usluga pristupati su [5]:

- Objektna pohrana (*eng. object storage*): Objektna pohrana slična je datotečnom sustavu. "Objekti" su obično datoteke koje se zatim pohranjuju pomoću mehanizma specifičnog za platformu računalstva u oblaku. Pristupa se većinom putem API-ja, a ne pomoću standardnih protokola za dijeljenje datoteka, no pružatelji usluga također mogu ponuditi pristupna sučelja (*eng. front-end interfaces*) kako bi podržali te protokole.
- Volumna pohrana podataka (*eng. volume storage*): Ovo je u biti virtualni tvrdi disk za instance/virtualne strojeve.
- Baza podataka: platforme i pružatelji usluga mogu podržavati niz različitih vrsta baza podataka, uključujući postojeće komercijalne opcije i opcije otvorenog koda (*eng. open source)* te vlastite sustave. Baze podataka na temelju vlastitih tehnologija obično koriste vlastito razvijene API-je. Komercijalne baze podataka ili baze podataka otvorenog koda hostirane su kod pružatelja usluga i obično koriste postojeće standarde za komunikaciju. Te baze podataka mogu biti relacijske ili nerelacijske.
- Aplikacija/platforma: Primjer toga bila bi mreža za isporuku sadržaja *eng. content delivery network* (CDN), datoteke pohranjene u SaaS-u, predmemoriji *eng. caching* i druge nove opcije.

Prije osiguravanja podataka u oblaku, većina organizacija zahtijeva neki način upravljanja podacima koji su pohranjeni u privatnim i javnim infrastrukturama pružatelja usluga. Ovo je često barem jednako bitno za sukladnost (*eng. compliance)*, a nekad i više, nego za sigurnost. Za početak bi organizacije trebale definirati politike za podatke, tj. koje vrste podataka su dozvoljene te koje su lokacije dozvoljene za te vrste podataka, a zatim se te politike povezuju sa temeljnim sigurnosnim zahtjevima. Pored toga organizacije moraju identificirati svoja ključna spremišta podataka te ih nadzirati kako bi se uočile velike migracije ili aktivnosti. Za takvo nadziranje se koriste alati kao što su nadzor aktivnosti baze podataka *eng. Database Activity Monitoring* i nadzor aktivnosti datoteka *eng. File Activity Monitoring*. S tim alatima se u suštini izgrađuje sustav ranog upozorenja za velike prijenose podataka, ali isto tako je to važna sigurnosna mjera za otkrivanje svih vrsta velikih napada i scenarija zlouporabe [5]. Kako bi se otkrile stvarne migracije podataka, organizacije bi trebale nadzirati korištenje računalnog oblaka i sve prijenose podataka. To se može učiniti pomoću sljedećih alata [5]:

- CASB: Brokeri za pristup i sigurnost u računalnom oblaku *eng. Cloud Access and Security Brokers* (također poznati kao *eng. Cloud Security Gateways*) oni otkrivaju internu upotrebu cloud usluga pomoću različitih mehanizama kao što je nadzor mreže, integracija s postojećim mrežnim pristupnikom *eng. network gateway* ili alatom za nadzor, ili čak praćenjem DNS (*eng. Domain Name System*) upita. Nakon što se otkrije na koje se usluge interni korisnici povezuju, većina tih proizvoda nudi praćenje aktivnosti na odobrenim uslugama putem API veza (ako su dostupne) ili presretanje u mreži *eng. inline interception*. Mnogi od tih proizvoda podržavaju DLP (*eng. Data Loss Prevention*) i druga sigurnosna upozorenja te čak nude mjere za bolje upravljanje korištenjem osjetljivih podataka pri korištenju usluga u računalnom oblaku (SaaS/PaaS/i IaaS).
- URL (*eng. Uniform Resource Locators*) filtriranje: Iako nije tako robusno kao CASB, URL filtar/web pristupnik može pomoći da se shvati koje usluge u oblaku korisnici u organizaciji koriste (ili pokušavaju koristiti).
- DLP (*eng. Data Loss Prevention*): Ako se prati web promet (i gleda unutar SSL veza, *eng. Secure Sockets Layer*) alat kao što je prevencija gubitka podataka (DPL) može pomoći u otkrivanju migracija podataka na usluge računalstva u oblaku. Međutim, neki SDK-ovi (*eng. Software Development Kit*) i API-ji u računalnom oblaku mogu enkriptirati dijelove podataka i prometa koje onda DLP alati ne mogu u potpunosti prepoznati i korektno klasificirati.

Naravno da organizacije moraju zaštiti svoje podatke i dok ih premještaju u računalni oblak. To zahtjeva razumijevanje mehanizama migracije podataka od odabranog pružatelja usluga, budući da je korištenje mehanizama pružatelja usluga često sigurnije i isplativije od manualnih prijenosa podataka kao što je pomoću SFTP protokol (*eng. Secure File Transfer Protocol*). Na primjer, slanje podataka u sustav objektnog pohranjivanja podataka pružatelja usluga i to putem API-ja vjerojatno je pouzdanije i sigurnije od postavljanja vlastitog SFTP poslužitelja na

virtualnom računalu istog pružatelja usluga. Postoji nekoliko opcija za enkripciju prijenosa podataka ovisno o tome što platforma računalstva u oblaku podržava. Jedan od načina je enkripcija prije slanja u oblak (enkriptiranje na strani klijenta). Mrežna enkripcija (TLS/SFTP/itd.) je još jedna opcija. Većina API-ja pružatelja usluga kao standardnu postavku koristi TLS (*eng. Transport Layer Security*), a ako to ne koriste, onda je uputno izabrati drugog pružatelja usluga jer je TLS izuzetno bitna funkcionalnost. Enkripcija temeljena na posredniku (*eng. proxy*) može biti treća opcija, u kojoj se posrednik zadužen za enkripciju postavlja u računalnu oblast (područje) od povjerenja ali i između pružatelja usluga i korisnika usluga, tada posrednik upravlja enkripcijom prije prijenosa podataka pružatelju usluga. U nekim instancama organizacije moraju prihvatiti javne ili nepouzdane podatke, ako organizacije dopuštaju partnerima ili javnosti da im šalju takve podatke onda bi organizacije trebale imati sigurnosne mehanizme za provjeru takvih podatka kako bi se oni očistili od neželjenih/zaostalih podataka. Uputno je uvijek izolirati i skenirati podatke prije miješanja ili integriranja sa postojećim podacima [5].

Mjere kontrole pristupa i enkripcije su temeljne mjere u području sigurnosti podataka u različitim tehnologijama. Kontrole pristupa trebaju biti implementirane s najmanje tri sloja [5]:

- Upravljački sloj: ovdje se nalaze kontrole za upravljanje pristupom korisnika koji izravno pristupaju upravljačkom sloju platforme u oblaku. Na primjer, prijava na web konzolu IaaS usluge omogućit će tom korisniku pristup podacima u pohrani objekta. Većina platformi i pružatelja usluga kao standardnu postavku imaju mjere zabrane pristupa ovom sloju.
- Javne i interne kontrole dijeljenja: ako se podaci dijele eksterno s javnošću ili partnerima koji nemaju izravan pristup platformi u oblaku, postojat će drugi sloj kontrola za ovaj pristup.
- Kontrole na razini aplikacije: ove kontrole implementiraju same organizacije koje izrađuju aplikacije.

Opcije za kontrolu pristupa razlikovat će se ovisno o modelu usluge računalstva u oblaku i značajkama specifičnim za pružatelja usluga. Organizacije bi trebale izraditi matricu ovlaštenja na temelju specifičnih mogućnosti platforme. Matrica ovlaštenja dokumentira koji korisnici, grupe i uloge trebaju pristupiti kojim resursima i funkcijama. Idealno bi bila kontinuirana provjera kontrola da li ispunjavaju zahtjeve organizacije, uz posebnu pozornost posvećenu svim javnim dijeljenjima podataka. Razina potencijalnih prava uvelike će se razlikovati od tehnologije do tehnologije. Neke baze podataka mogu podržavati sigurnost i na niskim

razinama (*eng. low-level*) dok druge podržavaju malo više od širokog pristupa. Važno je razumjeti mogućnosti, mapirati ih i izgraditi matricu [5].

Opcije enkripcije uvelike se razlikuju ovisno o modelu usluge, pružatelju usluga i specifičnostima aplikacije/implementacije. Upravljanje ključevima (*eng. key management*) jednako je bitno kao enkripcija. Enkripcija i tokenizacija su dvije odvojene tehnologije. Enkripcija štiti podatke primjenom matematičkog algoritma koji "šifrira/premeće" podatke, koji se potom mogu povratiti samo provođenjem procesa dešifriranja s odgovarajućim ključem. Tokenizacija, s druge strane, uzima podatke i zamjenjuje ih nasumičnim vrijednostima. Zatim pohranjuje izvornu i nasumičnu verziju u sigurnu bazu podataka za kasnije korištenje. Tokenizacija se često koristi kada je format podataka važan (npr. zamjena brojeva kreditne kartice u postojećem sustavu koji zahtijeva isti format). Postoje i enkripcije koje zadržavaju format podataka, kao što je to slučaj sa tokenizacijom, no te vrste enkripcije možda nisu toliko kriptografski sigurne kao standardne enkripcije zbog navedenog kompromisa oko formata. Tri su komponente sustava za enkripciju: podaci, mehanizam za enkripciju i upravljanje ključevima. Podaci su informacije koje se enkriptiraju. Mehanizam za enkripciju je ono što izvodi matematički proces enkripcije. Upravitelj ključeva rukuje ključevima za enkripciju. Cjelokupni dizajn sustava fokusiran je na to gdje implementirati svaku od ovih komponenti. Pri dizajniranju sustava enkripcije, trebalo bi se početi od modela prijetnji [5].

Kod IaaS modela računalstva u oblaku postoje različite metode enkripcije koje naravno ovise o podacima koji se koriste [5]:

- Enkripcija volumne pohrane podataka
  - Enkripcija kojom upravlja instanca volumne pohrane podataka: Mehanizam za enkripciju radi unutar instance, a ključ je pohranjen unutar sustava, ali je zaštićen zaporkom ili parom ključeva.
  - Eksterno upravljana enkripcija: Enkripcijski mehanizam se izvršava u instanci volumne pohrane podataka, ali se ključevima upravlja eksterno i izdaju se instanci na zahtjev.
- Objektna pohrana podataka i pohranjivanje datoteka
  - Enkripcija na strani klijenta: Kada se objektna pohrana podataka koristi kao pozadinski dio (*eng. back-end*) za aplikaciju (uključujući mobilne aplikacije), trebalo bi koristiti mehanizme za enkripciju koji su ugrađeni u aplikaciju ili klijenta (*eng. client*).
  - Enkripcija na strani poslužitelja: Podaci se kriptiraju na strani poslužitelja (u računalnom oblaku) nakon prijenosa. Pružatelj usluge ima pristup ključu i pokreće mehanizam za kriptiranje.
  - Enkripcija pomoću posrednika (*eng. proxy*): U ovom modelu se povezuje pohrana podataka (na strani računalnog oblaka) s posebnom instancom ili uređajem /softverom (koji služi za enkriptiranje), a zatim se povezuje instanca korisnika

usluge s instancom za enkriptiranje. Posrednik upravlja svim kripto operacijama i može čuvati ključeve interno ili eksterno.

Kod PaaS modela računalstva u oblaku enkripcija izrazito varira zbog različitih vrsta PaaS platformi. Vrste enkripcija u PaaS modelu su [5]:

- Enkripcija u aplikacijskom sloju: Podaci su enkriptirani u PaaS aplikaciji ili klijentu koji pristupa platformi.
- Enkripcija baze podataka: podaci su enkriptirani u bazi podataka pomoću enkripcije koja je ugrađena i koju podržava platforma baze podataka kao što je TDE (*eng. Transparent Database Encryption*).
- Ostali slojevi: Ovo su slojevi kojima upravlja pružatelj usluga u aplikaciji, kao što je sustav za prijenos poruka (*eng. messaging queue*).

Pružatelji SaaS usluga mogu koristiti bilo koju od opcija koje su prethodno navedene [5]. Preporuka u literaturi je da se koriste zasebni i jedinstveni ključevi za svakog korisnika usluga kada je to moguće, kako bi se implementirala multiklijentska izolacija. Vrste enkripcija u SaaS modelu [5]:

- Enkripcija kojom upravlja pružatelj usluga: podaci su enkriptirani u SaaS aplikaciji i općenito njima upravlja pružatelj usluga.
- Enkripcija pomoću posrednika (*eng. proxy*): Podaci prolaze kroz posrednika za enkripciju prije slanja u SaaS aplikaciju.

Temeljni zahtjevi za upravljanje ključevima su performanse, pristupačnost, latencija i sigurnost [5]. Postoje četiri moguće opcije za upravljanje ključevima [5]:

- HMS (*eng. hardware security module)* uređaj: Koristi se hardverski sigurnosni modul (HMS) koji obično mora biti na lokaciji i koji će isporučivati ključeve u računalni oblak preko posebne veze.
- Virtualni uređaj/softver: Implementira se virtualni uređaj ili softverski upravitelj ključeva u računalnom oblaku.
- Servis pružatelja usluga: Ovo je servis pri kojem upravljanje ključevima nudi pružatelj usluga.
- Hibridna opcija: Također se može koristiti kombinacija gore navedenih opcija.

Korisničko upravljanje ključevima omogućuje korisniku usluga da upravlja vlastitim ključevima za enkripciju dok pružatelj usluga upravlja mehanizmima za enkripciju. Na primjer, korištenje vlastitog ključa za enkriptiranje SaaS podataka unutar SaaS platforme. Mnogi pružatelji usluga enkriptiraju podatke jer to koriste kao standardnu postavku načina na koji rade, no pri tome koriste ključeve koji su u potpunosti pod njihovom kontrolom. Neki od tih pružatelja usluga dopuštaju da njihove ključeve korisnik usluga zamjeni s vlastitim ključevima koji se onda integriraju s njihovim sustavom enkriptiranja. Nužna je provjera da su li prakse pružatelja usluga u skladu sa sigurnosnim zahtjevima (organizacije). Neki pružatelji usluga mogu zahtijevati da se koristi isključivo njihov servis za upravljanje ključevima. Dakle, iako

ključem upravlja korisnik usluga, još uvijek je potencijalno dostupan pružatelju usluga. To ne znači nužno da je nesiguran, budući da se sustavi za upravljanje ključevima i sustavi za pohranu podataka mogu razdvojiti, potencijalna ugroza podataka bi zahtijevala tajni dogovor od strane više zaposlenika unutar organizacije pružatelja usluga. Međutim, ključevi i podaci i dalje mogu biti dostupni zahtjevima vlasti, ovisno o lokalnim zakonima. Postoji i opcija da se ključevi pohranjuju eksterno (ne kod pružatelja usluga) i da ih se prosljeđuje pružatelju usluga samo na zahtjev [5].

Arhitektura aplikacije značajno utječe na sigurnost podataka. Značajke koje nudi pružatelj usluga mogu smanjiti površinu napada, ali svakako se od pružatelja usluga treba zahtijevati visoku sigurnost metastrukture. Na primjer, stvaranje prekida u mreži korištenjem pohrane u računalnom oblaku ili sustava za prijenos poruka (*eng. queue service*) koji radi na mreži pružatelja usluga, a ne unutar vlastite virtualne mreže (od korisnika usluga). To prisiljava napadače da ili temeljno kompromitiraju pružatelja usluga ili da se ograniče na napade na razini aplikacije, budući da su putevi mrežnog napada zatvoreni. Primjer bi bio korištenje objektne pohrane za prijenos podataka i skupnu obradu (*eng. batch processing*), a ne SFTP prema statičkim instancama. Drugi primjer bi bio prekidanje tijeka poruka unutar sustava za prijenos poruka (*eng. massage queue gapping*) to znači pokretanje komponenti aplikacije na različitim virtualnim mrežama koje su premoštene samo prosljeđivanjem podataka kroz sustav prijenosa podataka od pružatelja usluga. Ovo eliminira mrežne napade s jednog dijela aplikacije na drugi. Funkcije nadzora, revizije i upozoravanja bi se trebale povezati s ukupnim praćenjem računalnog oblaka. Potrebno je identificirati i upozoriti na bilo kakav javni pristup ili promjene ovlaštenja za osjetljive podatke. Neophodno je nadzirati i pristup API-jima i pristup pohrani podataka, budući da podaci mogu biti izloženi kroz oboje, i pristupom podacima u objektnoj pohrani putem API poziva, i putem URL-a za javno dijeljenje. Jedna od opcija je i praćenje aktivnosti, uključujući praćenje aktivnosti baze podataka. Zapisi (*eng. logs*) se obavezno moraju pohraniti na sigurnu lokaciju, poput namjenskog računa za bilježenje (*eng. dedicated logging account*). DLP (*eng. Data Loss Prevention*) je obično način praćenja i zaštite podataka kojima korisnici pristupaju putem praćenja lokalnih sustava, weba, e-pošte i drugog prometa. Obično se ne koristi unutar podatkovnih centara i stoga je primjenjiviji na SaaS nego na PaaS ili IaaS (gdje se obično ne primjenjuje). Neki CASB-ovi uključuju osnovne DLP značajke za sankcionirane (dopuštene/ispravne) usluge koje štite. Na primjer, može se postaviti pravilo da se broj kreditne kartice nikada ne pohranjuje u određenoj usluzi u računalnom oblaku. Učinkovitost uvelike ovisi o određenom alatu, usluzi u oblaku i načinu na koji je CASB integriran u praćenje (*eng. monitoring).* Neki CASB alati također mogu usmjeriti promet na

namjenske DLP platforme za robusniju analizu nego što je obično dostupna kada CASB sadrži DLP funkcionalnost. Pružatelj usluga može ponuditi DLP mogućnosti kao sastavni dio servisa, poput pohrane datoteka u računalnom oblaku i platformi za suradnju koja skenira učitane datoteke i primjenjuje odgovarajuća sigurnosna pravila. Postoje i tehnike kao što su maskiranje podatka i generiranje testnih podataka, to su tehnike za zaštitu podataka koji se koriste u razvojnim i testnim okruženjima ili za ograničavanje pristupa podacima u aplikacijama u stvarnom vremenu. Generiranje testnih podataka je stvaranje baze podataka s neosjetljivim testnim podacima na temelju "prave" baze podataka. Pri tome može koristiti šifriranje i druge tehnike nasumičnog odabira za stvaranje skupa podataka koji veličinom i strukturom sliči izvoru, ali ne sadrži osjetljive podatke. Dinamičko maskiranje prepisuje podatke u hodu, obično koristeći posrednički (*eng. proxy*) mehanizam, kako bi se maskirali svi ili dio podataka isporučenih korisniku. Obično se koristi za zaštitu nekih osjetljivih podataka u aplikacijama, na primjer za maskiranje svih znamenki osim zadnjih znamenki broja kreditne kartice prilikom prikazivanja korisniku [5].

4.3. Identitet, ovlaštenja i upravljanje pristupom

Identitet, ovlaštenja i upravljanje pristupom (IAM - *eng. identity, entitlement and access management*) su pod velikim utjecajem računalstva u oblaku. U javnom i privatnom računalnom oblaku, dvije strane moraju upravljati IAM-om bez ugrožavanja sigurnosti. Računalstvo u oblaku uvodi višestruke promjene u način na koji se tradicionalno upravljalo IAM-om kod internih sustava. Ključna razlika je odnos između pružatelja usluga i korisnika usluga, čak i u privatnom računalnom oblaku. IAM-om ne može upravljati samo jedan akter i stoga je potreban odnos povjerenja između aktera, određivanje odgovornosti i tehničke izvedbe koje će to omogućiti. Često ta struktura poprimi oblik nalik nekakvom savezu (federaciji), jer većina organizacija ima velik broj (ponekad i stotine) različitih pružatelja usluga na koje trebaju proširiti svoj IAM. U suštini IAM je oblik mapiranja entiteta (osobe, sustava, dijela koda itd.) prema dokazivom (provjerljivom) identitetu povezanom s različitim atributima (koji se mogu mijenjati na temelju trenutnih okolnosti), a zatim donošenje odluke na temelju ovlaštenja identiteta o tome što taj entitet/identitet može učiniti, a što ne može. Čak i kada se kontrolira cijeli lanac tog procesa, upravljanje njime u različitim sustavima i tehnologijama na siguran i provjerljiv/dokaziv način je veliki izazov. U računalstvu u oblaku je temeljni problem što više organizacija upravlja identitetom i pristupom resursima, to može uvelike zakomplicirati proces. Na primjer, ako se pretpostavi da se istog korisnika morate stvoriti/registrirati na desecima ili

stotinama različitih usluga u računalnom oblaku. Primarni alat koji se koristi za upravljanje ovim problemom, izgradnjom odnosa povjerenja između organizacija i njihovim provođenjem kroz tehnologije temeljene na standardima se zove federacija (*eng. federation*) [5]. Konzultantska tvrtka Gartner definira IAM kao "sigurnosnu disciplinu koja omogućuje točno određenim (pravim) pojedincima pristup točno određenim resursima u pravo vrijeme iz pravih razloga [5]." CSA je definirao pojmove koji su najrelevantniji za IAM u računalstvu u oblaku [5]:

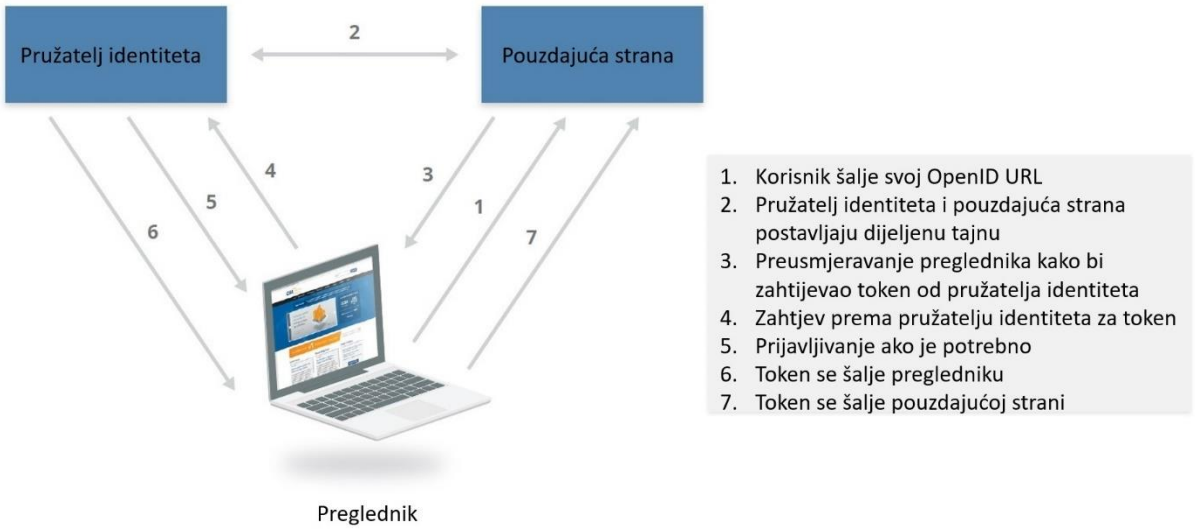
- Entitet (*eng. entity*): osoba ili "stvar" koja će imati identitet. To može biti pojedinac, sustav, uređaj ili aplikacijski kod.
- Identitet (*eng. identity*): jedinstveni izražaj entiteta unutar zadanog područje polja imena (*eng. namespace*). Entitet može imati više digitalnih identiteta, kao što pojedinac ima radni identitet (ili čak više identiteta, ovisno o sustavima), identitet na društvenim mrežama i osobni identitet.
- Identifikator (*eng. identifier*): sredstvo kojim se može potvrditi identitet. Za digitalne identitete ovo je često kripto token. U stvarnom svijetu to može biti putovnica.
- Atributi (*eng. attributes*): aspekti identiteta. Atributi mogu biti relativno statični (poput organizacijske jedinice) ili vrlo dinamični (IP adresa, uređaj koji se koristi ako je korisnik autentificiran pomoću MFA tj. *eng. Multi-factor Authentication,* lokacija itd.)
- Persona (*eng. persona*): izražaj identiteta s atributima koji označavaju/ukazuju kontekst. Na primjer, programer koji se prijavljuje na posao, a zatim se povezuje s okruženjem u oblaku kao developer na određenom projektu. Identitet je još uvijek pojedinac, a persona je pojedinac u kontekstu tog projekta.
- Uloga (*eng. role*): identiteti mogu imati više uloga koje označavaju kontekst. "Uloga" je zbunjujući izraz koji se koristi na mnogo različitih načina. U literaturi [5] uloga se smatra slično personi ili podskupu persone. Na primjer, određeni/specifični developer na određenom/specifičnom projektu može imati različite uloge, kao što su "super-administrator" i "developer", koje se zatim koriste za donošenje odluka o pristupu.
- Autentifikacija (*eng. authentication*): proces potvrde identiteta. Kada se prijavite u sustav, predstavljate korisničko ime (identifikator) i lozinku (atribut koji nazivamo čimbenikom provjere autentičnosti). Koristi se i izraz *eng. Authn*.
- MFA – multifaktorska autentifikacija (*eng. Multi-factor Authentication*): korištenje više faktora u autentifikaciji. Uobičajene opcije uključuju jednokratne zaporke generirane fizičkim ili virtualnim uređajem/tokenom (OTP – *eng. one-time password*), izvanpojasnu provjeru valjanosti putem OTP-a poslanog putem tekstualne poruke ili potvrdu s mobilnog uređaja, biometrijske podatke ili tokena kao programskog dodatka (*eng. plug-in*).
- Kontrola pristupa (*eng. access control*): ograničavanje pristupa resursu. Kontrola pristupa je proces upravljanja pristupom resursima.
- Autorizacija (*eng. authorization*): dopuštanje identitetu pristup nečemu (npr. podacima ili funkciji). Koristi se i izraz *eng. Authz*.

- Ovlaštenje (*eng. entitlement*): preslikavanje/mapiranje identiteta (uključujući uloge, osobe i atribute) u autorizaciju. Ovlaštenje je ono što je nekome dopušteno učiniti, a u svrhu dokumentiranja se vode zapisi u matrici ovlaštenja.
- Federirano (povezano) upravljanje identitetima (*eng. federated identity management*): proces potvrđivanja identiteta u različitim sustavima ili organizacijama. Ovo je ključni pokretač jedinstvene prijave, a također i srž upravljanja IAM-om u računalstvu u oblaku.
- Autoritativni izvor (*eng. authoritative source*): temeljni izvor identiteta, kao što je imenički poslužitelj (*eng. directory server*) koji upravlja identitetima zaposlenika.
- Pružatelj identiteta (*eng. identity provider*): izvor identiteta u federaciji. Pružatelj identiteta nije uvijek autoritativni izvor, ali ponekad se može osloniti na autoritativni izvor, posebno ako je on posrednik tom u procesu.
- Pouzdajuća strana (*eng. relying party*): sustav koji se oslanja na tvrdnju o identitetu od pružatelja identiteta.

Postoji podosta standarda za upravljanje identitetom i pristupom, a mnogi od njih mogu se koristiti i u računalstvu u oblaku. Unatoč širokom rasponu opcija, industrija se odlučila na osnovni skup koji se najčešće viđa u različitim implementacijama i podržava ih većina pružatelja usluga [5]. Sljedeći standardi se mogu koristiti za IAM u računalstvu u oblaku [5]:

- SAML 2.0 *(Eng. Security Assertion Markup Language 2.0)*
- OAuth
- OpenID
- XACML *(Eng. eXtensible Access Control Markup Language)*
- SCIM *(Eng. System for Cross-domain Identity Management)*

Kako funkcionira federirano upravljanje identitetima: Federacija uključuje pružatelja identiteta koji daje tvrdnje pouzdajućoj strani nakon izgradnje odnosa povjerenja. U srži je niz kriptografskih operacija za izgradnju odnosa povjerenja i razmjenu vjerodajnica (*eng. credentials*). Praktičan primjer je korisnik koji se prijavljuje na svoju radnu mrežu, koja hostira imenički poslužitelj za korisničke račune. Taj korisnik zatim otvara vezu na SaaS aplikaciju uz pomoć web preglednika. Umjesto prijave, postoji niz operacija iza kulisa, gdje pružatelj identiteta (interni imenički poslužitelj) potvrđuje identitet korisnika i potvrđuje da je korisnik autentificiran, kao i sve njegove atribute. Pouzdajuća strana vjeruje tim tvrdnjama i prijavljuje korisnika bez da korisnik ponovo unosi vjerodajnice. Zapravo, pouzdajuća strana nema čak ni korisničko ime ili lozinku za tog korisnika, oslanja se na pružatelja identiteta da potvrdi uspješnu autentifikaciju. Korisnik jednostavno ode na web stranicu za SaaS aplikaciju i prijavljen je, pod pretpostavkom da je uspješno autentificiran u internom imeniku [5].



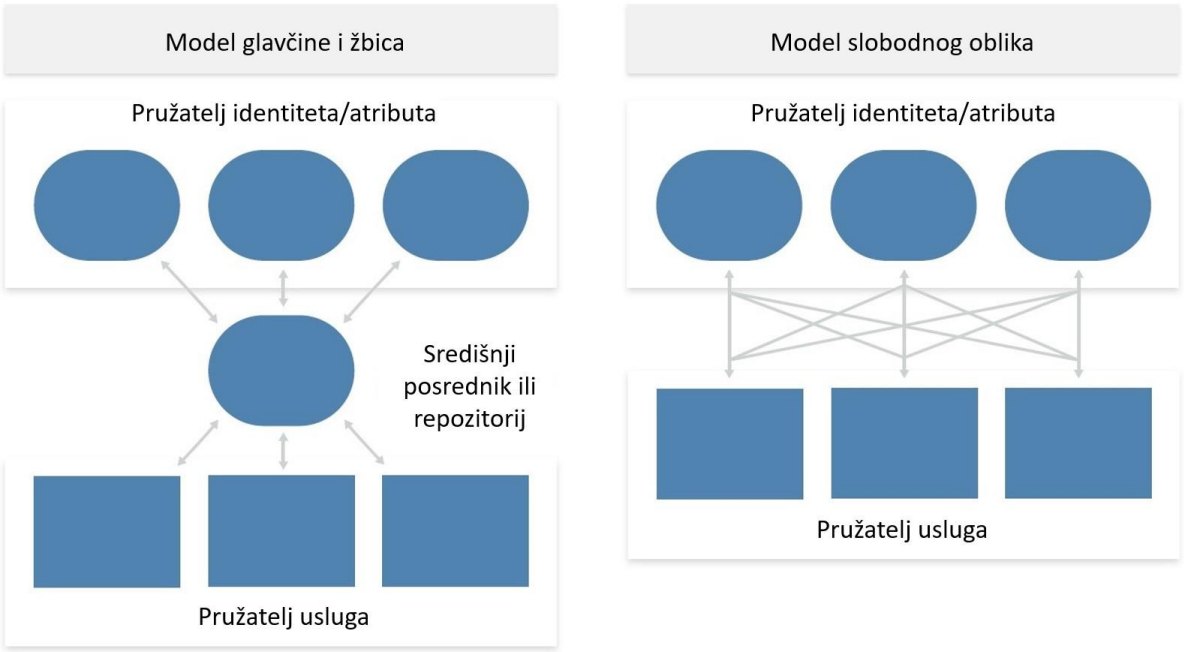
Slika 20. Federirano upravljanje identitetima [5]

Kod upravljanja identitetima pružatelji usluga i korisnici usluga započinju s temeljnom odlukom o tome kako upravljati identitetima:

- Pružatelji usluga moraju gotovo uvijek podržavati interne identitete, identifikatore i atribute za korisnike koji izravno pristupaju uslugama, dok također podržavaju federiranje kako organizacije ne bi morale ručno dodavati i upravljati svakim korisnikom u sustavu pružatelja usluga i svakome izdavati zasebne vjerodajnice.
- Korisnici usluga trebaju odlučiti gdje žele upravljati svojim identitetima i koje arhitekturne modele i tehnologije žele podržati za integraciju s pružateljima usluga.

Korisnik usluga se može prijaviti na računalni oblak pružatelja usluga i kreirati sve svoje identitete u sustavu pružatelja usluga. To nije najbolje rješenje za većinu organizacija, primarno zbog veličine organizacija, zbog toga se većina organizacija okreće federaciji kao rješenju. Postoje i iznimke u kojima je uputno držati neke identitete izoliranima, a to bi bili rezervni administratorski računi koji se koriste za otklanjanje problema. Kada koristi federiranje, korisnik usluga treba odrediti autoritativni izvor koji drži jedinstvene identitete koje će federirati. Ovo je često interni imenički poslužitelj. Sljedeći korak bi bila odluka hoće li se izravno koristiti autoritativni izvor kao pružatelj identiteta ili koristiti neki drugi izvor identiteta koji preuzima podatke iz autoritativnog izvora ili integrirati brokera identiteta [5]. Postoje dvije mogućnosti, koje su prikazane i na slici 21. [5]:

- Model glavčine i žbica: pružatelji/izvori internih identiteta komuniciraju sa središnjim posrednikom ili repozitorijem koji zatim služi kao pružatelj identiteta za federaciju s pružateljima usluga.
- Model slobodnog oblika: unutarnji pružatelji/izvori identiteta (često imenički poslužitelji) povezuju se izravno s pružateljima usluga.



Slika 21. Modeli federacije

Nakon određivanja modela, još uvijek postoje procesne i arhitekturne odluke potrebne za bilo kakvu implementaciju [5]:

- Kako upravljati identitetima za aplikacijski kod, sustave, uređaje i druge usluge.
- Definiranje procesa pružanja identiteta i kako to integrirati u implementacije oblaka.
- Provizioniranje (*eng. provisioning*) i podržavanje pojedinačnih pružatelja usluga. Trebao bi postojati definirani postupak za dodavanje novih pružatelja usluga u IAM infrastrukturu.
- Implementacija procesa deprovizije (*eng. deprovisioning*) ili promjene ovlaštenja za identitete i pružatelja usluga. S federacijom to zahtijeva rad s obje strane veze.

Autentifikacija je proces dokazivanja ili potvrđivanja identiteta. U informacijskoj sigurnosti autentifikacija se najčešće odnosi na čin prijave korisnika, ali se također odnosi na bilo koje vrijeme kad entitet dokaže tko je i preuzme identitet. Autentifikacija je odgovornost davatelja identiteta. Najveći utjecaj računalstva u oblaku na autentifikaciju je veća potreba za snažnom autentifikaciju pomoću više čimbenika (MFA) [5]. To je iz dva razloga [5]:

- Vrlo visoki kapacitet pristupa mreži znači da se uslugama u računalnom oblaku uvijek pristupa preko mreže, a često i preko interneta. Gubitak vjerodajnica mogao bi lakše dovesti do preuzimanja računa od strane napadača, jer napadi nisu ograničeni na lokalnu mrežu.
- Veća upotreba federacije za jedinstvenu prijavu (*eng. Single Sign On - SSO*) znači da jedan skup vjerodajnica može potencijalno ugroziti veći broj usluga u oblaku.

MFA je jedna od najjačih opcija za smanjenje rizika preuzimanja računa. To nije lijek za sve, ali oslanjanje na jedan faktor (lozinku) za usluge u računalnom oblaku je vrlo rizično. Kada se

koristi MFA zajedno sa federacijom, pružatelj identiteta može proslijediti i MFA status kao atribut pouzdajućoj strani [5]. Postoji više opcija za MFA [5]:

- Hardverski tokeni (*eng. hard token*). To su fizički uređaji koji generiraju jednokratne lozinke.
- Softverski tokeni (*eng. soft token*). To su tokeni koji rade slično kao hardverski tokeni, ali su to softverske aplikacije koje se pokreću na telefonu ili računalu.
- Izvanpojasne lozinke (*eng. out-of-band passwords*). To su tekstualne ili druge poruke koje se šalju obično na korisnikov telefon i zatim se unose kao bilo koja druga jednokratna lozinka koju generira token.
- Biometrija. Ona postaje sve veća opcija zahvaljujući biometrijskim čitačima koji su sada dostupni i na mobilnim telefonima.

4.4. Opća sigurnosna pitanja vezana za korištenje ERP aplikacija u računalnom oblaku

Sigurnost u računalnom oblaku jedna je od najvećih briga koja je spriječila organizacije da masovno usvoje ERP (*eng. Enterprise Resource Planning*) aplikacije na računalnom oblaku. Uzimajući u obzir osjetljivost poslovne aplikacije kao što je ERP, treba pomno razmotriti neka pitanja oko prelaska na računalni oblak. Rezidencija podataka je jedno od tih pitanja, jer najvažnija "imovina" ERP aplikacije su podaci koje ona sadrži, a ti podaci često podliježu mnogim propisima. Većina dobavljača ERP sustava u računalnom oblaku omogućit će kupcu da odabere podatkovni centar, a time i geografsku lokaciju svojih podataka. Zbog Europske opće uredbe od zaštiti podataka (*eng. European General Data Protection Regulations* – GDPR) postoje ograničenja i razmatranja koja se moraju uzeti u obzir u vezi s privatnošću osobnih podataka, kontrolama koje se koriste te gdje se ti podaci nalaze. Usklađenost s ovim propisima može nametnuti neka ograničenja za fleksibilnost korisnika. Drugi propisi, poput Uredbe o međunarodnom prometu oružjem (ITAR), također mogu nalagati gdje će se podaci nalaziti, kao i državljanstvo ljudi koji njima upravljaju [7].

Provizioniranje korisnika, autentifikacija, autorizacija i jedinstvena prijava (SSO) je sljedeće pitanje koje se mora razmotriti. ERP aplikacije obično imaju vlastita rješenja za upravljanje identitetom, kao i višestruke opcije za SSO. Postoje različiti načini pružanja SSO opcija, ali jedan od najčešće korištenih standarda je standard SAML. Standard SAML omogućuje autentifikaciju s jedinstvenom prijavom (SSO) između pružatelja identiteta i više aplikacija putem upotrebe digitalno potpisanih XML dokumenata. Pružatelj identiteta može biti interni servis koji je proširen za pružanje autentifikacije i autorizacije rješenjima u računalnom oblaku. Ovu opciju obično koriste organizacije koje koriste postojeće interne pružatelje identiteta. Na primjer, ako organizacija već koristi imenički direktorij (*eng. Active*

Directory), to se može proširiti za autentifikaciju i autorizaciju u oblaku korištenjem federiranih servisa imeničkog direktorija (*eng. Active Directory Federation Services* - ADFS). Alternativno, organizacija može koristiti treću stranu kao pružatelja identiteta kako bi ona isporučila SSO usluge u računalnom oblaku. Kada se koriste treće strane kao pružatelji identiteta važno je utvrditi podržava li ERP aplikacija u računalnom oblaku različite SSO protokole koje koriste te treće strane. Ako organizacije odluče ne koristiti rješenje za upravljanje identitetom, većina ERP rješenja u računalnom oblaku već dopušta provizioniranje, upravljanje korisnicima i autorizacijama kao standardnu funkcionalnost [7].

Praćenje korisničke aktivnosti i praćenje pristupa osigurava vidljivost oko toga što korisnici rade u bilo kojem trenutku te otkrivanje zlonamjernog i nepravilnog ponašanja korisnika. Ovo je važno jer svakodnevno funkcioniranje velikih organizacija zahtijeva da zaposlenici različitih razina povjerenja i uloga imaju pristup ERP rješenjima i drugim poslovno kritičnim aplikacijama, kao i vrlo osjetljivim podacima koji se nalaze u njima. Takav pristup i naknadnu korisničku aktivnost treba nadzirati kako bi se osiguralo da se ne događa zlonamjerna aktivnost. Različiti modeli usluga u oblaku (IaaS naspram SaaS) vjerojatno će zahtijevati prilagođena rješenja, ali konceptualno su potrebe iste za oba. Revizijske zapise (*eng. audit trails*)obično osigurava dobavljač aplikacije ili, ako ne, dobivaju se iz drugih izvora kao što je pružatelj identiteta ili CASB [7].

Upravljanje sigurnosnim ranjivostima (*eng. Security Vulnerabilities Management*) je isto jedna od tema koja se treba detaljno analizirati. Kada koriste SaaS ERP rješenja, organizacije prebacuju kontrolu i odgovornost na pružatelja SaaS usluga koji upravlja instalacijom zakrpa (*eng. patching*) i dostupnošću sustava za kupca/organizaciju. Organizacije će se možda trebati složiti s određenim razdobljima održavanja u kojima se može obaviti instalacija zakrpa ako upravljaju promjenama (*eng. change management*). Instalacija zakrpa će također osigurati da su sve nove značajke budu kompatibilne s podacima i tijekom rada (*eng. workflow*) organizacije. Nerazumijevanje važnosti ovih koraka može dovesti do gubitka usluge, oštećenja podataka ili nedostupnosti sustava. Prebacivanje odgovornosti na pružatelja SaaS usluga omogućuje veću fleksibilnost i dostupnost sustava. Iako je odgovornost pružatelja SaaS-a osigurati da njegovi proizvodi i usluge nemaju ranjivosti, organizacije moraju paziti da pružatelj stvarno upravlja ovim područjem [7].

Mogućnosti planiranja oporavka od katastrofe (*eng. Disaster Recovery Planning* - DRP) mogu se smatrati jednom od izravnih prednosti prebacivanja poslovnih aplikacija u računalni oblak. Bilo IaaS ili SaaS, pružatelj usluga u računalnom oblaku može se prebaciti na druge podatkovne centre diljem svijeta u slučaju većeg poremećaja. Tehnologija virtualizacije

dramatično je povećala učinkovitost računalstva u oblaku, čineći probleme s DRP-om lakše rješivima, a povećavajući operativnu učinkovitost. Postoje mnoge prednosti koje se mogu pronaći u DRP-u temeljenom na računalnom oblaku. Okruženja u oblaku značajno su olakšala proces praćenja i provjere spremnosti za slučaj katastrofe na nadogradiv/skalabilan način.
Provjera i potvrđivanje statusa sukladnosti ERP dobavljača s različitim standardima može biti izazovno. Mnogi od njih daju popise okvira (*eng. frameworks*) kojih se pridržavaju, kao i standarda revizije i atesta kojih se pridržavaju. Kao preventivnu mjeru, organizacije se potiču da postupaju s dužnom pažnjom i provjere standarde dobavljača ERP-a. Mnogi pružatelji SaaS usluga hostiraju svoje proizvode na IaaS infrastrukturi treće strane. U tim slučajevima pružatelj SaaS usluga možda neće imati uvid u to kako se tom infrastrukturom upravlja i instaliraju zakrpe. Međutim, pružatelj SaaS usluga može zatražiti pružatelja IaaS usluga atest/potvrdu (npr. ISO27000 ili ISAE3402) prema ekvivalentu vlastitih standarda [7].

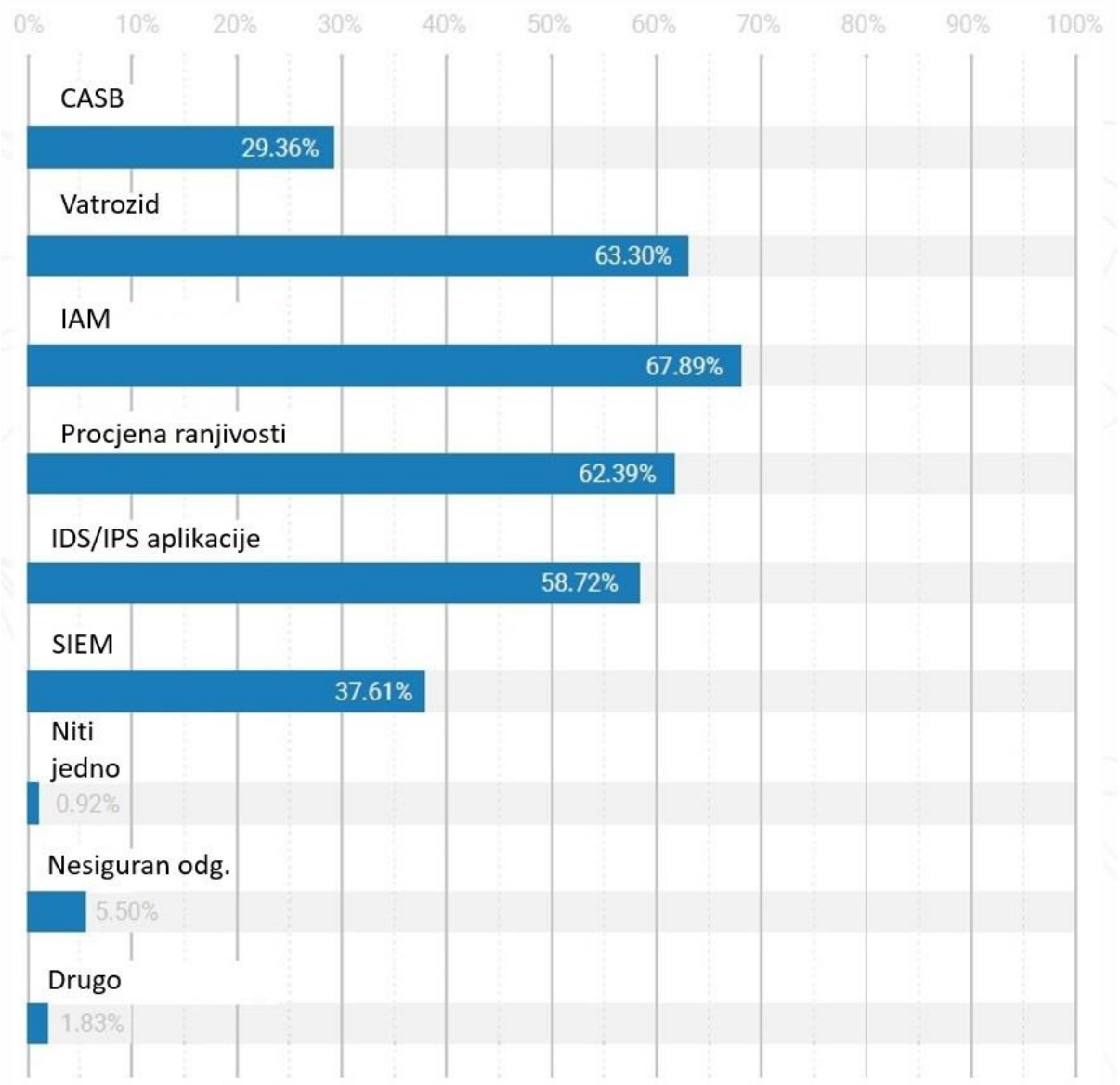
Zbog prirode ERP aplikacija, organizacije moraju biti spremne na kompromitirajući incident. Priprema počinje s planom odgovora na incidente (*eng. Incident Response - IR*), ali isto tako organizacije moraju biti u mogućnosti osigurati točne podatke u odgovarajućem vremenu od pružatelja usluga kada se incident dogodi. Uspostava mogućnosti za preuzimanje zapisa i tragova do pružatelja usluga (posebno kada je to potrebno za istragu) najvažnija je i najteža komponenta izgradnje odgovarajućeg IR plana. Ovaj bi proces trebao biti istaknut u ugovoru s pružateljem usluga [7].

Današnje aplikacije sve su više međusobno povezane. Internet opcija se prioritizira kako bi se pružila izravna usluga i stalna dostupnost kako organizacijama tako i njihovim klijentima. Stoga su aplikacije postale primarna površina za napad. ERP aplikacije u računalnom oblaku (SaaS) obično su izložene kao web aplikacije, dostupne su putem web preglednika ili mobilne aplikacije s bilo kojeg mjesta. Iako postoji mnogo aplikacija različitih funkcija i namjena, one su, sa sigurnosne točke gledišta, obično iste ili slične prirode. Dizajn softvera, implementacija i integracija sigurnosnih kontrola ostaju slični [7]. U SaaS okruženjima korisnici usluga bi trebali razmotriti pružaju li pružatelji usluga informacije i rješenja za rješavanje ključnih komponenti, kao što su [7]:

- Pohranjivanje osjetljivih podataka, uključujući upravljanje ključevima.
- Iskorištavanje sigurnosnog mehanizma programskog sučelja aplikacija (API).
- Validacija ulaza/izlaza.
- Sigurnosna revizija i bilježenje zapisa (*eng. logging*).
- Stvrdnjavanje na strani poslužitelja itd.
- Odgovarajuće razdvajanje "stanara" i infrastrukture

Organizacije koje traže transparentnost kod korištenja ERP-a u računalnom oblaku trebale bi razmotriti korištenje CASB-a, gdje su definirana pravila i uvjeti za kontrolu pristupa podacima, pristupa sustavu, sprječavanje curenja podataka, tokenizaciju, multifaktorsku autentifikaciju (MFA) i enkripciju. CASB se mogu implementirati interno ili kao usluga u računalnom oblaku. U skladu s tim, rizike takvih implementacija potrebno je razmotriti prije implementacije u usluge računalnog oblaka. CASB rješenja mogu izvršiti analizu ponašanja korisnika kako bi se identificiralo neuobičajeno ponašanje i poduzeli reaktivni koraci koji mogu blokirati korisnički pristup i/ili pristup značajki usluge. Alternativa je integracija opcija zapisivanja u CASB s postojećim upravljanjem sigurnosnim informacijama i događajima (*eng. Security Information and Event Management* - SIEM). Iako je SIEM dobar izbor za bilježenje događaja i revizija, na kraju je na organizacijama da odluče jesu li opcije bilježenja dostupne u CASB-u dovoljne same ili ih treba integrirati sa SIEM rješenjem [7].

Najčešća sigurnosna rješenja koja se koriste za ERP u računalnom oblaku su upravljanje identitetom i pristupom (IAM) (68%), vatrozidi (*eng. firewalls*)(63%), procjene ranjivosti (62%) i IDS/IPS aplikacije (*eng. Intrusion Detection Systems i eng. Intrusion Prevention Systems*) (59%), SIEM (38%) te CASB (29%). Većina (84%) pružatelja SaaS ERP-a također nudi događaje (*eng. events*), zapise (*eng. logs*) i aktivnosti (*eng. activity*) korisnika za pregled. Regionalno, CASB rješenja mnogo su češća u Sjevernoj i Južnoj Americi (42%) i manje popularan u regijama APAC (19%) i EMEA (11%) [8]. Slika 22. prikazuje koja sva sigurnosna rješenja organizacije koriste kako bi zaštitile usluge u računalnom oblaku.



Slika 22. Najčešće korištena sigurnosna rješenja [8]

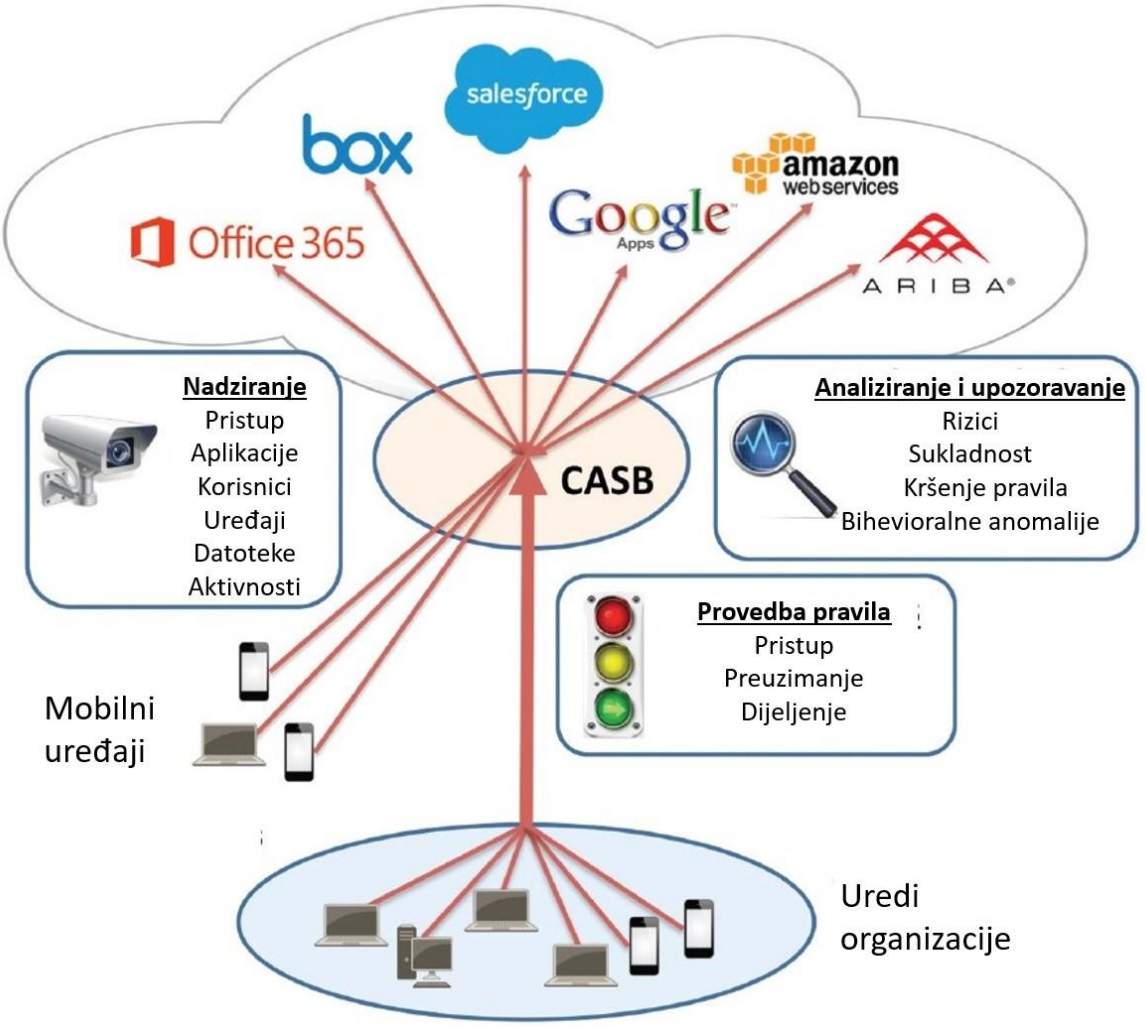
5. CLOUD ACCESS SECURITY BROKER - CASB

Pri korištenju SaaS usluga postoje izazovi kao što su upravljanje aplikacijama (pružatelj usluga upravlja aplikacijom, a ne vlastita organizacija), mobilni uređaji koje ne kontrolira organizacija i krajnji korisnici koji dijele podatke preko veze (linka). Također model podijeljene odgovornosti nalaže da korištenjem SaaS usluga organizacija ne može kompletno upravljanje sigurnošću prebaciti na pružatelja usluga [9]. Organizacija (korisnik usluga) još uvijek je odgovorna za [9]:

- Zaštita korisničkih vjerodajnica i pristupa aplikacijama u računalnom oblaku.
- Odlučivanje koji su podaci osjetljivi te provođenje pravila za pristup i dijeljenje podataka.
- Praćenje događaja i ponašanja radi otkrivanja zlonamjernih aktivnosti.
- Dokumentiranje sukladnosti s propisima i industrijskim standardima.

Kada se aplikacije nalaze u podatkovnim centrima organizacije, one mogu pratiti sve događaje i radnje povezane s pristupom i aktivnostima u aplikacijama. Ali za aplikacije smještene u računalnom oblaku, organizacije imaju samo onoliko vidljivosti koliko su pružatelji usluga spremni pružiti. Osim toga, svaki pružatelj usluga ima vlastite mehanizme za autentifikaciju i kontrolu pristupa, vlastite mogućnosti praćenja aktivnosti, vlastiti sustav upozorenja i vlastite revizijske tragove. Rezultat toga je da organizacije često ne mogu otkriti nepoštivanje propisa ili indikatore potencijalnih napada. Čak i kada se otkriju napadi, zahtjevno je povezivanje indikatora prijetnji i sigurnosnih podataka iz više aplikacija. Uređaji kojima ne upravlja organizacija te uređaji koji ne ispunjavaju zahtjeve sukladnosti su također izazov. Višestruko zahtjevnije je i nadziranje pristupa podacima. Odluke o dijeljenju informacija je u tradicionalnom modelu računalstva donosilo IT osoblje, u računalstvu u oblaku su te odluke ustupljene korisnicima i administratorima. Takvi korisnici su meta za kriminalce i hakere, jer je lakše uzeti podatke za pristup i podatke od ovih korisnika nego napasti pružatelja usluga. Uvijek je optimalna meta najslabija karika i tom smjeru se onda provode phishing napadi kako bi se ukrali podaci za pristup ili se pokušava kompromitirati kućno računalo korisnika, u slučajs kada se korisnik prijavi na usluge računalstva u oblaku s kućnog računala [9].

U literaturi [9] definicija za CASB jest: Platforma koja pruža vidljivost u aplikacijama u računalnom oblaku, nadzire pristup i korištenje više aplikacija temeljenih na računalstvu u oblaku, t provodi pravila za kontrolu pristupa, zaštitu podataka i sukladnost. Na slici 23. je prikazan koncept CASB-a



Slika 23. Konceptualni pogled na CASB [9]

Jedna od primarnih funkcija CASB-a, je praćenje pristupa svih korisnika, sa svih upravljanih i neupravljanih uređaja, svim aplikacijama u oblaku [9]. CASB prikuplja podatke koji se odnose na [9]:

- Aplikacije u računalnom oblaku.
- Korisnike koji pristupaju aplikacijama.
- Uređaje koji se koriste za pristup aplikacijama.
- Datoteke i podatke koji se stvaraju i pohranjuju u aplikacije.
- Aktivnosti vezane uz pristup aplikacijama i datotekama (npr. prijave i trajanje sesije).

Međutim CASB je više od pasivnog alata za praćenje. CASB može korelirati i analizirati podatke koje prikuplja kako bi se: identificirale ranjivosti i rizici, otkrilo neuobičajeno ponašanje koje ukazuje na napade, te kako bi se demonstriralo provođenje pravila i propisa. Također CASB može ojačati zaštitu od prijetnji i odgovor na incidente generiranjem upozorenja kada se otkrije rizike, kršenja pravila i neuobičajeno ponašanje. CASB može biti i platforma za provođenje korporativnih i regulatornih politika kako bi se: kontrolirao pristup

aplikacijama i datotekama te kontroliralo kada i kako se datoteke i podaci dijele ili preuzimaju [9]. Mogućnosti CASB-ova mogu se grupirati u četiri kategorije [9]:

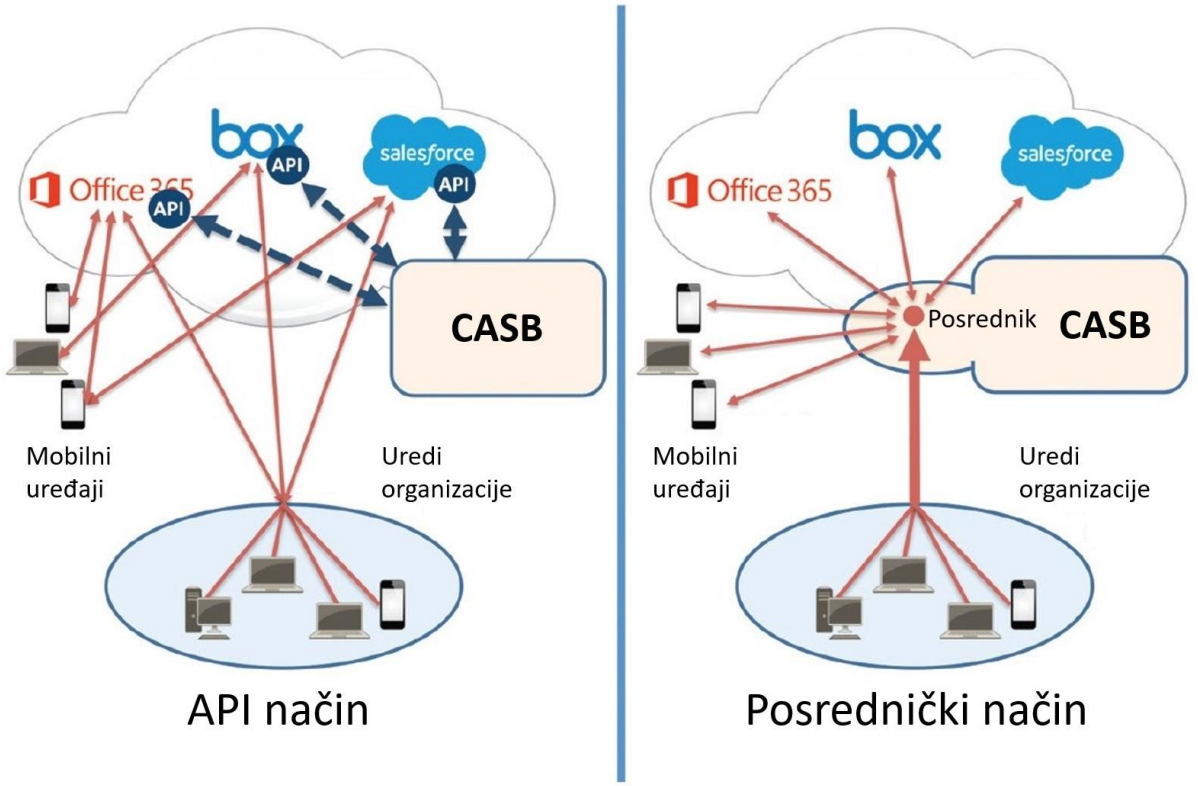
- Vidljivost.
- Zaštita od prijetnji.
- Kontrola pristupa.
- Sukladnost.

CASB-ovi mogu pružiti vrlo detaljne podatke o tome koje se aplikacije u računalnom oblaku koriste u poduzeću, tko im pristupa i kako im se pristupa (s kojih uređaja, kada i gdje). Također mogu pokazati koje se datoteke pohranjuju, tko ih posjeduje i kako im se pristupa i dijeli unutar i izvan organizacije. Ti se podaci mogu korelirati i analizirati kako bi se tvrtkama pomoglo u praćenju ponašanja korisnika, procjeni rizika, upravljanju politikama i poboljšanju sigurnosnih praksi. Zaštita od prijetnji je područje u kojem CASB-ovi pružaju usluge koje nisu dostupne iz nekog drugog izvora. CASB može nadzirati aktivnosti korisnika u više aplikacija u računalnom oblaku i na više uređaja te koristiti te podatke za stvaranje profila normalnog ponašanja. Na temelju tih informacija CASB može generirati upozorenja kada otkrije odstupanja od osnovnih vrijednosti. Velike količine podataka o aplikacijama, korisnicima, uređajima, datotekama i aktivnostima koje CASB-ovi prikupljaju također mogu biti iznimno vrijedni timovima za odgovor na incidente (IR), forenziku i upravljanje rizikom koji pokušavaju rekonstruirati napredne, višestupanjske napade, te odrediti taktike, tehnike i procedure napadača. U računalstvu u oblaku, organizacija će možda htjeti detaljnije razraditi odluke o pristupu. Kroz "adaptivnu kontrolu pristupa", CASB omogućuje stvaranje detaljnih pravila pristupa s više faktora i njihovo dosljedno provođenje u nizu aplikacija u računalnom oblaku. CASB-ovi osiguravaju revizijske zapise kako bi organizacije mogle pokazati da su aktivnosti aplikacije, pristup i dijeljenje datoteka u skladu s korporativnim politikama i industrijskim standardima. Također se mogu koristiti za provođenje zahtjeva sukladnosti i zaštitu podataka pomoću tehnologija kao što su: sprječavanje gubitka podataka (DLP, za prepoznavanje i blokiranje preuzimanja i dijeljenja datoteka koje sadrže osjetljive podatke poput intelektualnog vlasništva i podataka koji su povezani sa identitetom osobe tj. PII), enkripcija (kako bi se osiguralo da su datoteke enkriptirane prije nego što se učitaju ili preuzmu s računalnog oblaka), upravljanje pravima na informacije (*eng. Information rights management* - IRM), kako bi se spriječilo kopiranje, ispis ili drugačija distribucija osjetljivog sadržaja u dokumentima. CASB može pomoći u primjeni sofisticiranih pravila zaštite podataka, na primjer, provođenje enkripcije datoteka preuzetih na neupravljane uređaje ili blokiranje dijeljenja datoteka s uređajima koji se prijavljuju iz sumnjivih geografskih regija. Uvođenje CASB-a ne znači dodavanje novog sloja

tehnologije koji duplicira trenutna sigurnosna rješenja. Umjesto toga, CASB može proširiti postojeće sigurnosne alate i politike u računalni oblak. Na primjer, neki CASB-ovi mogu: upravljati pristupom aplikacijama u računalnom oblaku na temelju informacija sadržanih u imenicima poduzeća (eng. *enterprise directories*), korisničkim grupama i ulogama; proširiti postojeća DLP rješenja i rješenja za enkripciju kako bi zaštitili datoteke koje se preuzimaju iz aplikacija u računalnom oblaku; dijeliti podatke sa SIEM sustavima o pristupu aplikacijama, kršenjima pravila i sigurnosnim incidentima izvan korporativne mreže [9].

5.1. Implementacija CASB-a

Funkcionalnost CASB-ova ovisi o implementaciji te integraciji s ostalim aplikacijama. Neki CASB-ovi se integriraju s aplikacijama u računalnom oblaku putem API-ja. Preko API-ja CASB može dobiti informacije o korisnicima aplikacije, datotekama pohranjenim u aplikaciji, dopuštenjima i postavkama dijeljenja tih datoteka te aktivnostima kao što su prijave i odjave, izmjene, brisanja, prijenosi i preuzimanja datoteka, administrativne radnje i transakcije [9]. Postoje dvije opcije implementacije CASB-a: API način i posrednički način [9]. Oba načina su prikazana na slici 24.



Slika 24. Načini implementacije CASB-a [9]

CASB postavljen u API modu je "izvan pojasa" tj. mrežni promet između korisnika i aplikacija ne teče kroz CASB, korisnici izravno komuniciraju s aplikacijama u računalnom oblaku, a CASB dobiva podatke iz aplikacija putem njihovih API-ja. Ovaj pristup pruža vrlo detaljnu vidljivost podataka i aktivnosti korisnika, uključujući prijave i odjave, učitavanje i preuzimanje datoteka, dijeljenje informacija i administrativne radnje. CASB-ovi implementirani preko API-ja mogu obavljati administrativne zadatke i provoditi politike upravljanja. Na primjer, ako korisnik prekrši pravila javnim dijeljenjem datoteka koje sadrže osjetljive podatke, administratori mogu upotrijebiti CASB za promjenu dopuštenja pristupa datotekama ili za oduzimanje vlasništva nad datotekama korisniku koji je napravio prekršaj [9].

CASB implementiran kao posrednik je "u liniji", mrežni promet između korisnika i aplikacija u računalnom oblaku teče kroz CASB posrednika. To se postiže na jedan od dva načina: kod posredničkog poslužitelja (*eng. forward proxy*) mrežni uređaji (za uredske korisnike) ili agenti na svakoj krajnjoj točki (za vanjske korisnike) usmjeravaju promet na CASB posrednika; kod reverznog poslužitelja (*eng. reverse proxy*) aplikacije u računalnom oblaku su konfigurirane za vođenje prometa kroz CASB posrednik. Posrednički način rada omogućuje CASB-ima implementaciju vrlo detaljnih (granularnih) kontrola pristupa. Posrednički način implementacije daje CASB-u uvid u podatke i omogućuje provođenje pravila u stvarnom vremenu. Na primjer, CASB može osigurati da su datoteke koje se učitavaju enkriptirane i može blokirati preuzimanje osjetljivih datoteka na nesukladne uređaje. Također može generirati upozorenja u stvarnom vremenu, što omogućuje sigurnosnim timovima da odmah reagiraju na sigurnosne incidente, kršenja politika/pravila i nepravilna ponašanja. Neki CASB-ovi nude hibridni način rada koji kombinira API i posrednički način implementacije. To omogućuje CASB-u da podrži širok raspon slučajeva upotrebe s vidljivošću, provedbom pravila i načinima rješavanja neupravljanih uređaja [9].

Neke od značajki CASB-ova zahtijevaju integraciju s postojećim sigurnosnim proizvodima, ti proizvodi su [9]:

- Imenici (*eng. directories*) i SSO rješenja.
- DLP.
- NAC (eng. network access control) u računalnom oblaku.
- Izoliranje softvera u pješčaniku (*eng. sandboxing*).
- Enkripcija i IRM.
- SIEM.

No ne nude svi CASB-ovi integraciju sa svim navedenim proizvodima. Većina CASB-ova integrira se s imenicima poduzeća, SSO i drugim rješenjima za upravljanje identitetom i pristupom (IAM). Ove integracije CASB-u daju pristup dodatnim informacijama o

korisnicima, kao što su njihove uloge, odjeli i poslovne jedinice [9]. Oni također mogu pomoći CASB-ima u provedbi korporativnih politika, kao što su [9]:

- Zahtijevanje od korisnika da se autentificiraju u aplikacijama u računalnom oblaku putem SSO rješenja, a ne izravno preko weba.
- Blokiranje pristupa aplikacijama u oblaku čim korisnik promijeni uloge ili bude isključen (deprovizioniran).

DLP značajke u računalnom oblaku omogućuju CASB-u da otkrije osjetljive informacije u datotekama i spriječi preuzimanje tih datoteka na uređaje kojima se ne upravlja. Neki CASB-ovi se integriraju s DLP proizvodima kako bi iskoristili postojeća DLP pravila i klasifikacije datoteka, omogućujući da se jedan skup DLP pravila provede u računalnom oblaku i lokalnim podatkovnim centrima. CASB može raditi s NAC rješenjima u računalnom oblaku od trećih strana. Krajnjim točkama kojima se ne upravlja ili koje nisu u skladu s korporativnim standardima može se blokirati pristup aplikacijama u računalnom oblaku ili im se može dati ograničeni pristup i mogućnost preuzimanja ili dijeljenja datoteka [9]. CASB može raditi s proizvodom za izoliranje softvera u pješčaniku (*eng. Sandboxing*) kako bi testirao datoteke i softverski kod na zlonamjerni softver (*eng. malware*). Integracija CASB-a s enkripcijom i rješenjima za upravljanje pravima na informacije (IRM) može osigurati [9]:

- Da su datoteke prenesene u aplikacije u računalnom oblaku enkriptirane.
- Da su datoteke preuzete na neupravljane i druge nepouzdane krajnje točke enkriptirane.
- Da se osjetljivi sadržaj ne može ispisati, izvesti (eksportirati), kopirati ili dugo zadržati na krajnjim točkama.

Svaki način enkripcije ima svoje prednosti i mane, pa tako još nema konsenzusa u struci koji je općenito najbolji način enkripcije. Moguće opcije su: enkripcija svih podataka, enkripcija podataka na razini polja te enkripcija na razini datoteke. No za CASB-ove, enkripcija na razini datoteke je obično najbolja opcija. Enkripcija i dekripcija svih podataka stvara povećano opterećenje računalnih resursa, a enkripcija podataka na razini polja često ograničava funkcionalnost aplikacija. Na primjer, korištenje rješenja treće strane za enkripciju polja u Salesforce aplikaciji može ometati pretraživanje, kao i poremetiti integraciju s drugim aplikacijama. Sva upozorenja koja generira CASB, zajedno s povezanim informacijama (kontekst za upozorenje), mogu se proslijediti SIEM rješenjima. To omogućuje sigurnosnom operativnom centru (SOC) i timovima za odgovor na incidente (IR) da odmah vide upozorenja koja je izradio CASB, povežu ih s lokalnim aktivnostima, daju im prioritet uz druga upozorenja i odgovore na njih koristeći uspostavljene protokole. Uz navedene prednosti omogućava im i trenutni pristup kontekstualnim informacijama koje je prikupio CASB [9].

5.2. Usporedba CASB-ova

Neke od tvrtki koje nude CASB rješenja su: McAfee (Skyhigh), Netskope, Microsoft, Bitglass, Cisco, Oracle Corporation, Palo Alto Networks, Proofpoint, Symantec i Zscaler [10]. U tablici 2. je prikazana usporedba podržanih načina implementacije za tri CASB rješenja.

Tablica 2. Usporedba podržanih načina implementacije CASB rješenja [10, 11, 12]

Način implementacije	McAfee (Skyhigh)	Netskope	Cisco
API	**X**	**X**	**X**
Posrednički poslužitelj	**X**	**X**	**X**
Reverzni poslužitelj	**X**	**X**	**X**

McAfee (Skyhigh) ima podjelu za SaaS aplikacije koje podržava u 3 grupe: kolaboracijske aplikacije (*eng. collaboration apps*), strukturirane aplikacije (*eng. structured apps*) te aplikacije sa dugim repom (*eng. long-tail apps*) [12]. U te tri kategorije podijeljene su sljedeće aplikacije [12]:

- Kolaboracijske aplikacije: Office 365 (OneDrive, SharePoint, Teams, Exchange Online), G Suite for Business, Box, Slack, Zoom, Dropbox.
- Strukturirane aplikacije: Salesforce, ServiceNow, SuccessFactors, Workday, Microsoft Dynamics 365
- Aplikacije sa dugim repom: Atlassian (Jira, Confluence, Access), GitHub, Smartsheet, Cisco WebEx Teams, DocuSign, Egnyte, OneCollect, Oracle HCM, Zendesk, Citrix ShareFile, Domo, FileCloud, Cloud for Okta, OneLogin, SAP Concur, Wrokplace by Facebook, Clarizen.

U tablici 3. je prikazano s kojim aplikacijama CASB rješenje od tvrtke Netskope podržava integraciju [11].

Tablica 3. Netskope integracija s aplikacijama [11]

	Aplikacije
	ServiceNow
Aplikacije za produktivnost	Microsoft, Google, Box
Pohrana u računalnom oblaku	Microsoft Office 365 OneDrive, Google Drive, Box, Dropbox, Egnyte, Intralinks.
SSO aplikacije	Ping Identity, Centrify, Okta, OneLogin, Microsoft, SecureAuth
Aplikacije za upravljanje mobilnim uređajima/aplikacijama	AirWatch by VMware, Citrix, IBM, Microsoft, MobileIron
Klasifikacija podataka i IRM	Boldon James, Box, Microsoft, TITUS, Vera
Aplikacije za sigurnost i prijetnje	Carbon Black, Cyphort, FireEye, Juniper
Lokalni DLP	McAfee DLP Prevent, Symantec Network Prevent DLP, Forcepoint (Websense) TRITON AP Data
Korporativne aplikacije	Vatrozidovi, posrednici, SIEM itd.
Ostalo	Amazon Web Services, Demisto, Exabeam, Google Cloud Platform, Microsoft Azure, Slack, Salesforce, Splunk, Sumo Logic, Workplace by Facebook

Cisco ima popis pružatelja usluga računalstva u oblaku za koje Duo podržava integraciju. Ti pružatelji usluga su: Adobe Document Cloud, Aha!, AWS, Asana, Atlassian, BambooHR, Barracuda, BlueJeans, Bomgar, Bonusly, Box, Bugsnag, Canvas, Cisco (ASA, Firepower, Umbrella), Clarizen, CloudLock, Confluence SSO, Crashplan, Cyberark, Datadog, Desk, Digicert, DocuSign, Dropbox, Egnyte, Evernote, Expensify, Freshdesk, GitHub, GoTo Apps, Greenhouse, Google Workspace, Hackerone, HackerRank, Heroku, HipChat, Igloo, Intacct, Ivanti, Jamf PRO, JitBit, Jira SSO, Locker, Marketo, Meraki, Microsoft 365, Monday.com, Namely, Netdocuments, NewRelic, Pagerduty, Paloalto Networks, Remedyforce, RingCentral, Robin, Salesforce, Samanage, Saucelabs, ShareFile, Signal Sciences, Slack, Smartsheet, Splunk, StatusPage.io, SugarCRM, Sumologic, Syncplicity, Tableu, Udemy, Uservoice, Webex, Workday, Workplace, Zendesk, Zoom te još i razne generičke pružatelje usluga na SAML standardu [13].

Cisco Secure Access by Duo pruža sljedeća rješenja [13]:

- Multifaktorska autentifikacija (MFA) za brzu potvrdu identiteta.
- Provjera pristupnih uređaja. Može se pratiti zdravlje upravljanih i neupravljanih uređaja.
- Adaptivna pravila pristupa. Mogućnost postavljanja prilagođenih pravila i politika pristupa.
- Udaljeni pristup. Siguran udaljeni pristup bez instaliranog agenta na uređaju.
- Jedinstvena prijava SSO.

Cisco Secure Access by Duo sigurnosna je platforma temeljena na računalstvu u oblaku koja štiti pristup svim aplikacijama, za bilo kojeg korisnika i uređaj, s bilo kojeg mjesta. Duo je dizajniran pruža potpunu vidljivost i kontrolu krajnje točke. Duo provjerava identitete korisnika preko multifaktorske autentifikacije (MFA). Duo ima dubok uvid u uređaje korisnika te pruža mogućnost prilagođavanja pravila i politika za ograničavanje pristupa temeljenih na krajnjim točkama ili rizicima koje predstavlja korisnik, također Duo pruža i kontrolu tih pravila i politika. Duo ima jedistvenu prijavu (SSO) koja pruža centralizirani pristup i lokalnim i aplikacijama u računalnom oblaku. Dobro organiziran SSO kao što ga Duo pruža je ključan za za zaštitu od kompromitiranih vjerodajnica i rizičnih uređaja kao i od neželjenog pristupa aplikacijama i podacima. Ova kombinacija povjerenja u identitete korisnika i uređaja je temelj za izgradnju sigurnosnog modela nultog povjerenja (*eng. zero-trust security model*). Organizacije mogu uz pomoć Duoa: smanjiti rizik od kompromitirane vjerodajnice ili uređaja, smanjiti vrijeme kad sustav ponovo bude siguran nakon kompromitiranja, povećati vidljivost i granularnu kontrolu, centralizacijom sigurnosti pristupa smanjiti troškove [13].

Cisco Secure Access by Duo pruža sljedeća rješenja [13]:

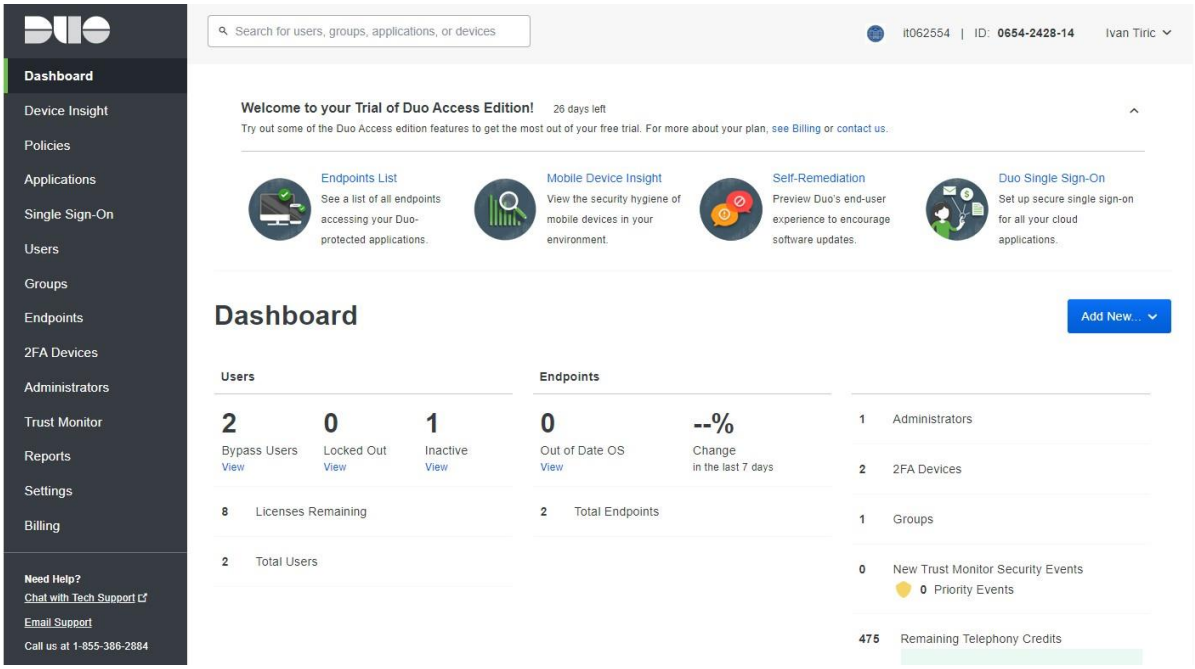
- Multifaktorska autentifikacija (MFA) za brzu potvrdu identiteta. Značajke:
  - MFA sa Duo Push (Duo mobilna aplikacija).
  - MFA sa sigurnosnim ključevima (Duo mobilna aplikacija, SMS, telefonski pozivi, hardverski token), biometrija (U2F, WebAuthN) itd.
- Provjera pristupnih uređaja. Može se pratiti zdravlje (sigurnosne postavke) upravljanih i neupravljanih pristupnih uređaja. Značajke:
  - Nadzorna ploča svih uređaja koji pristupaju aplikacijama.
  - Nadzor i identifikacija rizičnih uređaja.
  - Uvid u sigurnosno stanje prijenosnih i stolnih računala (aplikacija Duo Device Health)
  - Uvid u sigurnosno stanje mobilnih uređaja
  - Prepoznavanje prijenosnih i stolnih računala u vlasništvu poduzeća odnosno onih koji su u vlasništvu korisnika
  - Prepoznavanje mobilnih uređaja u vlasništvu poduzeća odnosno onih koji su u vlasništvu korisnika
  - Provjera da li je agent treće strane omogućen na uređaju (npr. antivirus, antimalware)
- Adaptivna pravila pristupa. Mogućnost postavljanja prilagođenih pravila i politika pristupa. Značajke:
  - Dodjeljivanje i provedba sigurnosnih pravila/politika globalno ili pojedinačno po aplikacijama.
  - Provedba pravila/politika na temelju dozvoljenih mreža.
  - Provedba pravila na temelju lokacije korisnika.
  - Dodjeljivanje i provedba sigurnosnih pravila/politika po grupama korisnika.
  - Blokiranje Tor preglednika i anonimnih mreža.
  - Otkrivanje nepravilnog ili rizičnog pristupa (Duo Trust Monitor).
  - Provedba pravila/politika o pouzdanosti uređaja na temelju sigurnosnog stanja prijenosnih i stolnih računala (zastarjeli softver, enkripcija, vatrozid itd.)
  - Provedba pravila o pouzdanosti uređaja na temelju sigurnosnog stanja mobilnih uređaja (enkripcija, neovlašteno mijenjanje, zaključavanje zaslona, biometrija itd.).
  - Upozorenje korisnika da provedu korektivne mjere na uređajima.
  - Ograničavanje pristupa aplikacijama za uređaje na temelju upisa u sustave upravljanja krajnjim točkama kao što su Landesk, JAMF, Microsoft Intune.
  - Ograničavanje mobilnog pristupa aplikacijama na temelju upisa u *eng. Mobile Device Management* - MDM (AirWatch, MobileIron, Microsoft Intune).
- Udaljeni pristup. Siguran udaljeni pristup bez instaliranog agenta na uređaju. Značajke:
  - Siguran pristup internim web aplikacijama tvrtke (Duo Network Gateway).

- Siguran pristup određenim internim poslužiteljima putem *eng. Secure Shell Protocol* - SSH (Duo Network Gateway).
- Siguran daljinski pristup aplikacijama koje se nalaze na AWS-u, Azure-u i GCP-u (Duo Network Gateway).

- Jedinstvena prijava SSO. Značajke:
  - Neograničene integracije aplikacija.
  - SSO temeljen na računalnom oblaku za sve SAML 2.0 aplikacije.
  - Jednostavan pristup aplikacijama uz Duo Central.

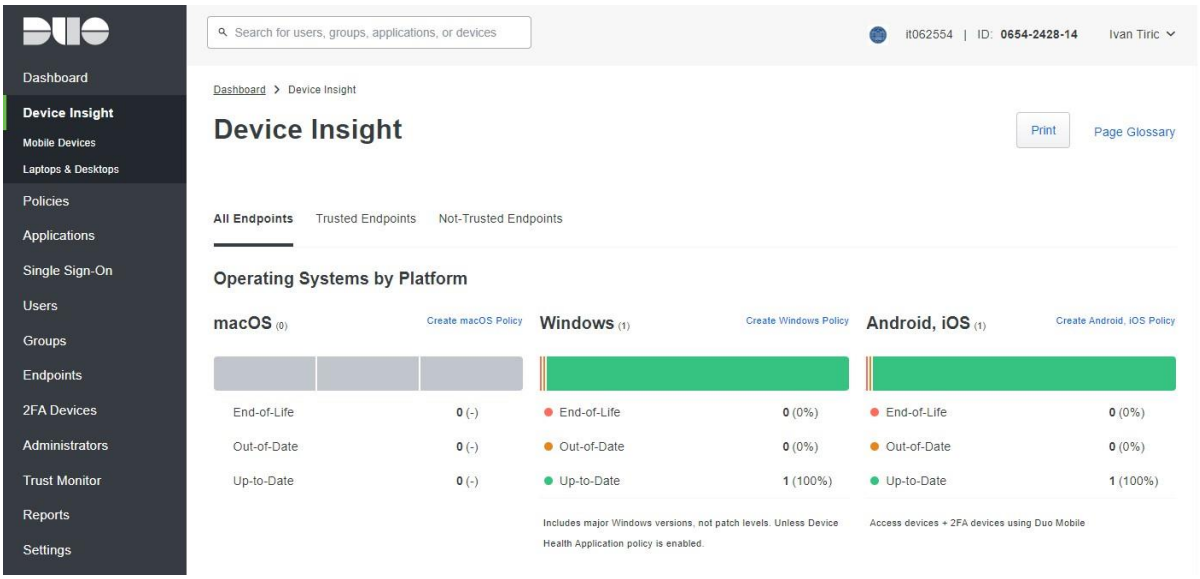
6. REALNI PRIMJER

Odabrano rješenje je aplikacija od tvrtke Cisco naziva Duo. Ova aplikacija je pogodna za primjer jer posjeduje razne sigurnosne značajke i funkcije te jer ima testni period za vrijeme kojeg je aplikacija besplatna za korištenje. Slika 25. prikazuje nadzornu ploču aplikacije Duo [14].



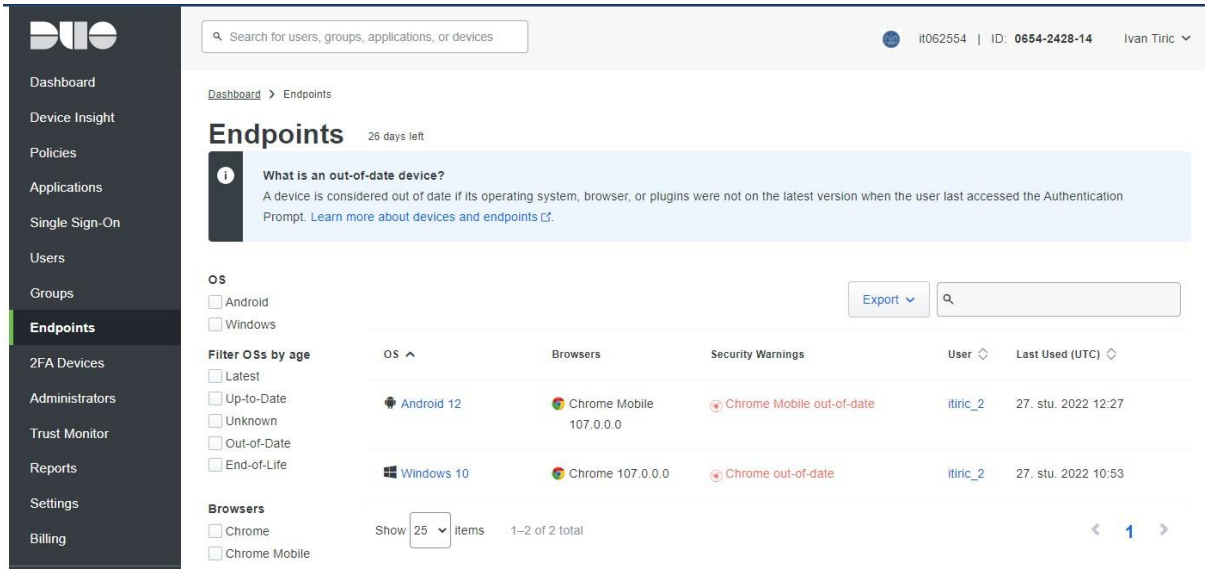
Slika 25. Nadzorna ploča aplikacije Duo [14]

Slika 26. prikazuje pregled pristupnih uređaja gdje se može pratiti zdravlje (sigurnosne postavke) uređaja kojima organizacija upravlja, ali i onih kojima organizacija ne upravlja [14].



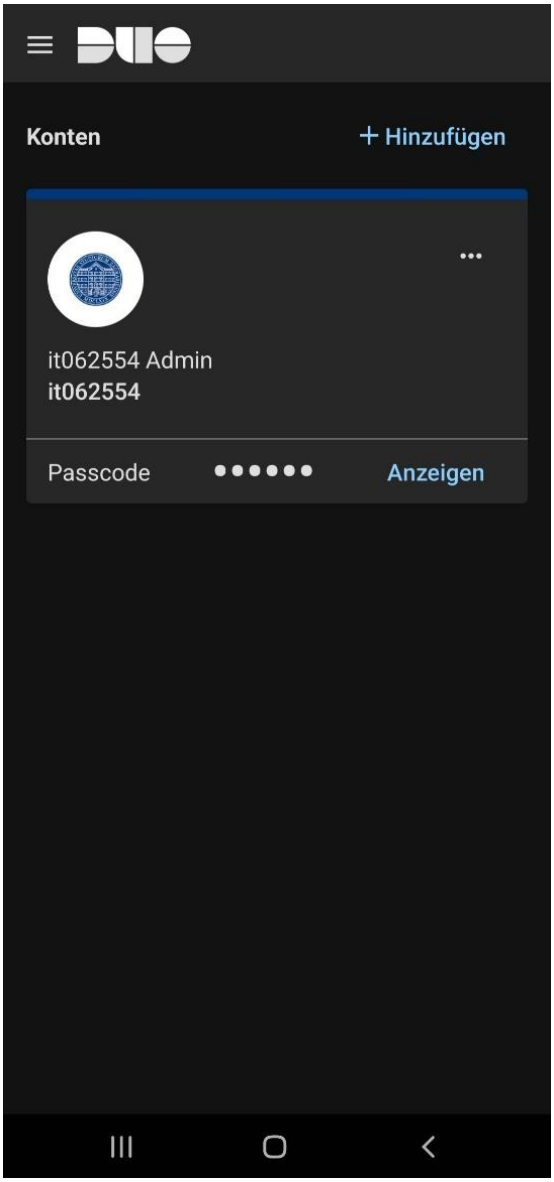
Slika 26. Pregled pristupnih uređaja [14]

Slika 27. prikazuje pregled sigurnosnih postavki i problema na krajnjim pristupnim točkama. U ovom primjeru su krajnje pristupne točke preglednici instalirani na uređajima te se može vidjeti sigurnosno upozorenje da nisu adekvatno ažurirani [14].

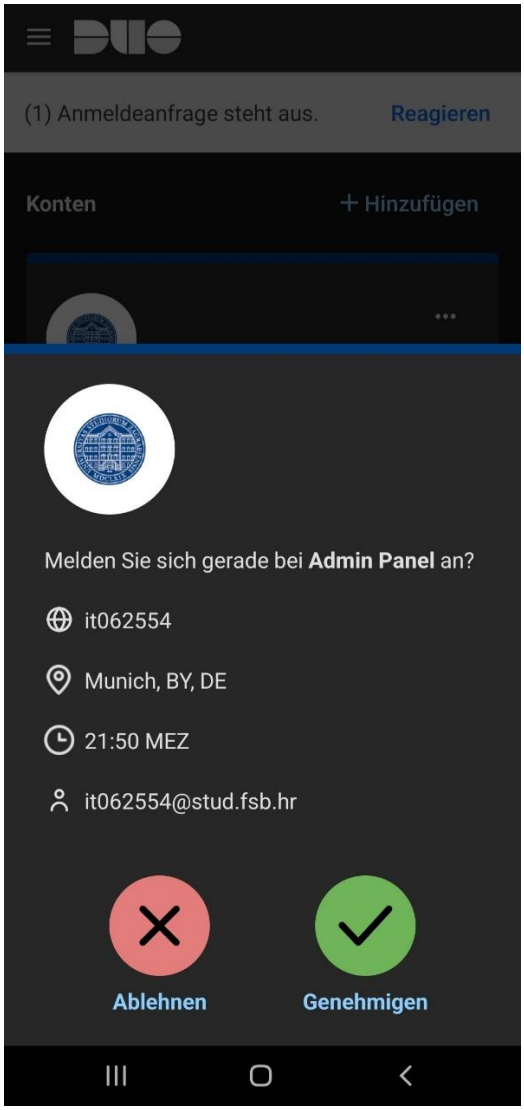


Slika 27. Pregled krajnjih pristupnih točki [14]

Na slici 28. prikazan je ekran mobilne aplikacije Duo za prikaz sigurnosnog ključa za multifaktorsku atentifikaciju (MFA) te pripadajućih korisničkih računa. Postoji i opcija autentifikacije preko Duo Push obavijesti u mobilnoj aplikaciji što je prikazano na slici 29. Lokacije uređaja se isto pregledavaju i spremaju [15].

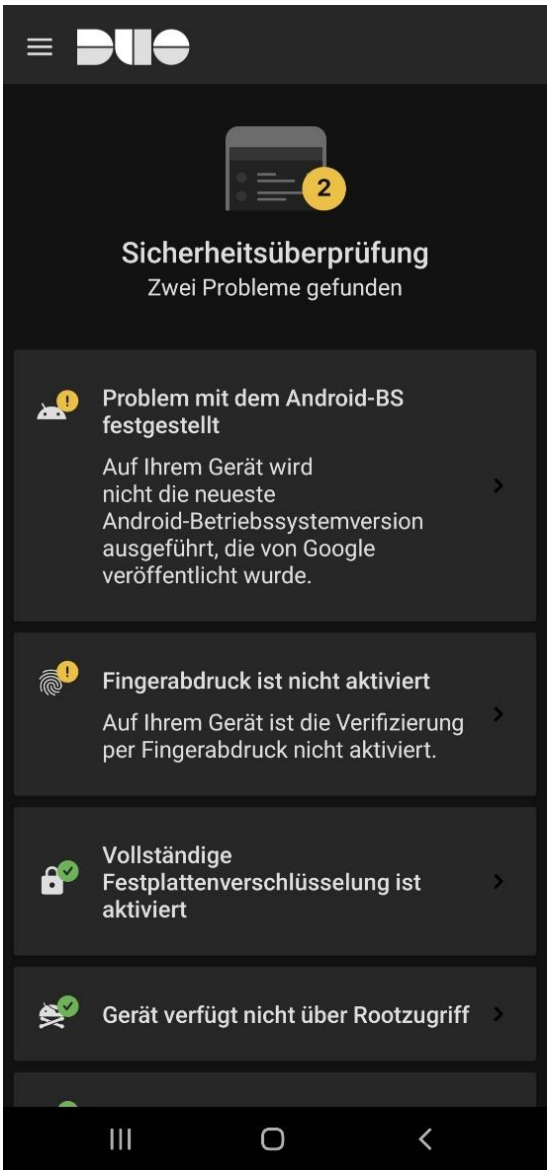


Slika 28. Mobilna aplikacija Duo [15]

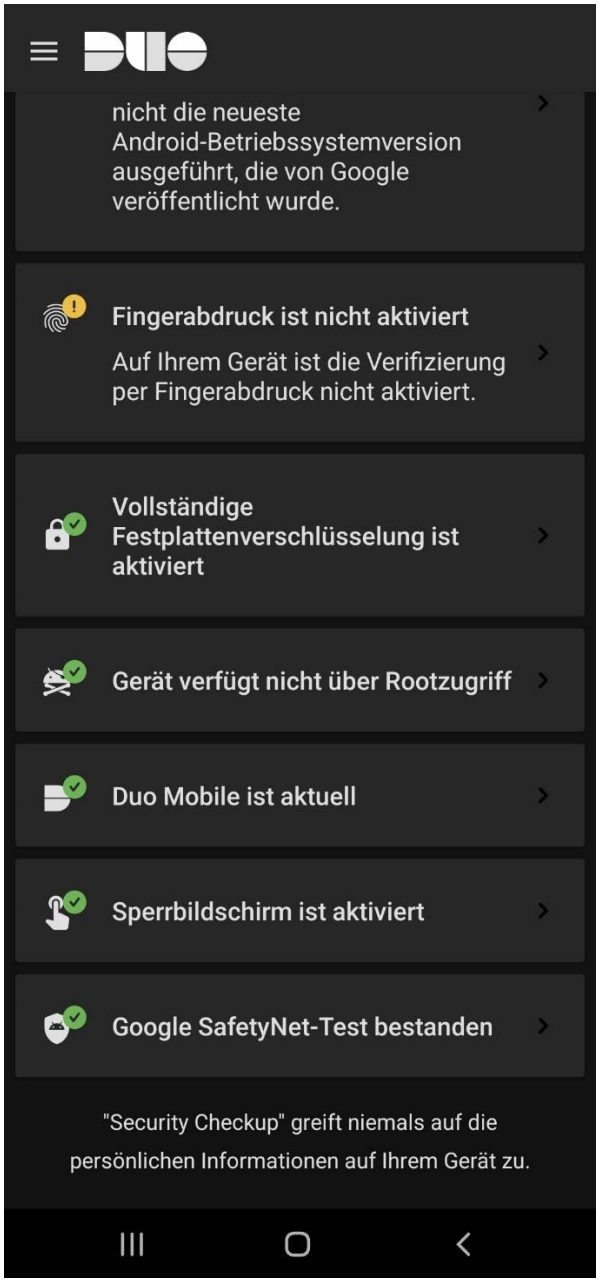


Slika 29. Duo Push [15]

Na slikama 30. i 31. su prikazana sigurnosna upozorenja za mobilni uređaj koje izdaje mobilna aplikacija. Na ovim slikama se vidi da Android operacijski sustav nije najnovija verzija te da se ne koristi biometrija točnije otisak prsta kao dodatnu sigurnosnu postavku, ali se također vidi da su ostale sigurnosne postavke zadovoljavajuće [15].

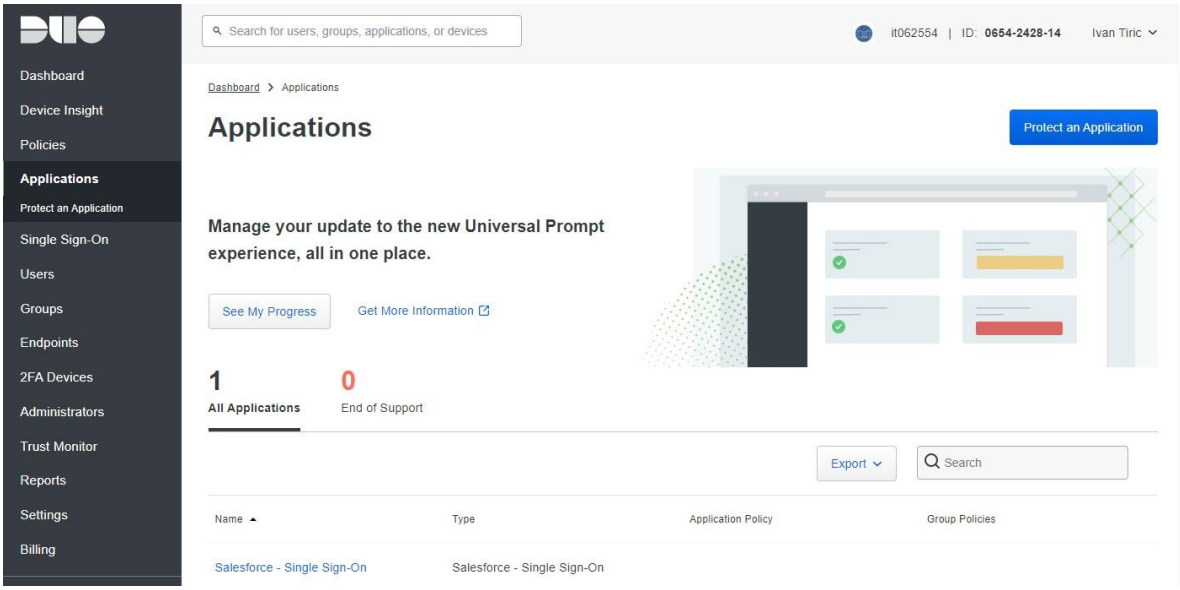


Slika 30. Sigurnosna upozorenja u mobilnoj aplikaciji (1) [15]



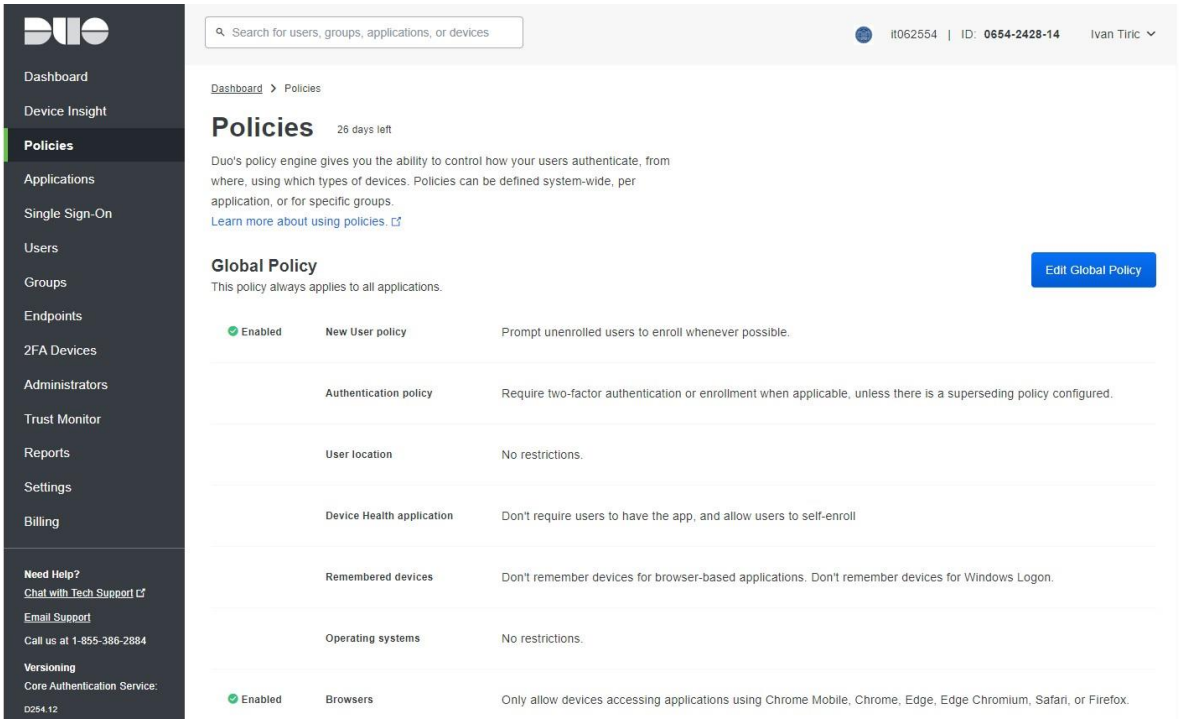
Slika 31. Sigurnosna upozorenja u mobilnoj aplikaciji (2) [15]

Slika 32. prikazuje pregled aplikacija za koje je aktivirana zaštita tj. kontrola pristupa [14].



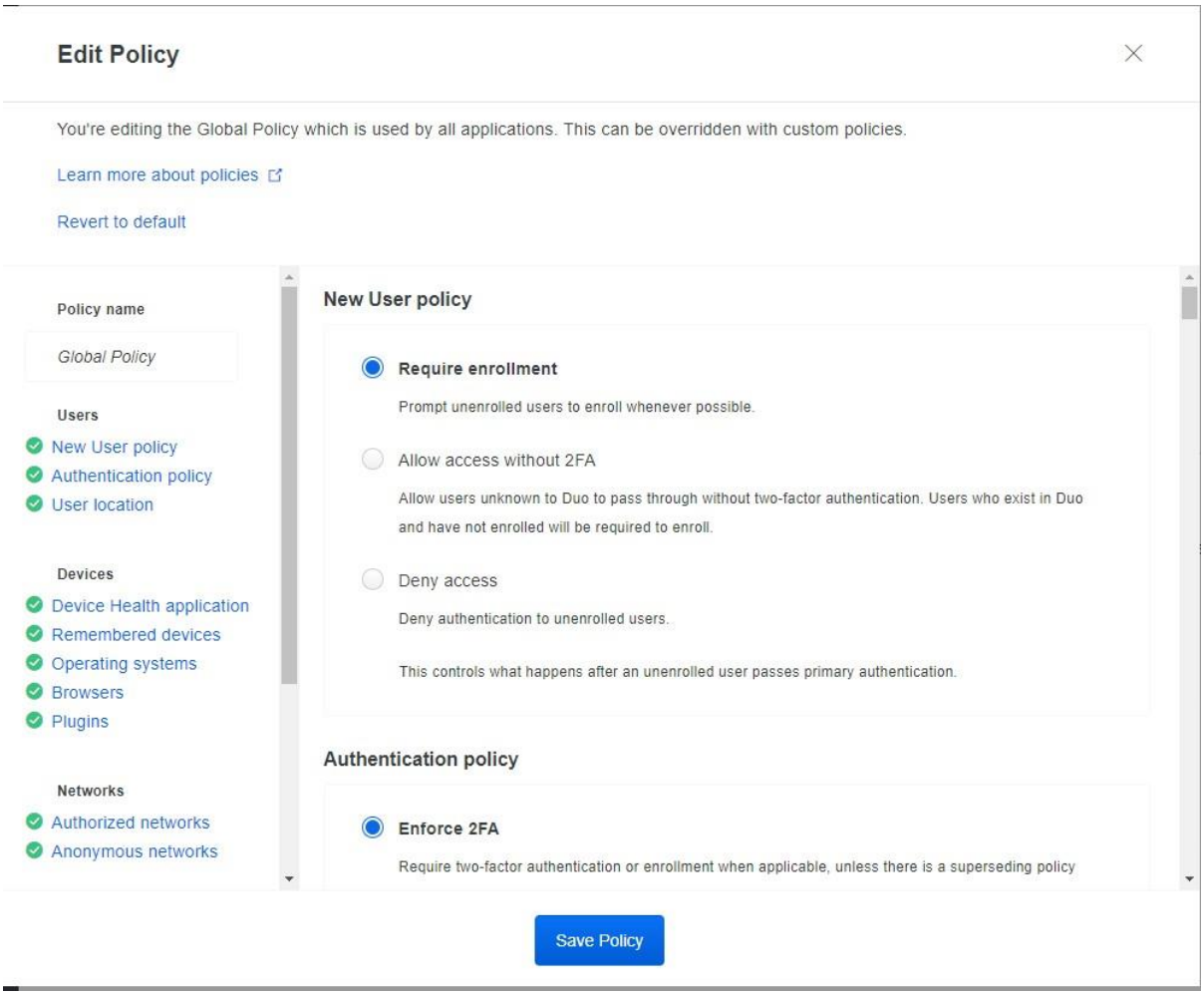
Slika 32. Pregled aplikacija [14]

Slika 33. prikazuje pregled mogućih (i primijenjenih) sigurnosnih postavki (pravila).



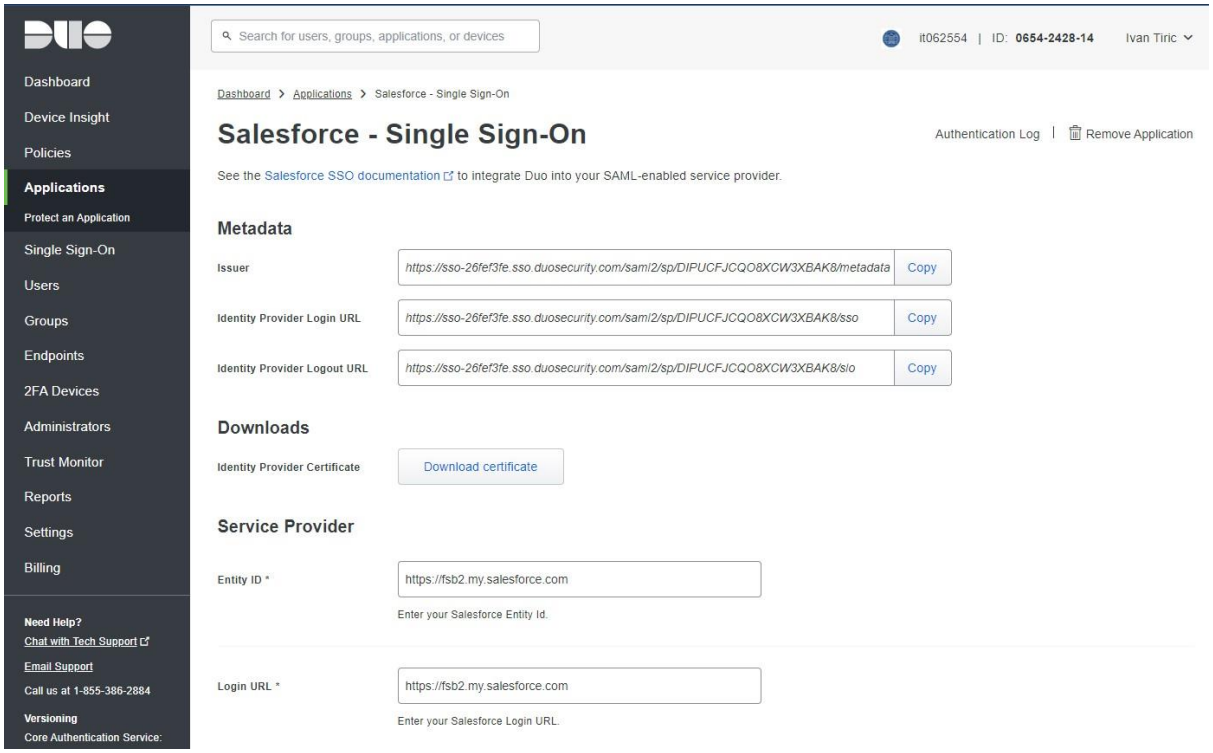
Slika 33. Pregled sigurnosnih postavki [14]

Slika 34. prikazuje ažuriranje sigurnosnih postavki, u ovom slučaju ažuriranje globalnih pravila za korisnike, uređaje i mreže [14].



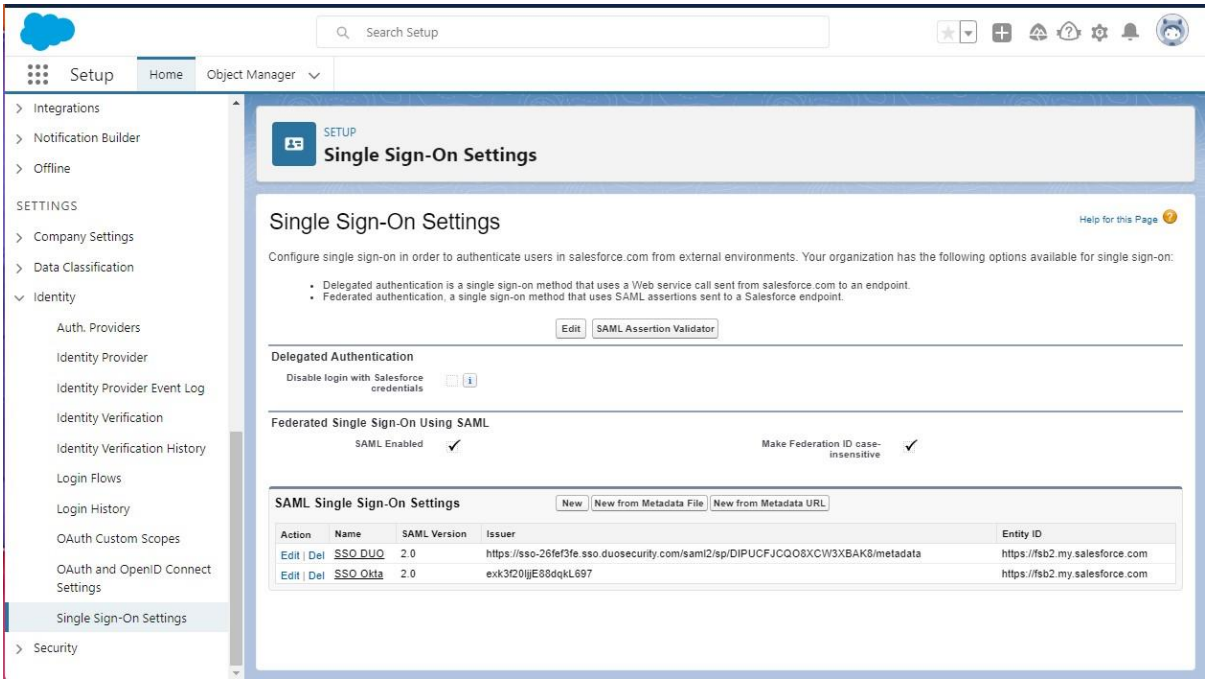
Slika 34. Ažuriranje sigurnosnih postavki [14]

Slika 35. prikazuje SSO postavke u aplikaciji DUO za integraciju s aplikacijom Salesforce.



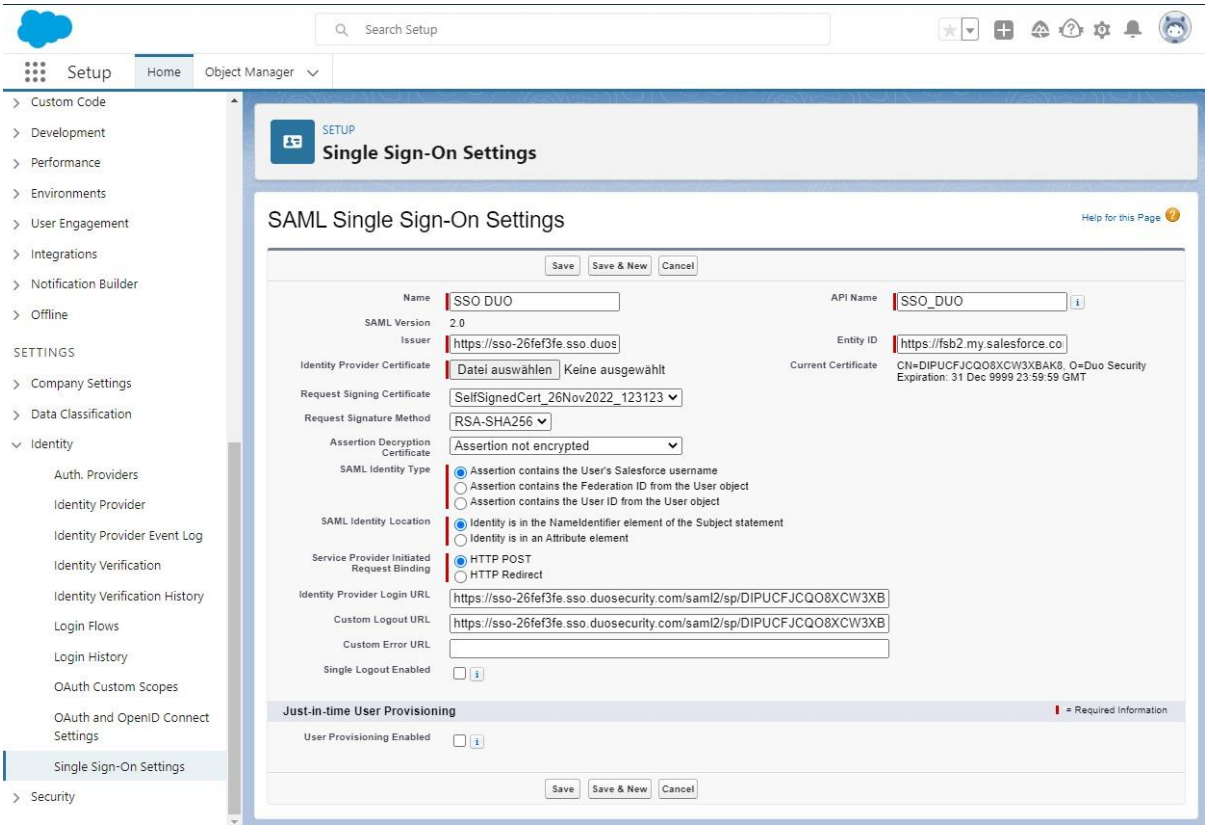
Slika 35. SSO postavke u Duo aplikaciji [14]

Slika 36. prikazuje pregled SSO integracija za aplikaciju Salesforce u samoj aplikaciji Salesforce.



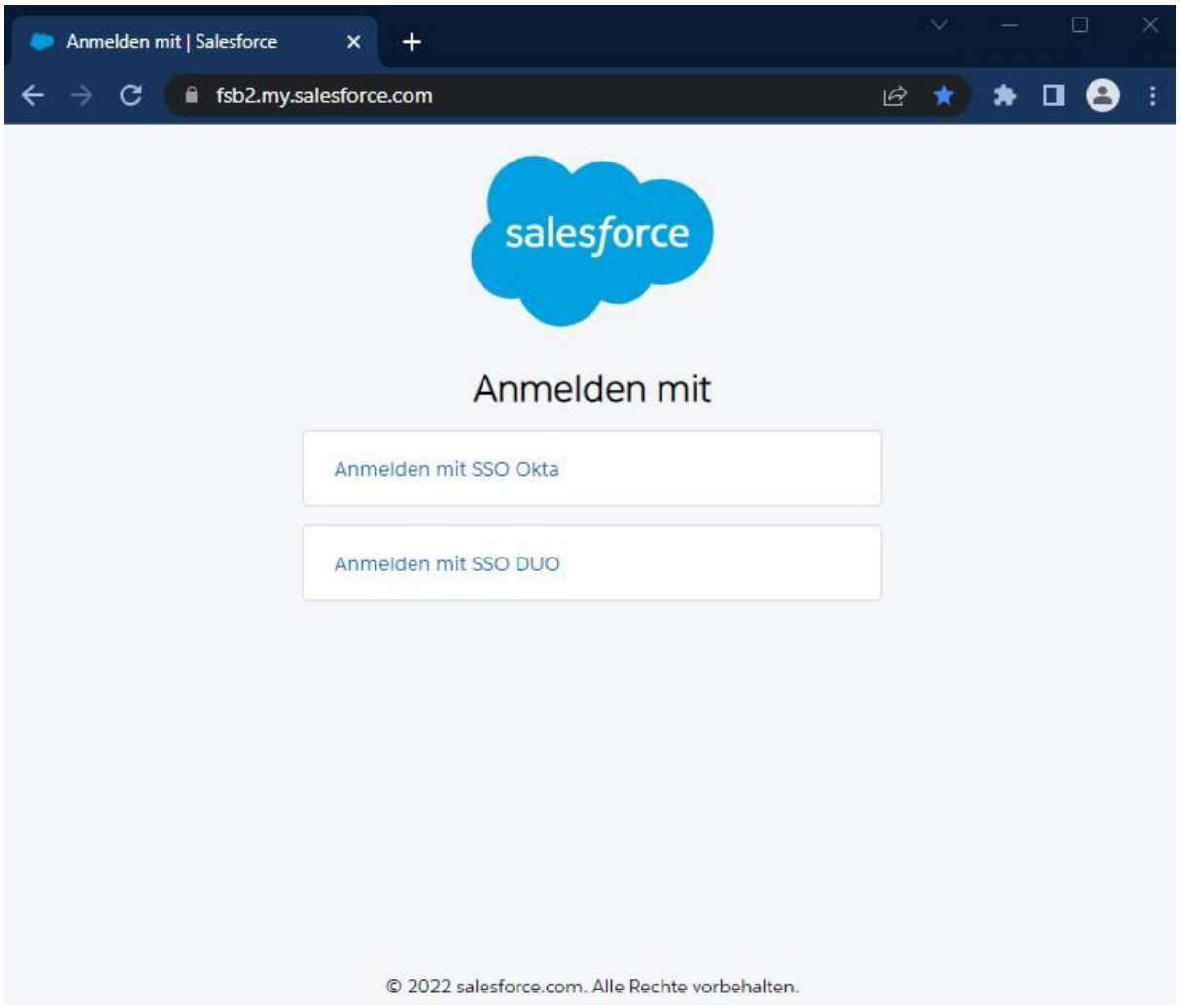
Slika 36. SSO integracije u aplikaciji Salesforce [14]

Slika 37. prikazuje SSO postavke za integraciju u aplikaciji Salesforce s aplikacijom Duo.



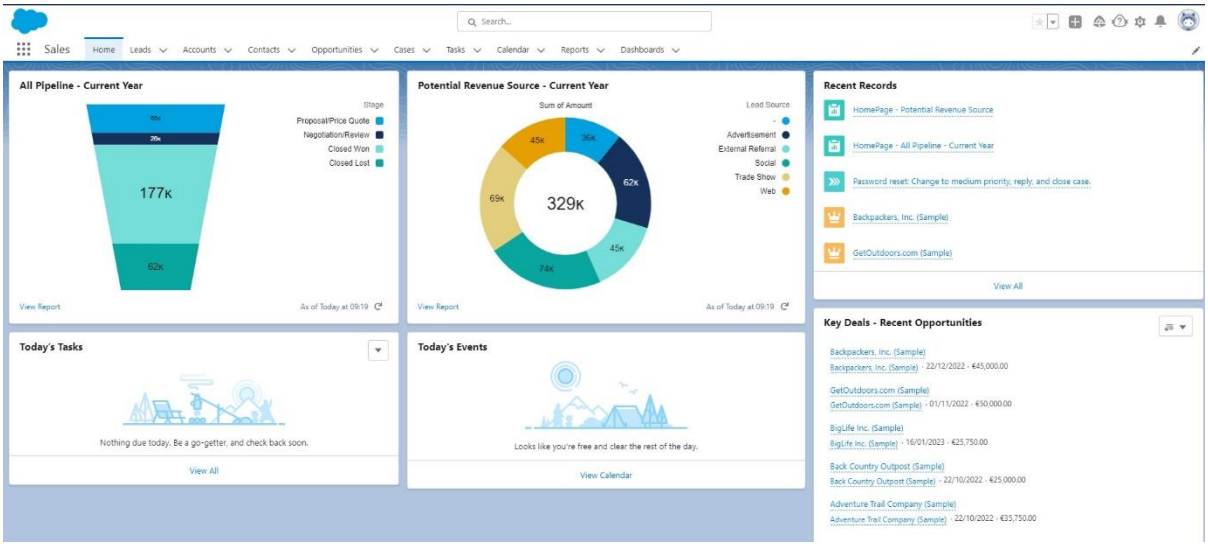
Slika 37. SSO postavke u aplikaciji Salesforce [14]

Slika 38. prikazuje prijavni ekran aplikacije Salesforce iz kojeg je vidljivo da se u aplikaciju može prijaviti isključivo preko SSO-a.



Slika 38. Prijavni ekran aplikacije Salesforce [14]

Slika 39. prikazuje početni ekran aplikacije Salesforce nakon SSO prijave preko aplikacije Duo.



Slika 39. Početni ekran aplikacije Salesforce [14]

7. ZAKLJUČAK

Analiza sigurnosnih rješenja za korištenje aplikacija u računalnom oblaku, pokazala je da CASB rješenja mogu pružiti kvalitetnu sigurnosnu zaštitu, ali je neophodna integracija s brojnim drugim sustavima za sigurnost te sa korisničkim uređajima, korisničkim aplikacijama, ali i raznim drugim servisima. Široki spektar funkcionalnosti pojedinih CASB rješenja, te kompleksnost implementacije i integracije zahtijevaju ekspertna znanja na mnogim područjima kako bi se ova rješenja mogla uspješno implementirati. Iz navedenih razloga bili bi dobro razmotriti postupnu implementaciju ovakvih sustava, i to najprije za upravljanje aplikacijama u računalnom oblaku koje su kritične za poslovanje, ili imaju visoke zahtjeve s obzirom na sigurnost ili zaštitu osobnih podataka, a nakon toga za aplikacije koje su manje rizične. Kod implementacije ovih sustava također treba uzeti u obzir i zaštitu osobnih podataka koje ovi sustavi obrađuju i pohranjuju, s obzirom da zbog integracije s raznim korisničkim uređajima i brojnim drugim sustavima nužno prikupljaju i podatke o aktivnostima i ponašanju krajnjih korisnika. S obzirom na nezaustavljivi rast broja aplikacija u računalnom oblaku i model podijeljene odgovornosti za sigurnost podataka neophodan je daljnji razvoj sigurnosnih rješenja ovog tipa kao i povećanje mogućnosti integracije s različitim aplikacijama i servisima.

LITERATURA

[1] Podaci o tržištu računalstva u oblaku: https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry , Pristupljeno: 21. studenoga 2022.

[2] Grance T., Mell P.: The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, U.S. Department of Commerce 2011.

[3] Liu F., Tong J., Mao J., Bohn R., Messina J., Badger L., Leaf D.: NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology, Special Publication 500-292, U.S. Department of Commerce 2011.

[4] Badger L., Grance T., Patt-Comer R., Voas J.: Cloud Computing Synopsis and Recommendations, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-146, U.S. Department of Commerce 2012.

[5] Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, CSA- Cloud Security Alliance, 2017.

[6] Gordon A. The Official (ISC)2 Guide to the CCSP CBK. 2nd ed. Hoboken: Wiley; 2016.

[7] Adiga G., Almasri Y., Chin V., Chung V., Evgey T., Ma A., Mason M., Perez-Etchegoyen J.P., Rao M. (ERP Security Working Group): State of Enterprise Resource Planning Security in the Cloud, CSA – Cloud Security Alliance, 2018.

[8] Yeoh J., Baron H.: The Impact of Cloud on ERP, A Survey Report on the Migration of ERP to Cloud Enviroments, CSA – Cloud Security Alliance, 2018.

[9] Friedman J, Bouchard M. Definitive Guide to Cloud Access Security Brokers: Visibility, Security, and Compliance for Applications and Data in the Cloud. Annapolis: Cyberedge press; 2015.

[10] Najkorištenije CASB aplikacije: https://www.sunnyvalley.io/docs/network-security-tutorials/top-cloud-access-security-broker-casb-vendors-for-2022 , Pristupljeno: 21. studenoga 2022.

[11] Dokumentacija od Netskope: https://docs.netskope.com/en , Pristupljeno: 22. studenoga 2022.

[12] Dokumentacija od McAfee/Skyhigh: https://success.myshn.net/Skyhigh_CASB , Pristupljeno: 22. studenoga 2022.

[13] Dokumentacija od Cisco Duo: https://duo.com/docs#web , Pristupljeno: 27. studenoga 2022.

[14] Cisco Duo web stranica: https://duo.com/trial , Pristupljeno: 27. studenoga 2022.

[15] Cisco Duo mobilna aplikacija, Pristupljeno: 27. studenoga 2022.