Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

SIGURNOST SALESFORCE PLATFORME I ZAŠTITA PODATAKA NJEZINIH KORISNIKA

Diplomski rad

Alen Kanceljak

Zagreb, lipanj 2024.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

SIGURNOST SALESFORCE PLATFORME I ZAŠTITA PODATAKA NJEZINIH KORISNIKA

SALESFORCE PLATFORM SECURITY AND DATA PROTECTION OF ITS USERS

Diplomski rad

Student: Alen Kanceljak

JMBAG: 0067587397

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, lipanj 2024.

Sažetak

Salesforce je popularna platforma koja pruža usluge računalstva u oblaku. Svojim raznim alatima omogućuje kompanijama upravljanje marketingom, prodajom i korisničkim odnosima. Radom se istražuju prijetnje, ranjivosti i metode zaštite podataka unutar platforme. Upravljanjem velikom količinom podataka, Salesforce-u je od izuzetnog značaja osigurati integritet, povjerljivost i dostupnost podataka. Analiziraju se razne kontrole zaštite poput: identifikacije, autorizacije, enkripcije podataka, praćenja aktivnosti korisnika i ograničenja nad podacima od samih zaposlenika. Također se razmatraju i pravni okviri i regulative koje utječu na zaštitu podataka korisnika kao što su Opća uredba o zaštiti podataka (GDPR), ISO standardi i drugi propisi. Revizijom se provjerava uspješnost informacijskog sustava, odnosno u kojoj mjeri su njegove kontrole učinkovite. Redovitom revizijom, konstantnim nadzorom nad sustavom i edukacijom zaposlenika, doprinosi se povećanju sigurnosti od raznih kibernetičkih prijetnji. Cilj ovog rada je opisati sigurnost korištenja Salesforce platforme, na koje načine upravlja podacima korisnika te kako se štiti od potencijalnih kibernetičkih napada. Kroz sveobuhvatnu analizu, diplomski rad pruža dublje razumijevanje sigurnosnih izazova i najboljih praksi na Salesforce platformi, čime se pomaže organizacijama da učinkovito zaštite podatke svojih korisnika u digitalnom okruženju.

Ključne riječi: Salesforce, računalstvo u oblaku, informacijski sustav, podaci, kibernetičke prijetnje

Abstract

Salesforce is a popular platform that provides cloud computing services. With its various tools, it enables companies to manage marketing, sales and customer relations. The work explores threats, vulnerabilities and data protection methods within the platform. By managing a large amount of data, it is extremely important for Salesforce to ensure the integrity, confidentiality and availability of the data. Various protection controls are analyzed such as: identification, authorization, data encryption, monitoring of user activities and restrictions on data from the employees themselves. Legal frameworks and regulations affecting user data protection such as the General Data Protection Regulation (GDPR), ISO standards and other regulations are also considered. The audit checks the success of the information system, that is, how effective its controls are. Regular auditing, constant monitoring of the system and employee education contribute to increasing security against various cyber threats. The aim of this paper is to describe the security of using the Salesforce platform, in which ways it manages user data and how it protects itself from potential cyberattacks. Through comprehensive analysis, the thesis provides a deeper understanding of security challenges and best practices on the Salesforce platform, helping organizations to effectively protect their users' data in the digital environment.

Key words: Salesforce, cloud computing, information system, data, cyber threats

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad / seminarski rad / prijava teme diplomskog rada isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada / prijave teme nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada / prijave teme ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada / prijave teme nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Alen Kancelják

(vlastoručni potpis studenta)

Zagreb, 23. studenoga 2023.

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

Alen Kancelják

(personal signature of the student)

Zagreb, 23. studenoga 2023.

(place and date)

Sadržaj

1. Uvod

U današnjem globaliziranom svijetu, gdje su ljudi međusobno povezani u sekundama, a aplikacije olakšavaju život i poslovanje, sigurnost podataka postaje ključna. S globalizacijom dolaze i kibernetičke prijetnje, poput phishinga, malware-a i društvenog inženjeringa, čime se naglašava važnost kibernetičke sigurnosti te opreznost korisnika. U kontekstu ovog diplomskog rada, fokus je na Salesforce CRM (sustav za upravljanje odnosima s kupcima, engl. Customer Relationship Management, u nastavku će se koristiti kratica CRM) platformi koja je danas među vodećim kompanijama u svijetu po pružanju usluga računalstva u oblaku. Svojim raznim aplikacijama poput: prodaje, marketinga, korisničke podrške, analitike, itd. pospješuje poslovanje kompanija. Raznim značajkama daje široku paletu mogućnosti svojim korisnicima. Salesforce je velika baza podataka u koju se pohranjuju osjetljivi podaci korisnika, stoga je osiguranje privatnosti nad podacima od izuzetne važnosti kako za Salesforce platformu tako i za korisnike. Raznim mjerama zaštite nastoje se smanjiti kibernetički rizici, no ipak i najmanja nepažnja može dovesti do povrede nad podacima.

1.1. Predmet i cilj rada

U ovom radu se istražuju aspekti sigurnosti Salesforce platforme te se analiziraju mjere zaštite korisnika unutar nje. Razjasniti će se uloge korisnika unutar Salesforce platforme te će se analizirati na koji način njihova aktivnost može utjecati na sigurnost podataka. Kroz definiranje različitih profila, skupova dopuštenja i licenci korisnika, rad će istražiti kakve sve ovlasti korisnici mogu imati unutar platforme te kako se osigurava da pristup podacima bude u skladu s korisničkim ulogama. Isto tako će se i istražiti kako je Salesforce usklađen s regulativama i standardima o zaštiti podataka. Rad će se usredotočiti na razumijevanje kibernetičkih prijetnji i ranjivosti koje mogu utjecati na privatnost podataka. Cilj je opisati sigurnost korištenja Salesforce platforme, na koje načine upravlja podacima korisnika te kako se štiti od potencijalnih kibernetičkih napada. Nadalje, kroz rad će se objasniti ključne sigurnosne značajke koje platforma pruža, uključujući kontrolu pristupa, mehanizme provjere autentičnosti, enkripciju podataka, praćenje aktivnosti korisnika i druge aspekte relevantne za očuvanje sigurnosti podataka. Kroz analizu povijesnih slučajeva kibernetičkih napada na Salesforce platformu, rad će identificirati nedostatke i propuste koji su doveli do takvih incidenata te predložiti bolje kontrole koje su mogle spriječiti takve napade.

1.2. Metode istraživanja i izvori podataka

Koristiti će se više metoda prilikom istraživanja. Metodom indukcije će se na temelju analize pojedinačnih činjenica doći do zaključka o općem sudu, dok će se deduktivnom metodom iz općih stavova doći do pojedinačnog i posebnog zaključka. Zatim će se koristiti i metoda analize gdje će se prikupiti informacije pomoću adekvatne literature iz raznih znanstvenih i stručnih članaka, knjiga, pravilnika, publikacija i izvora s interneta te će se te složene misaone tvorevine raščlaniti na jednostavnije sastavne dijelove. Isto tako će se i koristiti metoda kompilacije, gdje će se koristiti tuđi rezultati znanstveno-istraživačkog rada, kako bi se lakše objasnili neki dijelovi teme. Time će biti razrađen teorijski dio rada. Rad će obuhvaćati i metodu studije slučaja gdje će se izučavati stvarni slučajevi.

1.3. Sadržaj i struktura rada

Rad je strukturiran u 6 zasebnih cjelina: Uvod, uvod u Salesforce platformu, podaci kao temelj raspolaganja znanja o korisnicima u Salesforce platformi, zaštita podataka i sigurnost prijave u Salesforce platformu, revizija i nadzor podataka u Salesforce-u i na kraju zaključak. Kroz uvod se opisuje predmet i cilj ovog rada te metode istraživanja i izvori podataka korišteni za izradu rada. U drugoj cjelini će se reći nešto općenito o Salesforce-u i njegovoj primarnoj usluzi koju pruža, a to je računalstvo u oblaku. Treća cjelina će objašnjavati kakvi sve tipovi podataka postoje unutar platforme, kakva su ograničenja nad podacima te tko sve od korisnika može biti uključen u proces poslovanja. Također će biti i riječi u kolikoj je mjeri Salesforce usklađen sa Općom uredbom o zaštiti podataka (engl. General Data Protection Regulation, u nastavku će se koristiti skraćenica GDPR) i ostalim standardima za zaštitu podataka. U četvrtoj cjelini će se razraditi svi slojevi zaštite nad podacima koje koristi Salesforce kao i protokoli na temelju kojih radi identifikacija korisnika. Peta cjelina će na temelju studije slučaja prikazati nedostatke u zaštiti podataka unutar Salesforce platforme te će se dati osobna mišljenja o kontrolama koje su mogle spriječiti nastalu štetu. Isto tako će se u tom poglavlju objasniti načini na koje se prate radnje korisnika te moguća poboljšanja sustava zaštite. U zadnjem, šestom poglavlju će se navesti svi relevantni zaključci izradom ovog rada.

2. Uvod u Salesforce platformu

Salesforce je CRM softver temeljen na tehnologiji računalstva u oblacima (engl. cloud computing, u nastavku će se koristiti pojam cloud). Pruža inovativna rješenja upravljanja odnosima s kupcima te potencijalnim kupcima. Platforma svojom tehnologijom pomaže kompanijama pojednostavljujući im poslovne procese tako da ostanu u interakciji s klijentima te da im se poboljša profitabilnost. Pomaže svim odjelima unutar kompanije da produktivnije rade te da pružaju kupcima personalizirana iskustva. Platformom odjeli unutar kompanije lakše komuniciraju, automatiziraju se repetitivni zadaci, lakše je pružanje korisničke podrške zbog cjelokupnog pogleda na kupca, pojednostavljenje pogleda na performanse poslovanja kompanije pomoću izvješća i grafova, lakše dolaženje do rješenja pomoću tehnologije umjetne inteligencije (engl. artificial intelligence), itd. Salesforce koristi više od 150.000 kompanija svih veličina diljem svijeta, a neke od njih su: PayPal, IBM, Sonos, itd (Salesforce, 2023a).

Salesforce (Salesforce Inc) kompanija osnovana je 1999. godine u Kaliforniji u gradu San Francisco (Sjedinjenje Američke Države - SAD) gdje joj je i sjedište. Spada među najcjenjenije pružatelje usluga računalstva u oblaku. Companiesmarketcap.com (2023) iznosi podatke da je na dan 30. studenoga 2023. godine, Salesforce-ova tržišna kapitalizacija iznosila oko 238 milijardi američkih dolara, sa cijenom jedne dionice od oko 244 američkih dolara, svrstavajući je tako na 39 poziciju najvrjednijih kompanija u svijetu prema tržišnoj kapitalizaciji.[1] Lider je u pružanju CRM usluga. Tvrtka je osnovana od strane prethodnih službenika Oracle-a, a to su: izvršni direktor Marc Benioff (CEO), Parker Harris, Dave Moellenhoff i Frank Dominguez. Salesforce je dostupan u cloud-u te nema potrebe za preuzimanjem softvera ili korištenjem dodatnog hardvera kako bi se služilo platformom. Putem SWOT analize dolazi se do zaključka da su snage Salesforce kompanije: kvalificirana radna snaga, smanjenje troškova poslovanja zbog pružanja računalstva u oblaku putem interneta, mogu održavati postojeće distribucijske i prodajne mreže, pružanje inovativnih cloud usluga kroz razne aplikacije, tvrtke mogu jednostavno postaviti svoju infrastrukturu koristeći Salesforce. Slabosti su buduća produktivnost i visoka ulaganja u istraživanje i razvoj. Prilike su: popularnost usluga u oblaku može se poboljšati i povećati, Salesforce je rastuća ekonomija, veća stopa rasta i profitabilnost

[1] Izvor: https://companiesmarketcap.com/salesforce/marketcap/ [Pristupano 30. studenoga 2023].

te rizični kapital, Prijetnje su: promjena cijena, povećanje troškova radne snage i konkurencija sa inovativnijim rješenjima. Neki od najvećih konkurenata Salesforce-a su: Oracle Corporation, SAP, Net Suite i Yammer (Sneha i Krishna Prasad, 2018).

Salesforce omogućuje širok spektar aplikacija poput: prodaje, marketinga, korisničke podrške, analitike i mnogih drugih. Centralizirana je platforma koja povezuje sve te aplikacije unutar jednoga mjesta pružajući lako prebacivanje iz jedne aplikacije u drugu. Sneha i Krishna Prasad (2018) navode kako su Sales Cloud, Service Cloud i Marketing Cloud jedni od najvažnijih proizvoda, odnosno aplikacija koje nudi Salesforce. Takve aplikacije su savršeno integrirane unutar Salesforce-a te uz pomoć raznih funkcija pomažu kompanijama da uspješno posluju. Salesforce pruža cloud usluge kao softver (engl. software as a service, u nastavku će se koristiti skraćenica SaaS) i kao platforma (engl. platform as a service, u nastavku će se koristiti skraćenica PaaS). Sigurna je platforma visokih performansi čija je primarna uloga da pruža usluge računalstva u oblaku za pohranjivanje podataka svojim korisnicima. Na taj način omogućuje sigurno prikupljanje, organiziranje i korištenje podataka. Velte et al. (2010) ističu kako se računalstvo u oblaku smatra naprednom digitalnom tehnologijom koja na moderan i troškovno učinkovit način transformira zastarjele sustave i procese u visoko skalabilne sustave koji zahtijevaju malo održavanja. Više o modelima i općenito o računarstvu u oblaku objašnjeno je u nastavku.

„Računalstvo u oblaku (engl. Cloud Computing) je okruženje sastavljeno od resursa hardvera i softvera u centrima podataka koji pružaju različite usluge putem mreže ili interneta kako bi se zadovoljili zahtjevi korisnika“ (Leavitt, 2009 navedeno u Sun, Y. et al., 2014). Cloud pruža usluge na zahtjev korisnika te se sve više i više kompanija okreće korištenjem tih usluga kako bi smanjili svoje troškove. Gong et al. (2010) ističu neke karakteristike računalstva u oblaku, a to su: samoposluživanje na zahtjev, sveprisutni pristup mreži, udruživanje resursa neovisno o lokaciji, elastičnost resursa, cijene temeljene na korištenju i prijenos rizika. Da bi korisnici stekli povjerenje te koristili usluge računalstva u oblaku, Sun, Y. et al. (2014) navode 4 ključne mjere za osiguranje sigurnosti podataka koje moraju biti zadovoljene. To su: Integritet podataka – podaci se štite od neovlaštenog pristupa putem upravljanja pravima pristupa i autorizacijom. Povjerljivost podataka – osiguranje osjetljivih podataka u oblaku enkripcijom podataka. Dostupnost podataka – ukoliko dođe do nekog problema ili kvara, da podaci i dalje budu dostupni i oporavljivi korisnicima. Privatnost podataka – osiguranje da se osjetljivi podaci ne otkriju neovlaštenim osobama.

Ovisno o odgovornosti i razini kontrole koju korisnici žele preuzeti, Manaa (2018) nabraja i objašnjava tri modela korištenja cloud usluga, a to su: softver kao usluga (software as a service - SaaS), platforma kao usluga (platform as a service - PaaS) i infrastruktura kao usluga (engl. infrastructure as a service, u nastavku će se koristiti skraćenica IaaS). SaaS pruža gotove aplikacije koje omogućuju korisnicima njihovo korištenje putem softvera. Time je mala odgovornost na korisniku, a velika na pružatelju usluge koji brine za sigurnost aplikacije i njezinih podataka, sigurnosti nad mrežom, operativnim sustavom te infrastrukturom. SaaS omogućuje pristup softveru putem web preglednika. Primjeri takvog modela su Salesforce.com, Facebook, Google Apps, Dropbox, LinkedIn, itd. U PaaS-u pružatelj cloud usluge daje mogućnost razvoja, testiranja i implementacije aplikacije koristeći API koji omogućuje samostalno upravljanje resursima (Application Programming Interface), no pružatelj cloud usluga i dalje brine o mreži, operativnom sustavu i infrastrukturi. Primjeri takvih modela su: Salesforce.com, Windows Azure, Gigaspace, Appscale, Loglump i mnogi drugi. Kod IaaS-a, korisnik ima najveću odgovornost kod korištenja cloud rješenja. IaaS omogućuje korisnicima da unajme virtualne mašine i virtualna skladišta koja im daju veću fleksibilnost upravljanja nad operativnim sustavima, aplikacijama, konfiguraciji i postavki mreže te pohrani podataka. Korisnici imaju kontrolu nad operativnim sustavom, aplikacijama i konfiguracijom, ali nemaju kontrolu nad fizičkom infrastrukturom poput fizičkog hardvera, mrežne opreme, itd. Kod IaaS-a korisnici plaćaju prema potrošnji (pay-per-use paradigm), što znači da korisnici plaćaju samo za korištene resurse. RackSpace, Joynet, Savvis i Enamoly primjeri su IaaS računalstva u oblaku (Manaa, 2018).

Postoji puno tipova napada koji mogu ugroziti računalstvo u oblaku. Shiang Hwang et al., (2014) nabrajaju i opisuju neke od onih koji mogu nanijeti najveću štetu, a to su: povreda podataka (engl. Data Breaches), gubitak podataka (engl. Data Loss), otmica računa (engl. Account Hijacking), Distribuirano Odbijanje Usluge (engl. Distributed Denial of Service, u nastavku će se koristiti skračenica DDoS), itd. Do povrede podataka dolazi kada dođe do neovlaštenog pristupa nad podacima gdje npr. jedan korisnik svojom neopreznošću može dovesti u rizik sve ostale podatke u bazi podataka. Kod gubitka podataka korisnici gube pohranjene podatke, bilo zbog npr. ne postojanja backup opcije ili zbog gubitka ključa za šifriranje i dešifriranje podataka. Kod otmice računa, napadač preuzima kontrolu nad korisničkim računom gdje dalje može naštetiti sustavu i korisnicima unutar sustava. U DDoS-u napadači, koristeći velik broj računala ili uređaja kako bi istovremeno uputili veliki broj zahtjeva prema jednom ciljanom sustavu ili mreži, uskraćuju ovlaštenim korisnicima pristup i

korištenje cloud resursa. Szombathelyi (2021) ističe da kod DDoS napada, napadač velikom količinom prometa preoptereti poslužitelja, gdje poslužitelj najčešće treba obustaviti pružanje usluga svojim klijentima dok se ne ukloni navedeni problem. Manaa (2018) ističe kako Salesforce platforma omogućuje pristup, analiziranje i ažuriranje podataka u oblaku. Koristeći razne protokole i algoritme (WSDL, XML, SOAP, DES, itd), Salesforce omogućuje svojim korisnicima da u veoma kratkom periodu mogu prenijeti veliku količinu osjetljivih podataka na cloud koji su dalje kriptirani i zaštićeni od napadača.

Marańda, W., Poniszewska-Marańda, A. i Szymczy´nska, M. (2022) ističu kako neke kompanije nastoje pohranjivati informacije u vlastitom informacijskom centru što ne mora značiti da će imati veću zaštitu. Isto tako, troškovi za održavanje takvih podatkovnih centara su dosta skupi. Stoga je isplativije odabrati nekog dugogodišnjeg i iskusnog pružatelja cloud usluga koji će svojim sigurnosnim mehanizmima učinkovitije štititi podatke od kibernetičkih napadača nego sama kompanija. Čim je više podataka, to je teže njima upravljati. Marańda, W., Poniszewska-Marańda, A. i Szymczy´nska, M. (2022) navode neke od najvažnijih problema kod obrade i skladištenja velike količine podataka s kojima se suočavaju pružatelji cloud usluga, a su:

1. Pružanje odgovarajuće infrastrukture – povjerljive informacije se moraju obrađivati i skladištiti u profesionalnim uvjetima.
2. Troškovi skladištenja i obrade – nabava, održavanje i osiguranje servera, zapošljavanje stručnjaka, obuka djelatnika, itd. zahtijevaju troškove za cloud pružatelja usluga.
3. Sigurnost podataka – zaštita podataka od raznih kibernetičkih prijetnji gdje cloud pružatelji usluga stvaraju sigurnosne kopije podataka na raznim lokacijama kako bi smanjili rizik od njihove krađe.
4. Prikupljanje podataka – redundancija stvara probleme pri obradi i analizi podataka gdje se u izvješćima i grafovima pokazuju netočni rezultati.
5. Količina i kompatibilnost informacija – mogućnost skalabilnosti kompanije kod prikupljanja sve veće i veće količine informacija gdje će npr. izgraditi još jedan podatkovni centar. Isto tako format svih podataka bi trebao biti isti, omogućujući tako njihovo lakše upravljanje što zahtijeva stručnost zaposlenika.

3. Podaci kao temelj raspolaganja znanja o korisnicima u Salesforce platformi

U današnjem dinamičnom svijetu, poslovanje bez podataka je nemoguće. Svi događaji, transakcije, nazivi i adrese klijenata, stanje robe u skladištu, itd., moraju biti negdje zabilježeni ukoliko kompanija želi uspješno poslovati. Podaci se zapisuju na temelju skupova znakova. Pa tako na primjer znakovima abecede možemo zapisati neku riječ koja je nastala govorom, npr. tipkovnica. Nadalje, u prometnom govoru se služimo prometnim znakovima koji su postavljeni na ceste kako bi se vozači motornih vozila bolje i lakše snalazili. U matematici se koriste specifični znakovi (+, -. =, <. >, itd.) kako bi se riješile jednadžbe. Isto tako u programskim jezicima, svaki znak predstavlja nešto svojstveno koji kad se prenesu u program tvore podatak. Interpretacijom podataka se dobije informacija koja je bitna za donošenje odluka. Informacija je kvalitetna kada je: točna, potpuna, primjerena i pravovremena. Ukoliko se na protumačeni podatak ili skup podataka doda ekspertno mišljenje, dobiva se znanje, dok mudrost nastaje upotrebom znanja za određenu svrhu (Varga, 2021).

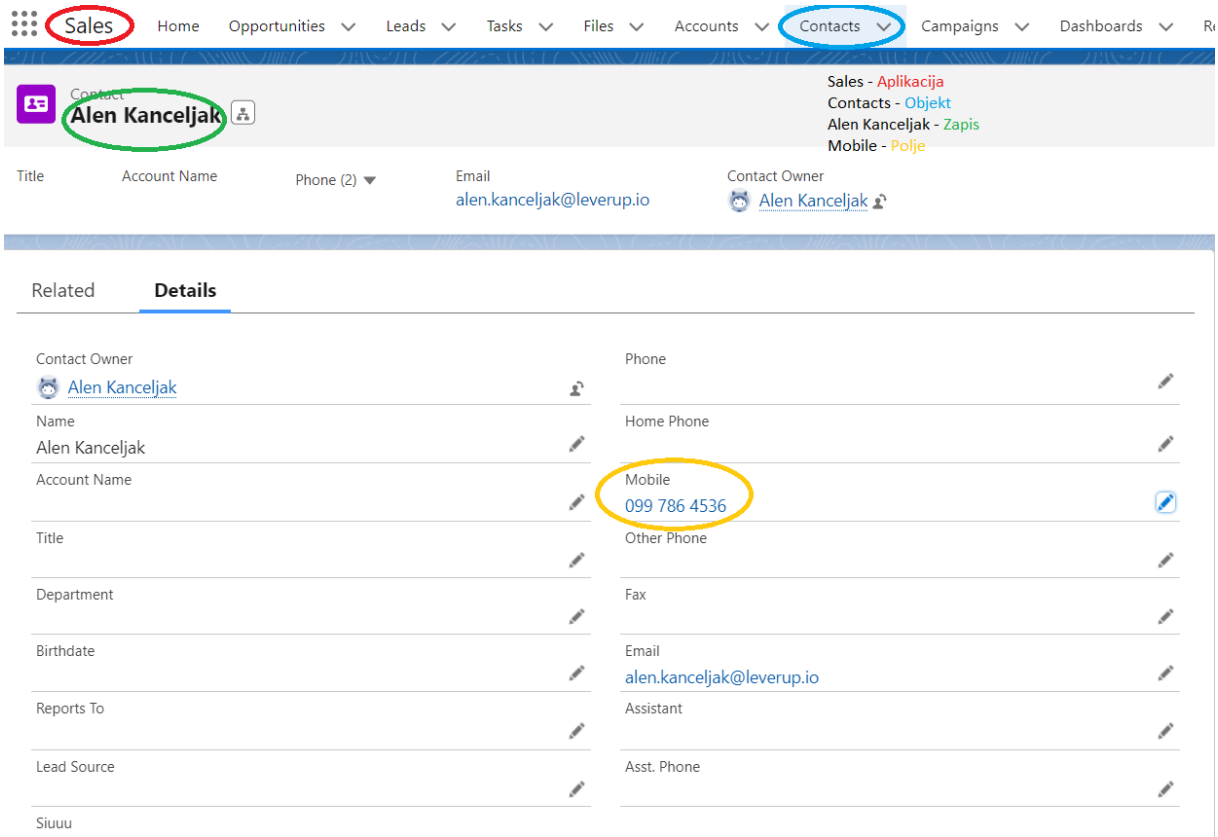
Zahvaljujući razvijenoj informacijskoj tehnologiji, podatke je danas moguće pohraniti u digitalnom obliku koje je nadalje pomoću raznih alata moguće pripremiti za automatizaciju. Ljudskom mozgu je teško zapamtiti veliku količinu podataka odjednom te ako se i zapamte, teško je da će se sjetiti svih podataka već i nakon nekoliko dana. Stoga, da bi se došlo do svih prethodno iznesenih podataka, oni moraju biti negdje pohranjeni. To je danas izuzetno važno za poslovanje jer kupci više ne žele da ih se putem raznih marketinških alata „bombardira" proizvodima za koje nisu zainteresirani. Kupci žele da im se šalju ponude na temelju njihovih preferencija, a to je jedino moguće ako kompanije dovoljno poznaju kupca, odnosno imaju njegove podatke (ime, prezime, email adresa, država porijekla, itd.) i za koje proizvode je zainteresiran kada navigira stranicom. Kupci danas žele imati osjećaj da se kompanija obraća izravno njima, nudeći im proizvode i usluge koje žele, a to je jedino moguće ako su podaci o kupcu negdje zapisani. Podaci se pohranjuju u bazu podataka na nekom od servera. U poslovanju se kaže da ukoliko nešto nije zabilježeno podacima, to se nije ni dogodilo, stoga je bitno da podaci postoje kako ne bi došlo do neke konfuzije. Podaci su bitni da bi se održala lakša i uspješnija komunikacija između ljudi. Vidljivo je da su podaci temelj sporazumijevanja iz kojih se razvijaju ostali pojmovi, a to su već spomenuti: informacija, znanje i mudrost. Salesforce se sastoji od velike baze podataka u kojoj su pohranjeni razni podaci. Baza podataka

služi kako bi se lagano pristupilo podacima u bilo kojem trenutku kada je to potrebno. U nastavku će biti spomenuti i objašnjeni svi tipovi podataka koji mogu biti u Salesforce-u.

3.1. Vrste podataka i njihova upotreba

Odabir skupa podataka koje mogu vidjeti korisnici, jedna je od glavnih stvari koje utječu na sigurnost u Salesforce-u. Podaci koji postoje ili mogu biti kreirani u Salesforce-u su: Objekti (npr. kontakt), zapisi (npr. Alen Kanceljak) i polja (npr. broj mobitela). Dakle, objekti su tablice u Salesforce bazi podataka koje pohranjuju određenu vrstu informacija. Zapisi su redovi u tablicama baze podataka objekata. Dok su polja stupci u tablicama baze podataka objekata. I objekti i zapisi i polja se nalaze u aplikacijama unutar Salesforce-a. Aplikacije bi bile kao neki odjeli gdje samo određeni zaposlenici (korisnici) zaduženi za taj odjel imaju pristup. Tako se npr. aplikacija može zvati Marketing te samo korisnici koji su u marketinškom odjelu imaju pristup podacima u toj aplikaciji, dok kod npr. aplikacije Prodaja (engl. Sales), samo prodajni službenici imaju pristup toj aplikaciji. Na sljedećoj slici je prikazan primjer podataka kojima mogu pristupiti samo korisnici aplikacije za prodaju.

Slika 1. Prikaz objekta, zapisa i polja unutar Sales aplikacije u Salesforce-u (Izvor: vlastiti rad autora)

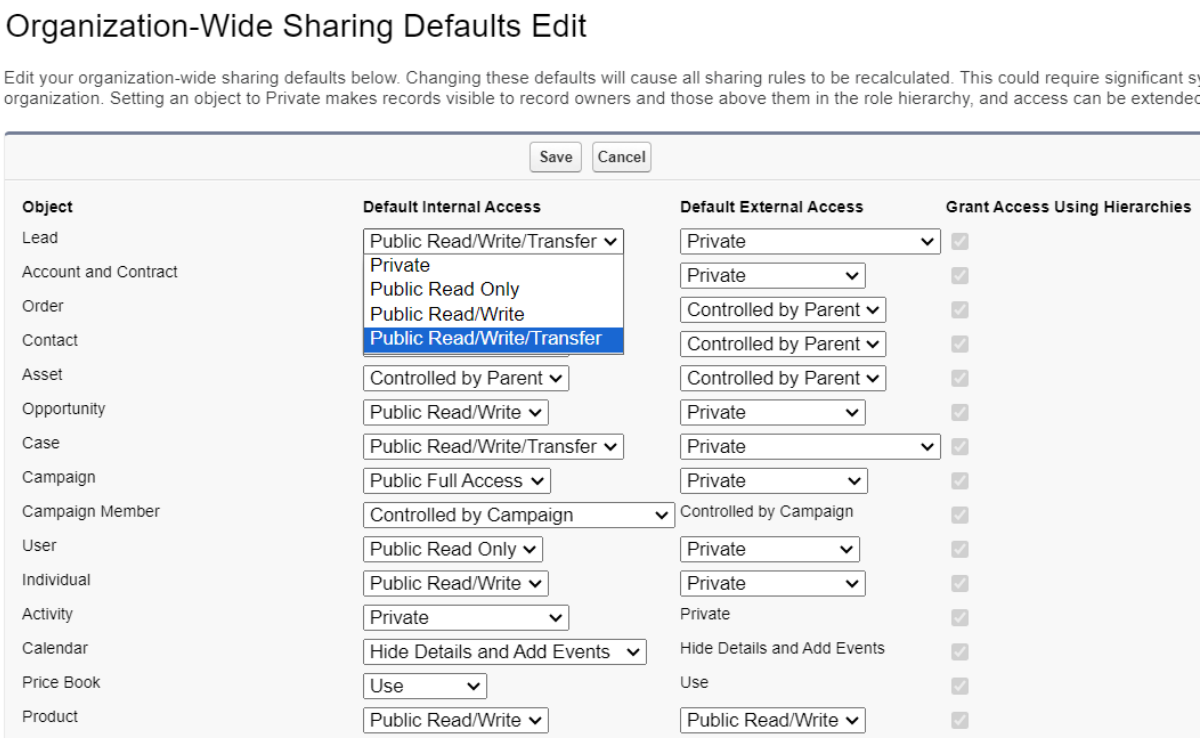


Administrator (skraćeno admin) koji ima ovlaštenje upravljanja korisnicima unutar kompanije, može dodijeliti koje ovlasti će korisnici imati nad podacima (objekt, zapis, polje) u Salesforce-u. Tako kod postavljanja posebnih dozvola (engl. „permission sets“) za objekte, administrator može podesiti koji će se zapisi unutar objekta moći kreirati , brisati, uređivati ili samo imati mogućnost gledanja. Te postavljene dozvole se zatim dodjeljuju korisnicima. Npr. kreira se dozvola pod imenom „zaposlenje“. U dozvoli „zaposlenje“ se urede sva moguća ograničenja te se zatim ta dozvola dodjeljuje nekom korisniku. Na taj način će npr. anketari moći vidjeti prijave za posao i pozicije, ali ih neće moći brisati ili uređivati. Kod polja se na sličan način mogu podesiti ograničenja. Pa tako npr. polje prihoda nije vidljivo anketarima, dok je s druge strane vidljivo regruterima (engl. recruiter) i menadžerima za zapošljavanje. Kod zapisa ima nešto više mogućnosti podešavanja vidljivosti nad podacima gdje se omogućuje da korisnik osim svojeg privatnog zapisa može vidjeti i nečiji drugi zapis. To ovisi o sljedećim četirima postavkama unutar Salesforce-a: Org-Wide defaults, Role hierarchies, Sharing rules i Manual Sharing (Sharma, 2020).

Org-Wide defaults – je osnovna i najviše restriktivna razina sigurnosti nad zapisima ostalih korisnika. Ta razina se može mijenjati s ostalim alatima za sigurnost i dijeljenje prema potrebama korisnika unutar kompanije. **Role hierarchies -** Osigurava da osoba koja je iznad osobe po hijerarhijskoj ljestvici ima pristup zapisu podređenoj osobi, dok osoba koja je ispod njega nema pristup zapisu njoj nadređenoj osobi. **Sharing rules –** su iznimke gdje se mijenjaju zadane (engl. default) postavke kod Org-Wide defaults te se na taj način daje korisnicima veći pristup nad zapisima nego je to prvotno bilo podešeno. **Manual Sharing –** Omogućuje vlasnicima zapisa da daju dopuštenja za čitanje i izmjenu, korisnicima koji inače nemaju pristup nad tim podacima. To može biti korisno kada npr. regruter novih zaposlenika ode na godišnji odmor pa mora svoje ovlasti nad podacima dodijeliti nekoj drugoj osobi koja će ga mijenjati (Salesforce Security Guide, 2020).

Zapisi mogu biti postavljeni na: „**Private**“ gdje samo vlasnici zapisa i oni koji su po hijerarhiji na većoj razini od njega mogu pregledavati i mijenjati zapise, „**Public Read Only**“ gdje svi korisnici unutar kompanije imaju pristup gledanja zapisu, ali samo vlasnici i po hijerarhiji superiorniji korisnici imaju mogućnost modificiranja, „**Public Read/Write**“ gdje svi korisnici mogu modificirati i gledati zapise, te „**Controlled by Parent“** što znači da se nad nekim zapisom mogu vršiti određene radnje jer je taj zapis pod izravnom kontrolom, odnosno podređen nekom drugom zapisu. U konkretnom smislu, nad nekim zapisom koji je označen kao „dijete“ (engl. child), korisnik može npr. modificirati, brisati i gledati zapis, isto kao što ima i ovlasti nad zapisom koji je označen kao „roditelj“ (engl. parent), upravo zbog toga jer je zapis koji je označen kao „roditelj“ nadređen zapisu koji je označen kao „dijete“, korisnik može izvoditi iste radnje nad zapisom „dijete“ koje su postavljene i kod zapisa „roditelj“ (Sharma, 2020).

Slika 2. Dozvole nad podacima kod određenih objekata unutar Salesforce platforme (Izvor: vlastiti rad autora)



Gornja slika prikazuje dozvole nad podacima za određene objekte unutar Salesforce-a. „Default Internal Access“ određuje kako se zapisi dijele među internim korisnicima, dok „Default External Access“ kontrolira zadanu razinu pristupa koju vanjski korisnici (partneri i dobavljači) imaju nad zapisima i objektima. Uzmimo primjer kod „Opportunity“ gdje je „Org-Wide defaults“ postavljen na „Public Read/Write“ što znači da svi korisnici unutar kompanije mogu raditi sve radnje nad podacima koji su unutar tog objekta. Kod „Default External Access“ ta mogućnost nad podacima je ograničenija te je postavljena na „Private“. Ukoliko se npr. promijeni postavka sa „Public Read/Write“ na „Public Read Only“, korisnici neće više imati mogućnost uređivanja zapisa unutar objekta „Opportunity“, već će ga moći samo gledati. Također je vidljivo da je „Grant Access Using Hierarchies“ za sve objekte omogućen, što znači da svi oni korisnici koji imaju neki određeni pristup nad podacima, njihovi će nadređeni po hijerarhijskoj ljestvici također imati taj pristup. Može se zaključiti da se otvorenost nad zapisima unutar objekta povećava ovim redoslijedom postavki: Org-Wide defaults → Role hierarchies → Sharing rules → Manual Sharing.

Kod prijenosa podataka unutar Salesforce-a, platforma automatski vrši repliciranje podataka kako bi se osigurala njihova dostupnost u slučaju nekog incidenta gdje bi se izgubili podaci.

Također, platforma obavlja automatsko sigurnosno kopiranje podataka na zasebnu lokaciju u Salesforce oblaku za potrebe njihovog oporavka. Isto tako, korisnicima se pruža plan oporavka nad podacima ukoliko dođe do nekog incidenta (Perception Point, 2023).

3.2. Sudionici Salesforce platforme

Svijet je ušao u industrijsku revoluciju 4.0 koja se u mnogim slučajevima poistovjećuje sa digitalnom ekonomijom. Digitalna ekonomija označava nove modele poslovanja, proizvoda, usluga, tržišta i rastućih sektora koji su temeljeni na digitalnoj tehnologiji.[2] U takvom novom dobu, svijet se brzinski razvija pod utjecajem znanja, inovacija i informacija. Spremić (2017a) naglašava kako je razvoj novih digitalnih tehnologija (računalstva u oblaku, društvenih mreža, tehnologije velikih podataka, Interneta tvari (engl. Internet of Things, skraćenica IoT), 3D printera, robotike, virtualne stvarnosti, itd.) donio velike promjene u gotovo svim industrijama. Digitalne tehnologije imaju svrhu poboljšanja poslovanja i inovacija poslovnih modela. Pomoću interneta, nove tehnologije omogućile se ljudima lakše povezivanje po cijelome svijetu. U 2023. godini, procjenjuje se da u svijetu postoji više od 5 milijardi korisnika pametnih mobilnih uređaja, što je povećanje za 2 milijarde u odnosu na 2017. godinu kada je ukupno bilo nekih 3 milijarde korisnika pametnih mobilnih uređaja.[3] Spremić (2017a) dodaje kako se količina prenesenih podataka udvostručuje svakih 20 mjeseci pa je tako u 2021. godini stvoreno više podataka nego u prethodnih 5000 godina. Kompanije koje su uspješno implementirale nove trendove u doba digitalne ekonomije, značajno su unaprijedile iskustvo korištenja proizvoda i usluga od strane korisnika.

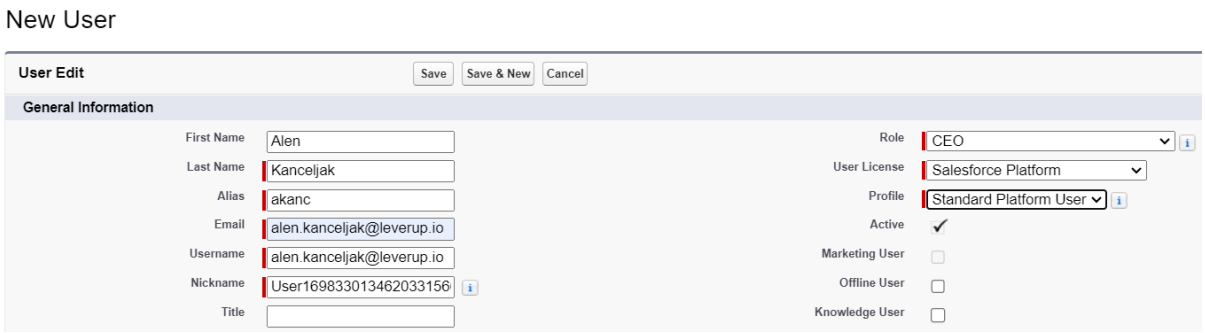
Jedna od kompanija koja je iskoristila nove digitalne trendove je Salesforce koja danas broji oko 150 tisuća korisnika diljem svijeta. Pošto se Salesforce koristi za poslovne svrhe kao što su: stvaranje potencijalnih klijenata, praćenje i analiziranje kupaca, personalizirani marketing, nuđenje podrške, itd., korisnici Salesforce-a u širem smislu su kompanije, pa se stoga može zaključiti da je 150 tisuća poprilično velik iznos korisnika. Kompanije koje koriste Salesforce su svih veličina s nekoliko desetaka zaposlenika pa sve do nekoliko tisuća zaposlenih bez obzira radi li se o javnim ili privatnim poduzećima. Neke od poznatijih kompanija koje koriste Salesforce su: Spotify, Walmart, Toyota, BMW, Amazon Web Services, U.S. Bank, L'Oreal Americas, American Express, T-Mobile, McDonald's, itd. Vidljivo je da kompanije dolaze iz

[2] Izvor: https://hr.theastrologypage.com/digital-economy [Pristupano 1. prosinca 2023].
[3] Izvor: https://www.oberlo.com/statistics/how-many-people-have-smartphones [Pristupano 1. prosinca 2023].

različitih grana industrije (Uslužna djelatnost – 34.3%, Financije – 15.5%, Maloprodaja – 13.9%, Transport – 13.6%, Proizvodnja – 11%, itd.) gdje više od 59% klijenata Salesforce-a dolazi iz Sjedinjenih Američkih Država (SAD) (Snisarenko, 2023).

Korisnik (engl. user) u užem smislu unutar neke kompanije je svatko tko se prijavi u Salesforce platformu. Korisnici su zaposlenici u kompaniji, kao što su npr: prodajni predstavnici, menadžeri, IT stručnjaci, itd., a koji trebaju pristup podacima u kompaniji. Korisnika u Salesforce platformi kreira *admin* (osoba sa najvišom razinom privilegija u sustavu) te mu on daje prava i ograničenja koja će imati nad podacima i značajkama koje Salesforce nudi. Prilikom kreiranja novog korisnika, *admin* upisuje osnovne podatke kao što su ime, prezime, korisničko ime, email, itd. Također mu postavlja i ograničenja nad podacima putem tzv. rola, korisnikove licence i korisnikovog profila. Role određuju što korisnici mogu vidjeti u Salesforce-u na temelju svojeg položaja u hijerarhiji. Korisnici na vrhu hijerarhije mogu vidjeti sve podatke u vlasništvu korisnika ispod njih, dok korisnici na nižim razinama ne mogu vidjeti podatke u vlasništvu korisnika iznad njih. Pa tako npr. CEO kompanije može vidjeti sve podatke koje i jedan prodajni predstavnik može vidjeti, dok prodajni predstavnik ima ograničenja nad podacima koje CEO može vidjeti. Nadalje, korisnička licenca određuje kojim značajkama korisnik može pristupiti u Salesforce-u pa se tako npr. korisniku može omogućiti da samo sudjeluje u razgovoru s drugim korisnicima bez da ima pristup ijednim drugim podacima. Profili određuju što korisnici mogu raditi i koje podatke mogu vidjeti unutar Salesforce-a. Oni mogu biti već zadani ili *admin* može kreirati potpuno novi profil sa ograničenjima nad podacima. Profil se daje korisniku prema poslovnoj funkciji koju ima unutar kompanije te se nikako ne preporuča davanje više pristupa korisniku nego što mu je potrebno za obavljanje posla jer može takve podatke zloupotrijebiti.

Slika 3. Kreiranje novog korisnika od strane administratora unutar Salesforce platforme (Izvor: vlastiti rad autora)



Sudionicima Salesforce platforme mogu se smatrati oni koji su na bilo koji način uključeni u proces poslovanja sa Salesforce-om. To su prije svega korisnici koji koriste usluge Salesforce-a i za koje njihova kompanija plaća mjesečni iznos kako bi koristili određene funkcionalnosti. Ovisno od kompanije do kompanije mogu postojati razni korisnici sa različitim funkcijama unutar Salesforce platforme. Pa tako mogu postojati marketinški odjeli koji će na temelju kupčeve interakcije odrediti da li je kupac vrijedan daljnjeg truda kompanije u slanju marketinških aktivnosti te da li je idealan da kupi proizvod, prodajni odjeli koji primaju od marketinškog odjela zainteresirane kupce prema kojima finaliziraju prodaju proizvoda, odjeli korisničke podrške i servisa koji će rješavati razne upite, probleme i slučajeve od strane kupaca, IT odjeli i administratori koji održavaju Salesforce platformu unutar kompanije te se brinu za njezinu sigurnost. Tu su i mnogi drugi odjeli poput poslovnih analitičara, programera, mobilnih korisnika, itd. Svi ti odjeli korisnika unutar platforme imaju određena prava nad podacima. Osim korisnika, sudionicima se mogu smatrati partneri i dobavljači koji posluju s kompanijom. Pa tako kompanija može proširiti pristup Salesforce-u svojim partnerima i dobavljačima radi suradnje i razmjene informacija. Naposljetku tu su i sami kupci kojima kompanija pruža svoje proizvode i usluge putem raznih marketinških aktivnosti. Kupci tako mogu imati razne upite i slučajeve koje kompanija treba riješiti ako želi povećavati svoju reputaciju.

Spremić, M. i Popovic, M. (2007) ističu kako menadžment organizacija koji koristi informacijske sustave treba biti svjestan sustavnog upravljanja rizicima povezanima s informacijskom tehnologijom (engl. information tehnology, u nastavku će se koristiti skraćenica IT). To uključuje ne samo tehničke ili operativne aspekte već i izvršne okvire poput upravljanja IT-om (engl. IT Governance) i revizije IT-a (IT Audit). Spremić, M. i Popovic, M.

(2007) naglašavaju kako se s IT rizicima ne bi trebali nositi samo IT odjeli već cjelokupna organizacija gdje upravni odbor i izvršni menadžment mora provoditi IT strategiju kako bi se upravljalo IT rizicima na učinkovit način.

Spremić (2013) pojašnjava važnost upravljanja informacijskom sigurnošću na razini izvršnog menadžmenta, a ne samo na razini odjela za informacijsku tehnologiju (IT). Upravljanje informacijskim sustavom (IS) je i dan danas dosta neučinkovito kod mnogih kompanija jer smatraju da je IS siguran ako su tehnološki dijelovi poput hardvera, algoritama, infrastruktura i drugih ostalih alata sigurni, pa stoga i stavljaju odgovornost samo na IT odjel da osigurava sigurnost kompanije. Negira se činjenica da se IS sastoji i od ostalih komponenta kao što su: ljudi, postupci, procesi i politika (Spremić, 2013).

Nadalje, Spremić i Šimunić (2018) istražuju zrelost sigurnosnih kontrola hrvatskih kompanija koje spadaju u tzv. kritičnu nacionalnu infrastrukturu. U provedenom ispitivanju zaključili su da su sigurnosne kontrole dosta učinkovite, no najveća slabost su bili zaposlenici koji nisu bili dovoljno upoznati s problemima kibernetičke sigurnosti te koji nisu bili dovoljno educirani za to područje, odnosno da nedostaje kompetentnih stručnjaka sa tehničkim vještinama koji bi se znali nositi ukoliko dođe do kibernetičkih napada. Isto tako, došli su do zaključka da je kibernetička sigurnost još uvijek isključiva odgovornost IT odjela, dok bi trebala biti odgovornost svakog zaposlenika koji se nalazi u kompaniji. Iz navedenog je vidljivo da korisnici igraju važnu ulogu u kompaniji te njihov manjak znanja i ne poznavanje kibernetičkih prijetnji mogu itekako naštetiti kompaniji.

3.3. Usklađenost Salesforce platforme s odredbama GDPR regulative i ostalim standardima

Napredna suvremena informacijska tehnologija omogućila je brz protok podataka i informacija zbog čega se morao promijeniti i pristup obrade osobnih podataka. Tu zato stupa na snagu Opća uredba o zaštiti podataka (engl. General Data Protection Regulation - GDPR) koja omogućuje jednaku zaštitu osobnih podataka fizičkih osoba koje se nalaze na prostoru Europske Unije (EU). GDPR jamči osobama sigurno upravljanje njihovim podacima. GDPR se primjenjuje u svim zemljama EU od 25. 05. 2018. godine te promiče važnost povjerenja između uključenih strana koji je ključan za razvoj digitalne ekonomije na prostoru EU (Vlada Republike Hrvatske, 2021).

Diligenski, Prlja i Cerović (2018) ističu „Direktiva o zaštiti podataka“ koja je poslužila kao baza za donošenje GDPR-a. „Direktiva o zaštiti podataka“ osnovana je 1995. godine te predstavlja zakon kojim se vjerovalo da se temeljna prava pojedinaca moraju zaštititi gdje su kompanije i vlade morali biti transparentni glede privatnih podataka koje procesuiraju. Stupanjem na snagu 2018. godine, GDPR-arova pravila su se uglavnom nadogradila u odnosu na „Direktiva o zaštiti podataka“. Neke od novih izmjena koje je doveo zakon GDPR su: Dobivanje privole od sudionika koja mora biti iskazana slobodnom voljom, davanje suglasnosti o dijeljenju podataka sa trećim stranama, ukoliko dođe do povrede podataka treba se u najkraćem mogućem roku obavijestiti osobu koja je dala svoje osobne podatke, organizacije koje trguju osjetljivim podacima moraju imenovati službenika za zaštitu podataka, kazne za kršenje zakona su mnogo veće nego su bile te mogu iznositi do 20 milijuna eura ili 4% ukupnog godišnjeg prihoda tvrtke (navedeno ovisi o ozbiljnosti kršenja zakona te nastale štete), brisanje svih podataka o osobi nakon prekida suradnje s kompanijom, suradnja organizacija s nadzornim tijelima oko prekogranične zaštite podataka, itd (EUR-Lex: EU law, 2016).

Koliko je poznato, Salesforce se drži svih prethodno navedenih pravila. Salesforce danas koriste brojne kompanije kao pomoć u poslovanju sa klijentima. Kompanije tako prikupljaju, pohranjuju i koriste osobne podatke rezidenata Europske Unije kako bi imale bolji uvid s kim posluju i na koji način nude svoje proizvode i usluge. Podatke poput imena, prezimena, adrese, godine starosti, spola, itd., stavljaju na Salesforce platformu kako bi lakše surađivali sa svojim klijentima. Na Salesforce-u je zatim da ima dobro postavljene zaštitne mehanizme koji će spriječiti krađu podataka. Upravljane podacima je jako velika odgovornost jer dospijećem takvih podataka u krive ruke ili zbog dijeljenja podataka sa krivim osobama, kompanije mogu biti izuzetno kažnjene od strane zakona iza kojeg stoji Europska Unija. Izuzetno je važno da osobe imaju povjerenje u kompaniju s kojom posluju jer ukoliko podaci korisnika „procure“, upitno je da li će i dalje htjeti surađivati s takvom kompanijom, što joj naposljetku može značajno narušiti reputaciju.

Proces prijenosa podataka unutar Salesforce-a koji se provodi u skladu sa GDPR-om ide sljedećim tijekom. U prijenosu podataka sudjeluju 3 entiteta, a to su osoba koja daje svoje podatke, kompanija koja pohranjuje te podatke, Salesforce u koji se unose podaci radi poboljšanja poslovanja kompanije. Kada osoba posjeti neku web stranicu te je zainteresirana za proizvod ili uslugu, ona popunjava formu na stranici kako bi se ulogirala. Ta stranica je u vlasništvu neke kompanije koja se bavi npr. prodajom laptopa. Ukoliko kompanija posluje u skladu sa GDPR-om, osoba je obavezna označiti polje sa privolom koja objašnjava na koji način

će se koristiti njezini podaci u marketinške svrhe kompanije. Kada osoba označi to polje sa GDPR-om i pošalje obrazac, podaci se šalju kompaniji koja dalje može upravljati podacima, ali pod uvjetom da se drži zakona o GDPR-u. Kompanija nikako ne smije raditi radnje s podacima koje nisu navedene u privoli. Isto tako kompanija ne smije skupljati podatke o osobi, a da nisu u skladu sa proizvodom ili uslugom koju nudi. Kompanija zatim manualno ili putem automatizacije prenosi podatke u Salesforce koji služi kao usluga kompaniji za lakše upravljanje podacima. U Salesforce-u se podešavaju ograničenja, odnosno koji ljudi unutar kompanije imaju pristup podacima o osobi koja se zanima za proizvod, u ovom slučaju je to laptop. Kompanija se na primjer ne mora baviti prodajom samo laptopa, već i na primjer prodajom usisavača, stoga je važno postaviti postavke unutar Salesforce-a, da korisnici koji su zaduženi za bavljenje aktivnostima vezanih za usisavač unutar platforme, nemaju pristup podacima o klijentima koji se zanimaju za laptop. Na taj način se unutar Salesforce-a štite podaci, kako ne bi došli u krive ruke.

Ukoliko kompanije u svojem poslovanju koriste Salesforce, one također moraju imati pisani ugovor sa Salesforce-om koji se odnosi na obradu podataka. Pošto je Salesforce neovisan o kompaniji, kompanija mora obavijestiti klijenta da će se njegovi podaci dijeliti sa Salesforce-om. GDPR-om se također preporuča da prilikom prijenosa podataka, podaci budu kriptirani kako hakeri ne bi zloupotrijebili takve podatke. Posebno je to važno kod kupovine nekog proizvoda ili usluge kada se unosi broj bankovne kartice (Salesforce, 2023a).

Usklađivanje s GDPR-om zahtijeva partnerstvo između Salesforce-a i njihovih korisnika. Da Salesforce brine o zaštiti podataka svojih korisnika, dokazuje i činjenica da imaju mnoge certifikate, odnosno sigurnosne potvrde temeljene na administrativnim, tehničkim i fizičkim mjerama zaštite korisnikovih osobnih podataka izdanih od europski zakonodavaca, tijela EU za zaštitu podataka i industrijskih udruženja. Salesforce (2023a) ističe neke od certifikata koji garantiraju sigurnost korištenja Salesforce-ovih usluga, a to su: ASIP Santé certification, Cloud Computing Compliance Controls Catalogue (C5) certification, Data Privacy Framework Certifications, HITRUST certification, ISO 27001/27017/27018 certification, Japan CS Gold certification, TRUSTe certification, itd. Tu je i usklađenost sa HIPAA regulacijom koja pruža saveznu zaštitu nad osobnim osjetljivim informacijama. Certifikati o sigurnosti korištenja Salesforce-a su dokazi o tome da je organizacija implementirala odgovarajuće sigurnosne prakse i standarde za zaštitu podataka i informacija koje se obrađuju putem Salesforce platforme. Salesforce pruža mnogo svojih usluga, a te usluge koje su u skladu sa raznim pravilima o sigurnosti i zaštiti podataka korisnika, imaju potvrdu od strane raznih certifikata

koji potvrđuju da su usluge sigurne za korištenje. Certifikati su važan alat za potvrdu sigurnosti, ali također je važno kontinuirano pratiti i ažurirati sigurnosne postavke kako bi se očuvala sigurnost podataka na Salesforce platformi (Salesforce, 2023a).

ISO 27001 – „Predstavlja minimalne zahtjeve i mjere koje organizacija treba poduzeti kako bi se uspostavio sustav upravljanja sigurnošću informacija (engl. information security management system, u nastavku će se koristiti skraćenica ISMS)“. ISO 27001 sadrži preporučene kontrole kako bi se sigurnosni rizik sveo na primjerenu razinu (Spremić, 2007). Međutim, „ISO 27001 standard ne daje točne informacije kako se mora razviti dokumentacija za ISMS (information security management system), koje kontrole moraju biti povezane s određenim poslovnim ulogama te kako se to može postići.“ (Beckers et al. navedeno u Hajdarević, Allen i Spremić, 2016). ISO 27017 - pruža smjernice o sigurnosti informacija za računalstvo u oblaku te preporučuje implementaciju kontrola sigurnosti informacija specifičnih za oblak. ISO 27018 - štiti privatnost za obradu osobnih podataka od strane pružatelja usluga u oblaku. (Salesforce.com, 2022.)

S podacima se treba postupati s velikom mjerom opreznosti. Uprava neke kompanije treba biti itekako osviještena oko mogućih prijetnji koje vrebaju u kibernetičkom prostoru. Isto tako treba educirati sve zaposlenike o svim mogućim kibernetičkim prijetnjama. GDPR je uveo tu dozu sigurnosti jer se kompanije sada moraju pridržavati propisanih pravila, što omogućuje klijentima da znaju na koji način se upravlja njihovim podacima.

4. Zaštita podataka i sigurnost prijave u Salesforce platformu

Da bi se moglo više govoriti o opasnostima koje vrebaju putem virtualnog prostora i načinima kako se zaštititi od takvih opasnosti, potrebno je razumjeti osnovne pojmove od kojih se sastoji cjelokupno digitalno okruženje. Spremić (2017b) navodi kako se informacijski sustav (IS) sastoji od niza komplementarnih komponenti poput: Hardware, Software, Dataware, Orgware, Lifeware i Netware, koji služe za obradu, pohranjivanje i distribuciju informacija te na taj način čine informacijsku strukturu poslovanja. Nadalje, Spremić (2017b) nabraja osnovne funkcije IS-a, a to su: provođenje i dokumentiranje poslovnih transakcija, pohrana podataka, izvještavanje o stanju poslovanja. Danas je teško ne biti meta hakerskim napadima, pogotovo ako kompanija dobro posluje. Informacijski sustavi i danas griješe i to na temelju: jako lošem upravljanju lozinkama, zastarjelom software-u, lošoj enkripciji podataka, premaloj svijesti zaposlenih o cyber sigurnosti, itd. Spremić (2017b) opisuje kibernetičku sigurnost kao sustav aktivnosti i mjera kojima se nastoje zaštititi podaci u kibernetičkom prostoru, dok je kibernetički prostor virtualni prostor unutar kojeg se odvija komunikacija između informacijskih i mrežnih sustava neovisno o tome jesu li povezani na internet. Hrvatska enciklopedija (2021) definira kibernetički prostor (engl. Cyberspace) kao cjeloviti informacijski prostor ostvaren globalno umreženim računalima. Za razliku od informacijske sigurnosti koja je tehnički orijentirana, kibernetička sigurnost uključuje tehnološke, organizacijske, društvene i ostale aspekte te se fokusira na specifične i visoko sofisticirane metode napada. Na taj način kibernetička sigurnost pruža višu razinu zrelosti i zaštitu od raznih kibernetičkih napada (Spremić, 2017b).

Spremić (2017a) u svojoj knjizi „Digitalna transformacija poslovanja“ ističe da su troškovi sigurnosnih incidenata i krađe podataka $ 1 trillion godišnje. Također, da se 100 milijardi spam poruka šalje svaki dan. Spremić (2017b) navodi da bi neki informacijski sustav (IS) bio kvalitetan, on mora imati kvalitetnu infrastrukturu (uređaji, računalna oprema, komunikacijska infrastruktura) i kvalitetan softver koji će omogućiti rad infrastrukture. Podaci trebaju biti dostupni, cjeloviti i sigurni. IS treba omogućiti učinkovitost kod poslovanja i transakcija te također treba biti jednostavan za korištenje od strane korisnika (user-friendly). (ISACA, 2015. navedeno u Spremić, 2017a) ističe da se 97% cyber napada moglo izbjeći da su kompanije imale učinkovitije sustave zaštite. Također, 6 od 10 zaposlenika između 18-35 godina koristi osobni uređaj za posao s kojim se spaja na mrežu organizacije, a koji može biti zaražen nekim zloćudnim programom. Hajdarević, Allen i Spremić (2016) ističu dodatni problem s kojim se

današnje kompanije suočavaju, a to je što zaposlenici dovode svoje vlastite uređaje na posao kako bi mogli obavljati razne aktivnosti (engl. Bring Your Own Device - BYOD). Na taj način se spajaju na mrežu te mogu predstavljati rizik za kompaniju. Kompanija bi trebala implementirati i održavati najbolje prakse i standarde kako bi informacije ostale sigurne. Hajdarević, Allen i Spremić (2016) naglašavaju sigurnosne mehanizme koji se temelje na ISO 27000 međunarodnim standardima koji govore kako se zaštititi od pokušaja krađe informacija od uređaja koji su spojeni na organizacijsku mrežu.

Spremić (2017b) ističe 3 temeljna parametra putem kojih se štite informacije i informacijski sustavi, a to su: Povjerljivost – zaštita resursa od neovlaštenog pristupa, Integritet – zaštita cjelovitosti i ispravnosti podataka u prijenosu i mirovanju, Raspoloživost – omogućavanje stalnog i pravodobnog pristupa informacijama i informacijskom sustavu ovlaštenim osobama. Da bi se zaštitila povjerljivost podataka, potrebno je postaviti mjere zaštite kao što su identifikacija i autorizacija korisnika. Kod zaštite integriteta podataka, treba kriptirati povjerljive podatke te primijeniti sigurnosne protokole. Dok se kod zaštite raspoloživosti podataka treba prije svega omogućiti dostupnost sustava koji će biti u funkciji ako se dogodi napad na IS te također unutar sustava moraju postojati metode oporavka poslovanja (Spremić, 2017b).

Szombathelyi (2021) naglašava kako se cyber stručnjaci za sigurnost IS-a drže koncepata kao što su: autentifikacija, autentičnost, autorizacija i odbijanje. Ti koncepti predstavljaju sigurnosni stup informacijskog sustava te ako bilo koji od ovih koncepata napadač probije, informacijski sustav će pasti. Autentifikacija provjerava da li je neka osoba stvarno osoba kakvom se predstavlja. Autentičnost osobe se provjerava na temelju zaporke, pitanja na koja samo ovlaštena osoba zna odgovor, višefazne provjere autentičnosti, itd. Autorizacijom se daju dopuštenja koja korisnik ima kada se ulogira u sustav. Odbijanje predstavlja jamstvo korisnika da ne može poreći podrijetlo, valjanost ili cjelovitost nečega, npr. podataka ili informacija. Uz navedene koncepte, Szombathelyi (2021) ističe i tri dodatna koncepta, poznatijih kao CIA-ina trijada koje se također stručnjaci za kibernetičku sigurnost drže. CIA-ina trijada se sastoji od: povjerljivosti, integriteta i dostupnosti nad podacima i informacijama. Povjerljivost znači da se podaci ili informacije ne bi smjele objavljivati nekoj trećoj, neovlaštenoj strani. Dakle, npr. korisnik C ne smije imati pristup informacijama bez privole korisnika A. Integritet znači logičku cjelovitost hardvera i softvera koji ne smiju imati neku slabost koju bi mogao iskoristiti cyber napadač i time nanijeti štetu podacima. Dostupnost sustava je koncept koji označuje da je nešto pravovremeno i pouzdano. Najpoznatiji napad na dostupnost je DDoS napad. Dakle,

sustav treba uvijek biti dostupan kako bi korisnici imali pristup uslugama bilo na web stranicama, e-pošti, ili bankovnim uslugama (Szombathelyi, 2021).

Salesforce je platforma koja surađuje s aplikacijama trećih strana. Platforma uz svoju sigurnost pruža različite aplikacije za podršku osiguravanju sigurnosti. Unutar Salesforce-a postoji tržnica gdje se mogu preuzeti razne aplikacije koje koštaju ili su besplatne („AppExchange"). Pa tako trenutno postoji 1127 aplikacija na tržištu spremnih za preuzimanje, a koje pružaju dodatnu sigurnost u korištenju Salesforce platforme. Dakle, korisnici mogu dodatno zaštititi svoje podatke instaliranjem takvih aplikacija koje se zatim koriste unutar Salesforce platforme (Jallow, 2022). Sigurnost Salesforce-a je uspostavljena samo ako se pružatelj platforme (Salesforce) i pružatelj aplikacije obvezuju na sigurnost informacija te na stvaranje potrebne sigurnosne mjere opreza. Za takvo što, bitno je da je integracija između Salesforce - a i drugih aplikacija ispravno podešena i u skladu sa ostalim zakonodavnim aktima kako ne bi došlo do povrede privatnosti podataka. Stoga, pružatelji aplikacija trebaju izraditi sigurne aplikacije pravilnom upotrebom značajki platforme Salesforce-a (Soni & Vala 2017 navedeno u Jallow, 2022).

Integracija služi za povezivanje i razmjenu informacija između dva ili više odvojena sustava, u ovom slučaju Salesforce-a i neke druge aplikacije. Tako npr. Salesforce može služiti kao sustav za pohranu podataka, drugi sustav za obradu informacija, a treći sustav za kreiranje vizualnih izvješća i grafova. Kada se spoje ta tri sustava, vrijednost informacija raste. Informacije postaju više iskorištenije i dostupnije te se na taj način štedi dosta manualnog rada koji može biti iskorišten negdje drugdje na nekom drugom području. Kod povezivanja sustava, moraju se poštivati razni standardi kako bi povezivanje bilo uspješno i zaštićeno. Takvi standardi su ISO standardi, poput: ISO 27001 i ISO 9000 koji opisuju kako kreirati visoko kvalitetan i siguran softver, ISO 15926, ISO 55000 i ISO 14224 koji pružaju bitne informacije za stvaranje integracije zbog njihova fokusa na upravljanje imovinom, podacima i informacijama (Tähtinen 2005, navedeno u Jallow, 2022).

(Johan i Ahmad, 2023) naglašavaju da Salesforce broji sve više i više korisnika, pa je stoga potreba za snažnim sigurnosnim mjerama kako bi se zaštitili osjetljivi podaci postala od izuzetne važnosti Salesforce-u. Ističu kako zaštita podataka zahtijeva kombinaciju tehničkih sigurnosnih mjera i najbolje prakse te kako se sigurnost Salesforce-a sastoji od niza sigurnosnih mjera.

Salesforce već ima ugrađene sigurnosne mjere u platformu koje automatski štite od raznih prijetnji, bilo unutarnjih ili vanjskih. Takve mjere su: pružanje backup opcije, repliciranje podataka i oporavak od katastrofe, sigurnost mreže gdje se kriptiraju podaci u prijenosu i otkrivaju napredne prijetnje, ograničenje pristupa korisnika kroz objekte, zapise i polja, sharing model (Wayburn, 2023). Također, Salesforce nudi dodatne sigurnosne mjere koje administrator mora podesiti unutar platforme, a to su: višestruka provjera autentičnosti (engl. multi-factor authentication, u nastavku će se koristiti skraćenica MFA), ograničenje pristupa putem IP raspona, podešavanje profila (engl. profiles) i dozvola (engl. permission sets), upravljanje lozinkama, podešavanje broja neuspjelih prijava u sustav i „Salesforce Shield" (Padmanabhan, 2021). Važno je naglasiti da su takve mjere jako važne u prevenciji od raznih napada te ih je potrebno podesiti unutar platforme. Ipak takve mjere neće moći zaštiti kompaniju jedanput kada malware zahvati i uđe u sustav i to najčešće korisnikovom greškom kada klikne na neki link ili dokument koji je zaražen virusom. Salesforce-ove razne značajke omogućuju korisnicima komunikaciju s raznim dobavljačima, partnerima, klijentima, itd., gdje možda neka osoba poželi naštetiti kompaniji. Stoga je važno uz sve navedene preventivne mjere, imati instaliran antivirusni program koji će skenirati sve linkove i dokumente koji se pojave u Salesforce instanci te će tako na vrijeme otkriti da li je neka kompanija zahvaćena nekim zlćudnim programom (Wayburn, 2023).

4.1. Arhitektura zaštite podataka u Salesforce-u

Arhitektura osigurava povjerljivost, dostupnost i cjelovitost podataka pohranjenih na platformi. Njom se nastoji zaštititi kompaniju od neovlaštenih pristupa, povrede podataka i napada zlonamjernim softverom (malware). Sastoji se od 3 sloja: fizičkog sloja, mrežnog sloja, i aplikacijskog sloja. Fizički sloj uključuje fizičke sigurnosne mjere kao što su; biometrijske kontrole pristupa, video nadzor i ograda, sve kako bi se zaštitio podatkovni centar Salesforce-a i time spriječio neovlašten pristup. Mrežni sloj štiti od vanjskih prijetnji, a uključuje postavljanje vatrozida, sustava za otkrivanje i sprječavanje upada te kontinuirano praćenje mrežnog prometa. Aplikacijski sloj uključuje kontrole pristupa, mehanizme provjere autentičnosti i druge sigurnosne značajke koje štite od prijetnji poput: cross-site scripting(XSS), SQL injection i phishing (Johan i Ahmad, 2023).

4.1.1. Fizički sloj

Prvo pravilo sigurnosti je fizička zaštita sustava i mreže. Sustavi, mediji i komunikacijska oprema trebali bi biti smješteni u nekom sigurnom objektu. Serveri, usmjerivači, sigurnosne kopije i sva ostala oprema trebala bi se držati u sigurnim prostorijama koje su dostupne samo ovlaštenim osobama. Osim moguće nastale štete ljudskim činom, štete za poslovanje mogu nastati putem prirodnih sila: potresa, požara, poplava, itd., stoga kompanije moraju uzeti u obzir te naći načine na koje će zaštititi svoje podatkovne centre od takvih prirodnih katastrofa (Canavan, n.d.). Pravilno planiranje može itekako ublažiti posljedice od mogućih prirodnih katastrofa. Tako se npr. organizacije mogu zaštiti od potresa tako da bolje učvrste svoju opremu u zgradama kako se ne bi lagano polomila ili da se izgrade bolji temelji kod zgrada. U slučaju požara podatkovni centri trebaju imati protupožarne alate koji bi odmah upozorili na prijetnju, dok kod mogućih poplava, kompanije ne bi trebale smjestiti svoja računala i opreme u podrum zgrade. (Canavan, n.d.). Jedan takav primjer dolazi iz Hrvatske kada je zaposlenik Hrvatske kontrole zračne plovidbe (HKZP) u panici zbog nevremena i prodora vode u zgradu, isključio glavno napajanje, dok je nad Hrvatskom bilo više od stotinu zrakoplova. Naime, namjera zaposlenika bila je da spasi uređaje koji su se nalazili u prostoriji u koju je počela ulaziti voda jer da je voda ušla do takvih uređaja, došlo bi do kratkog spoja te bi vjerojatno nastupila još i veća tragedija (Marinović, 2014). Stoga je nužno da organizacija postavi svoje sofisticirane uređaje na neko više mjesto kako se ubuduće ne bi događali takvi incidenti.

Salesforce ulaže znatne napore kako bi zaštitio svoje podatke na razini fizičke sigurnosti. Mjere su usmjerene na zaštitu hardverske infrastrukture i fizičkog okruženja u kojem su podaci pohranjeni te kako bi se mogle pružati usluge. Salesforce ima brojne podatkovne centre diljem svijeta koji su opremljeni sigurnosnim tehnologijama poput biometrijskim kontrolama pristupa, nadziranog prostora video kamerama i ogradama kako bi se spriječili fizički pristupi neidentificiranih osoba u podatkovne centre. Podatkovni centri su također dobro osigurani od prirodnih katastrofa poput poplava, potresa, požara itd., sve u namjeri kako bi podaci ostali zaštićeni. Salesforce-ovi podatkovni centri su skloni korištenju redundantnoj infrastrukturi, što bi značilo da ukoliko npr. dođe do nestanka struje, koristili bi rezervni sustav napajanja kako bi se promet podataka nastavio odvijati. Pridaju se i veliki napori u obuci radne snage kako bi znali kako postupati u nekoj prijetećoj situaciji. Takvu sigurnost pružanja fizičke zaštite potvrđuju i razni certifikati i dokumenti poput „Dokumenta politike sigurnosti“ (DSP) koji

potvrđuju da je Salesforce usklađen sa standardima i regulativama (The Complete Guide to Salesforce Data Security - Keeping Salesforce Data Safe, n.d.).

4.1.2. Mrežni sloj

Sigurnost mreže se odnosi na zaštitu tvrtkine imovine od strane raznih prijetnji koje dolaze od interneta. Informacije trebaju biti povjerljive, što znači da neovlašteni korisnici ne smiju biti u mogućnosti presretati, kopirati ili replicirati osjetljive informacije. Također je nužan integritet informacija tako da organizacije imaju dovoljno povjerenja u točnost informacija. Isto tako je bitna i mogućnost dohvaćanja podataka u bilo kojem trenutku kao i postavljanje kontrole identifikacije kako bi se utvrdio da li je korisnik ovlašten za pristup (Canavan, n.d.). Nijedna kompanija nije apsolutno zaštićena od vanjskih prijetnji, neke su manje, a neke više zaštićene. Sve ovisi o osviještenosti shvaćanja takvog problema od strane organizacije te spremnost na veća ulaganja u sigurnost informacijskog sustava. Bitno je naglasiti da zaštita imovine nije samo zaštita od vanjskih napadača, već i zaštita od osoblja koje radi za organizaciju (Canavan, n.d.).

Spremić (2017a) opisuje mrežu kao tip imovine putem koje se ostvaruje komunikacija i razmjena sadržaja između dva ili više elektroničkih uređaja na udaljenim lokacijama s ciljem razmjene podataka, a ostvaruje se fizičkom vezom (kabel) ili bežičnim pristupom (WiFi). Funkcionira na način da klijentsko računalo traži neku informaciju, koje mu zatim server (poslužitelj), tražeći u svoju bazu podataka, pruži takvu informaciju koja se zatim pojavljuje na klijentskom računalu. Komunikacija se odvija tako da svako računalo ima IP adresu na koju se šalju poruke dijeleći se u pakete koji omogućuje TCP protokol (Transmission Control Protocol). Spremić (2017a) ističe da računalne mreže putem kojih se razmjenjuju podaci i informacije mogu biti intranet, ekstranet i internet. Intranet je privatna računalna mreža koja omogućuje pristup informacijama i komunikaciju unutar tvrtke. Ekstranetom se povezuju više nezavisnih privatnih mreža u sustav pa tako kompanija može komunicirati s raznim dobavljačima, bankama, kartičnim institucijama, pružateljima logističkih usluga, itd., pod uvjetom da ima povjerenja u svoje partnere koji ne bi zlouporabili podatke. Internet pruža razmjenu podataka i komunikaciju između računala i uređaja diljem svijeta koji su povezani putem različitih komunikacijskih tehnologija poput: okosnice, usmjernika, pristupnika, WiFi-ja, itd (Spremić, 2017a).

Mjere opreza koje koristi Salesforce, a koje se odnose na sigurnost mreže su: Vatrozid (engl. firewall), dopušteni raspon IP adresa (engl. Trusted IP Range Edit), postavke sati prijave (engl. Login Hours), enkripcija podataka putem SSL/TLS protokola te „Salesforce Shield Platform Encryption“.

Informacije i sadržaji koji dolaze putem interneta ili drugih nepovjerljivih lokalnih mreža moraju biti provjereni prije nego dođu na lokalnu mrežu. To omogućuje vatrozid koji predstavlja barijeru između 2 mreže te na taj način ograničava slobodan protok podataka iznutra i izvana (Bellovin i Cheswick, 1994). Spremić (2017a) objašnjava da vatrozid analizira podatkovne pakete i provjerava po zadanim pravilima smije li podatkovni paket ili ne u mrežu te da je na vlasniku lokalne mreže da konfigurira koje pakete će propuštati sa globalne ili neke druge lokalne mreže. Vatrozid stoga može značajno povećati računalnu sigurnost. Bellovin i Cheswick (1994) dodatno ističu kako vatrozid može biti implementiran u hardver, softver ili kao kombinacija i hardvera i softvera. Sav promet mora proći kroz vatrozid ukoliko kompanija želi imati sigurnu računalnu mrežu. Nadalje, samo ovlašteni promet, kako je definirano lokalnom sigurnosnom politikom, je dopušten proći kroz vatrozid. Osim prijetnji koje dolaze putem interneta, napadači su također skloni napasti organizaciju iznutra (Bellovin i Cheswick, 1994).

Generirajući sigurnosnu kopiju podataka na tjednoj ili mjesečnoj bazi, Salesforce omogućuje korisnicima da izvade sve podatke unutar svoje organizacije u obliku CSV datoteke, tako da ukoliko podaci i budu kompromitirani, podaci u kompaniji neće biti zauvijek izgubljeni. (Salesforce, 2023b). Salesforce koristi vatrozid kako bi spriječio moguće prijetnje ili upad neovlaštenih korisnika. Jedan od vatrozida koji koristi je Web application firewall (WAF) koji filtrira i nadzire HTTP/s promet između web aplikacije i interneta. Funkcije WAF-a unutar Salesforce-a su da provjerava adrese web stranica (URL) kako bi otkrio nešto neobično, filtrira zlonamjerni promet koji pokušava iskoristiti određene ranjivosti aplikacije te sprječava da zlonamjerne prijetnje iskoriste ranjivosti koda. [4]

Za razliku od identifikacije i autorizacije koje određuju tko se od korisnika može prijaviti, mrežna sigurnosna ograničenja limitiraju otkuda se korisnici mogu sve prijaviti i kada se mogu prijaviti. Za takvo nešto su zaslužne opcije „Trusted IP Range Edit“ i „Login Hours“ unutar Salesforcea (Salesforce Security Guide, 2020).

Dopušteni raspon IP adresa (engl. Trusted IP Range Edit) dopušta pristup instanci Salesforce-a samo onim korisnicima koji su unutar dozvoljene granice IP adresa. Prvi puta kada se korisnik prijavi u Salesforce instancu, IP adresa se pohranjuje na pregledniku od korisnika. Kada se

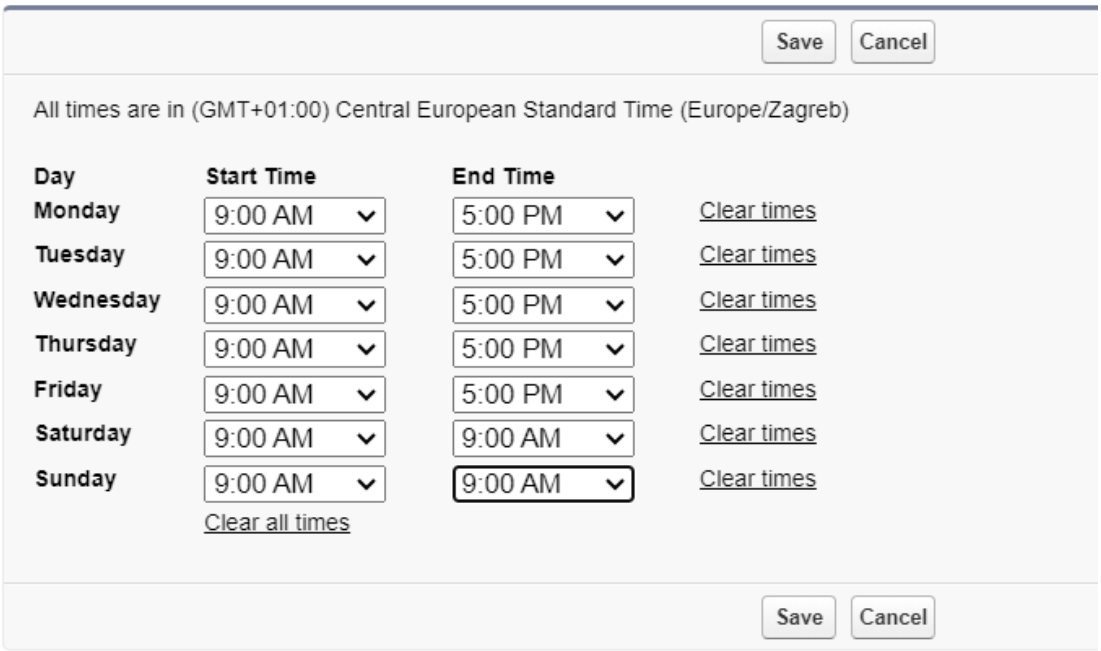
[4] Izvor: https://help.salesforce.com/s/articleView?id=cc.b2c_waf_protection.htm&type=5 [Pristupano 10.studenoga 2023].

korisnik istim korisničkim imenom i lozinkom prijavljuje s drugog uređaja koji ima drugu IP adresu, sustav će tražiti unos kontrolnog koda kako bi provjerio da se radi o pravom korisniku. Administrator može podesiti da u postavkama definira raspon IP adresa, omogućujući tako da sustav neće tražiti kontrolni kod od onih korisnika koji su u tom rasponu (Sharma, 2020).

Slika 4. Opcija raspona IP adresa (Izvor: vlastiti rad autora)

Opcija „Login Hours“ dopušta administratorima konfiguraciju da zaposlenici kompanije imaju pristup sustavu samo u radnom vremenu, npr. od 9 do 17 sati. Nakon toga se sustav zaključava te oni više nemaju pristupa do idućeg radnog dana u tjednu (Sharma, 2020).

Slika 5. Sati prijave u sustav (engl. Login Hours) (Izvor: vlastiti rad autora)

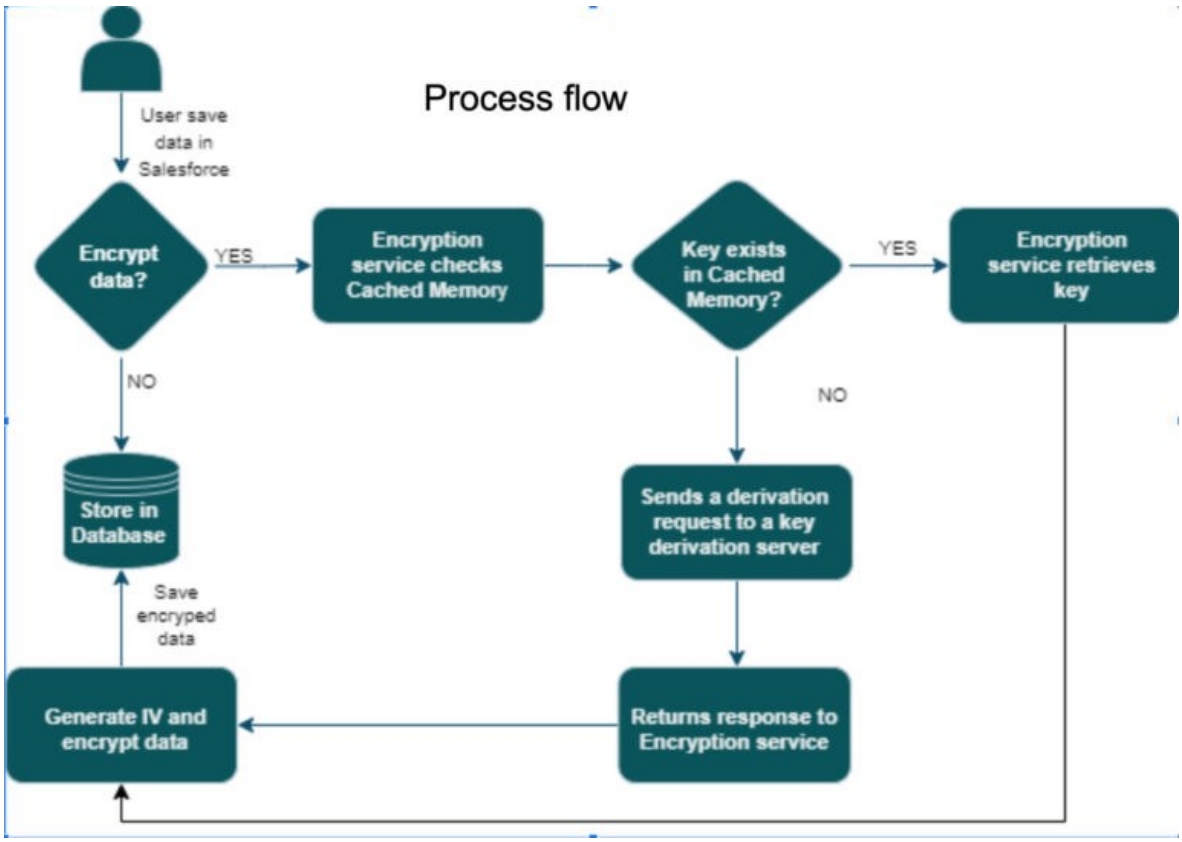


Salesforce osigurava sigurnost podataka njihovom enkripcijom u tranzitu i mirovanju putem SSL/TLS protokola. Salesforce koristi naprednu tehnologiju poput Sigurnosti transportnog sloja (engl. Transport Layer Security, u nastavku će se koristiti skraćenica TLS) koji se često naziva i Sloj sigurnih utičnica (engl. Secure Sockets Layer, skraćenica SSL). To je protokol koji štiti podatke korisnika pomoću provjere autentičnosti poslužitelja i enkripcije podataka, što

dokazuje i mala ikonica lokota na web mjestu koja znači da je uspostavljena veza sa Salesforce poslužiteljem sigurna (Salesforce, 2023b). TLS protokol omogućuje da klijent/poslužitelj aplikacije budu sigurne te da komuniciraju na način na koji ih se ne može prisluškivati. Protokol je dizajniran za autentifikaciju poslužitelja. Isto tako, TLS zahtijeva pouzdan transportni protokol kao što je TCP protokol kako bi se prenosili i primili podaci. Svi podaci koji se šalju ili primaju su šifrirani te se zaštitna veza uspostavlja prije slanja ili primanja poruke (Hickman, 1994). Proces se može opisati na način da se na poslužiteljskoj razini prima poruka → rastavljanje → dodavanje kontrolnog broja → kriptiranje → komprimiranje, pošiljanje, dok se na klijentskoj razini primaju dijelovi → dekomprimira → dekriptira → provjeravaju kontrolni brojevi → sastavlja poruku → predaje poslužiteljskoj razini (Spremić, 2017a).

Salesforce koristi vlastitu lokalnu uslugu pristupnika za kriptiranje kao što je „Salesforce Shield Platform Encryption“. Ovakav mehanizam kriptiranja omogućuje šifriranje osjetljivih podataka dok miruju i dok se prenose mrežom na temelju čega se stvara dodatan sloj zaštite nad podacima, a kompanija se pouzdano pridržava regulatornih zahtjeva i pravila privatnosti. Za razliku od klasične enkripcije koja omogućuje zaštitu samo posebne vrste prilagođenog tekstualnog polja, „Salesforce Shield Platform Encryption“ omogućuje šifriranje polja u Salesforce-u, ali i šifriranje datoteka i privitaka tako da samo ovlaštene osobe mogu pristupiti takvim podacima. „Salesforce Shield Platform Encryption“ je dodatna značajka unutar Salesforce-a koju mora omogućiti tehnički osposobljeno osoblje unutar neke kompanije (Salesforce, 2023c).

Slika 6. Tijek procesa kod Salesforce Shield Platform Encryption (Chaudhary, 2022).



Slika iznad prikazuje proces kriptiranja podataka putem „Shield Platform Encryption“. Dakle, kada korisnici promijene neku vrijednost u polju ili prenesu neke datoteke, slike ili privitke na platformu, takvi podaci se spremaju u bazu podataka u Salesforce-u. Kompanija može odabrati da Salesforce generira ključ za kompaniju ili kompanija može učitati svoj vlastiti ključ. Usluga od strane Salesforce-a koja kriptira podatke provjerava predmemoriju te ako ključ za šifriranje (engl. encryption key) postoji u predmemoriji, onda ta usluga koja kriptira dohvaća encryption key te kriptira podatke. Na taj način ključ već postoji izvan Salesforce-a te je on potreban da bi se podaci dekriptirali kada ovlašteni korisnici trebaju pristup takvim podacima. Ukoliko ključ za kriptiranje podataka ne postoji u predmemoriji, šalje se zahtjev za derivaciju ključa derivacijskom poslužitelju koji zatim generira ključ i kriptira podatke unutar Salesforce-a.

Enkripcijom podataka, ukoliko se hakeri domognu osjetljivih podataka, oni neće moći pronaći smisao tih podataka jer nisu pisani jezikom koji je razumljiv. To može pomoći u zaštiti osjetljivih podataka od neovlaštenog pristupa korisnika koji ne smiju vidjeti takve podatke.

4.1.3. Aplikacijski sloj

Kontrole sprječavaju, otkrivaju i ispravljaju neželjeni događaj. Česta je pogreška što kompanije smatraju informacijski sustav odvojenim od ukupnog organizacijskog sustava unutarnjih kontrola. Spremić (2007) objašnjava kako menadžment kompanije treba surađivati sa menadžmentom informacijskog sustava kako bi se provele, oblikovale i ocijenila efikasnost sustava internih kontrola unutar IS-a. Također, Spremić (2007) ističe da postoji mnogo vrsta kontrola koje se dijele prema različitim kriterijima te da su neke od vrsta kontrola: upravljačke, procesne, opće, aplikacijske, preventivne, detektivne, korektivne, itd. Provedbom takvih kontrola, IS neke kompanije biti će puno sigurniji od neovlaštenih upada. Kontrole se mogu razvrstati i prema okvirima i normama poput CobiT i ISO 27001. Pa tako npr. CobiT propisuje 6 procesnih i 18 aplikacijskih kontrola (Spremić, 2007).

Administratori unutar Salesforce-a osiguravaju da samo ovlašteni korisnici imaju pristup osjetljivim podacima. Mehanizmi kontrola pristupa koje platforma pruža su: korisnički profili (user profiles), uloge korisnika (roles) i skupovi dopuštenja (engl. permission sets). Korisničkim profilima se definira osnovni pristup nad podacima koje imaju korisnici. Ulogama se određuje razina pristupa nad zapisima, dok se skupovima dopuštenja dodjeljuju dodatna dopuštenja korisnicima bez obzira na ono što je definirano u korisnikovom profilu i ulogom (Jahan i Ahmad, 2023).

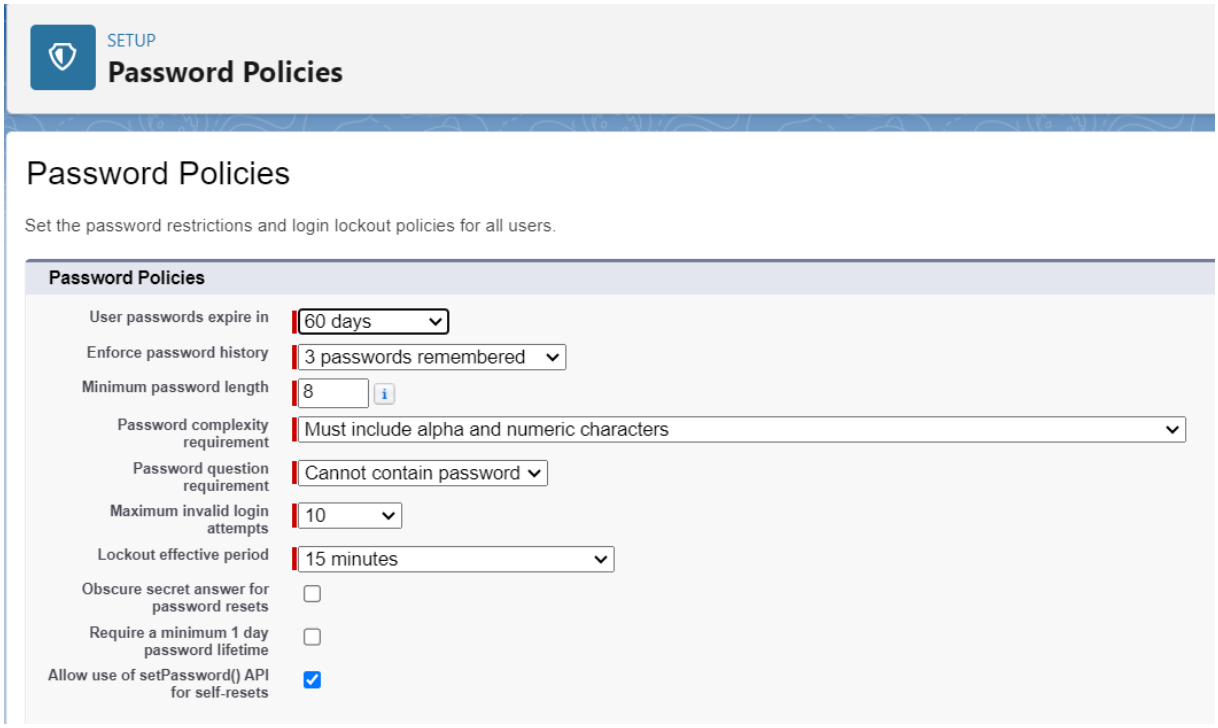
Mehanizmi provjere autentičnosti predstavljaju način na koji će Salesforce prepoznati da se radi o pravom i ovlaštenom korisniku prilikom ulogiravanja u Salesforce platformu. Jahan i Ahmad (2023) nabrajaju načine identifikacije koje platforma zahtijeva, a to su: osnovni mehanizam provjere autentičnosti kao što su lozinka i korisničko ime, jedinstvena prijava (engl. single sign-on, u nastavku će se koristiti skraćenica SSO) koja omogućuje da se svojom lozinkom i korisničkim imenom od Salesforce-a, prijavljuje i u ostale alate koje pruža Salesforce, bez ponovnog upisa lozinke i korisničkog imena, zatim multi-factor authentication (MFA) gdje *admin* može podesiti da se kod ulogiravanja korisnika zahtijeva dodatna informacija kako bi se sa većom sigurnošću moglo utvrditi da se radi o ovlaštenom korisniku. To se uz korisničko ime i lozinku kao osnovne provjere identifikacije, postiže jednokratnom lozinkom (engl. one-time password, u nastavku će se koristiti skraćenica OTP) ili biometrijskom identifikacijom. (Jahan i Ahmad, 2023).

Kod identifikacije i autorizacije korisnika samo ovlašteni korisnici imaju pravo ulaska u informacijski sustav. Neovlaštene osobe bi se pravim mjerama zaštite trebale na vrijeme otkriti te im se onemogućiti pristup u sustav. Upravo je identifikacija jedna od ključnih kontrola koje sprječavaju neovlašteni pristup IS-u. Identifikacija korisnika je postupak provjere korisnika od strane sustava, odnosno da li je korisnik osoba kojom se predstavlja.[5] Kako navodi Spremić (2017b), identifikacija korisnika se može ostvariti na 3 načina. To su: fizička identifikacija, logička identifikacija i biometrijska identifikacija. Fizičkom identifikacijom se provjerava identitet korisnika na temelju nekog predmeta (osobna karta, pametna kartica, token, ključ, identifikacijska kartica, itd.). Logička identifikacija se zasniva na nečemu što bi korisnik trebao znati, poput: lozinke, ključa, identifikacijskog ključa, osobnog identifikacijskog broja (PIN), korisničkog imena, ključne riječi, itd. Naposljetku, biometrijskom se identifikacijom provjerava različitost i jedinstvenost korisnika u odnosu na ostale osobe (otisak prsta, glas, sliku očne šarenice, DNK karakteristiku, itd.) (Spremić, 2017b).

Valja naglasiti da je na kompaniji da odredi koje će kriterije postaviti pri identifikaciji korisnika. Pa tako može osigurati da lozinke od korisnika budu čvrste i sigurne. Neke od opcija koje se mogu postaviti su: da se lozinka mora promijeniti nakon određenog perioda, kompleksnost znakova, dužina lozinke, na koliko vremena se onemogućuje ulaz u sustav ako je korisnik prekoračio dozvoljen ponovljeni upis lozinke, itd (Sharma, 2020).

[5] Izvor: https://www.indicative.com/resource/user-identification-user/ [Pristupano 6. prosinca 2023].

Slika 7. Politika lozinki (Izvor: vlastiti rad autora)



Slika iznad prikazuje da su postavke lozinke podešene da: valjanost lozinke ističe nakon 60 dana što znači da će se nakon isteka tog vremenskog perioda lozinka morati mijenjati, sustav neće dopustiti promjenu lozinke u prethodne 3 lozinke, minimalna duljina lozinke je podešena na 8 znakova, kompleksnost lozinke zahtijeva unos velikog slova i broja, maksimalan broj pokušaja ulaska u sustav je 10 puta nakon čega će se sustav zaključati na 15 minuta nakon čega će korisnik ponovno dobiti mogućnost pokušaja ulaska u sustav.

Uz sigurnost koju pruža Salesforce, kompanija mora odrediti unutar svoje organizacije tko će i na koji način koristiti podatke. Autorizacija je proces davanja i oduzimanja privilegija korisnicima za pristup određenim resursima, podacima ili uslugama (Griftiths i Wade. 1976 navedeno u Fagin, 1978). Ključna je za osiguravanje sigurnosti i integriteta podataka u mnogim sustavima i aplikacijama. Ovlaštenje se primjenjuje u različitim sektorima, poput: informacijske tehnologije, financije, zdravstvo i itd. Autorizacija se često provodi nakon identifikacije korisnika, gdje se korisnik prvo identificira, a zatim se provjerava jesu li mu dodijeljene ovlasti za pristup resursima (Okta, 2023).

Za poduzeća je važno da osiguraju da je njihova Salesforce instanca sigurna. Osim postojećih sigurnosnih mjera, u Salesforce-u se mogu podesiti dodatne sigurnosti, poput: dvofaktorska provjera autentičnosti (engl. two-factor authentication, u nastavku će se koristiti skraćenica

2FA), My domain i single sign-on (SSO). Navedeno su dodatne mjere zaštite koje bi svako poduzeće trebalo koristiti kako bi osiguralo sigurnost prijave na svoju Salesforce instancu. (Soni & Vala 2017 navedeno u Jallow, 2022).

Salesforce-u je osim važnosti pružanja sigurnosti kod identifikacije korisnika, bitna i jednostavnost kojom će se korisnici prijavljivati u platformu. Ovo su glavne značajke koje Salesforce pruža kod identifikacije: Single Sign-On (SSO), Social Sign-On, Multi-Factor Authentication (MFA) i My Domain.

SSO omogućuje korisnicima pristup svim ovlaštenim resursima bez prijavljivanja zasebno na svaki od njih. Na taj način korisnici jednom kada su se prijavili na svoju Salesforce instancu, mogu pristupiti ostalim aplikacijama s kojima je Salesforce instanca povezana i konfigurirana. Tako se korisnik automatski može povezati na aplikacije poput npr. Google Apps i Microsoft Office 365 bez da ponovno unosi svoje korisničko ime i lozinku (Salesforce Security Guide, 2020).

Kod prijave putem društvenih mreža (engl. Social Sign-On) korisnici mogu ući u svoju Salesforce instancu koristeći podatke za prijavu od vanjskih aplikacija kao što su: Google, PayPal, LinkedIn, Facebook, Twitter, Amazon, itd. Pa tako umjesto unošenja korisničkog imena i lozinke, korisnici mogu samo kliknuti na ikonicu npr. Facebook-a ili LinkedIn-a kako bi se prijavili u svoju instancu. Navedeno povezivanje s aplikacijama se mora naknadno podesiti unutar platforme te to radi administrator koji mora čuvati korisničke informacije sigurnima, ažurnima te na jednome mjestu (Salesforce Security Guide, 2020).

Ometov et al. (2018) ističu kako Multi-Factor Authentication (MFA) predstavlja više načina za provjeru identiteta, što znači i veću sigurnost. MFA osigurava veću zaštitu korisničkih računa od prijetnji. MFA zahtijeva od korisnika da navedu dva ili više faktora prilikom prijave, koje samo oni znaju, kako bi potvrdili svoj identitet. MFA traži od korisnika par sekundi više nego što se traži za običnu prijavu, ali zato na taj način pruža poboljšanu sigurnost za račune korisnika. Burger (2022) dalje objašnjava način na koji radi MFA unutar Salesforce-a, a to je da nakon što korisnik unese lozinku i korisničko ime, dobiva push notifikaciju na mobilnom uređaju gdje mora potvrditi da se to uistinu radi o ovlaštenom korisniku. Što znači da ako i napadač provali lozinku od korisnika, on neće moći ući u sustav zato jer nije potvrdio korisnikovu identifikaciju na mobilnom uređaju. Kako bi se to podesilo korisnik mora na mobitelu instalirati aplikaciju koja se zove „Salesforce Authenticator“. Također osim same potvrde da se radi o pravom korisniku, u navedenoj aplikaciji se može podesiti da prilikom

svakog pokušaja prijave u sustav, aplikacija generira verifikacijski kod za korisnika. Ti verifikacijski kodovi se zovu TOTP (Timebased one-time passwords) gdje korisnik mora unijeti kod kako bi se prijavio u sustav. Nakon podešavanja MFA, administratori mogu nadgledavati sve nepravilnosti prilikom prijave i time povećati sigurnost prijave unutar sustava. MFA se osim kod ulogiravanja korisnika, može postaviti i kada korisnik želi pristupiti izvješćima ili povezanim aplikacijama (Burger, 2022).

My Domain je sigurnosna značajka od strane Salesforce-a kojom organizacija definira svoju subdomenu kako bi prije svega naznačila korisnicima da se prijavljuju u pravi sustav. Također, kompanija može brendirati i prilagoditi svoju login stranicu. Može se podesiti da se preusmjere ili blokiraju zahtjevi korisnika prema drugim stranicama koje ne koriste pravu domenu, kao još i mnoge druge postavke koje omogućuju korisnicima da sa sigurnošću posluju unutar svoje Salesforce instance (Salesforce Security Guide, 2020).

4.1.3.1. Industrijski standardi i protokoli za upravljanje identitetom i pristupom

Standard predstavlja široko prihvaćene prakse koje slijede članovi industrije. Standard uključuje protokole koji određuju kako sustavi razmjenjuju informacije između sebe. Tri su protokola koji omogućuju suradnju između pružatelja usluge (service provider) i pružatelja identiteta (identity provider). To su: SAML protokol, OAuth 2.0 protokol i OpenID Connect protokol.[6] Razlika između pružatelja identiteta i pružatelja usluge je ta da pružatelj identiteta provjerava da li je to zaista korisnik kakvim se predstavlja provjeravajući bazu podataka, dok pružatelj usluge kada korisnik želi koristiti njegovu uslugu, traži od pružatelja identiteta identifikaciju da se radi o ovlaštenom korisniku. Jednom kada pružatelj identiteta potvrdi da se korisnik već nalazi u bazi podatka, korisnik može iz jedne aplikacije prijeći u drugu bez ponovnog prijavljivanja. Salesforce može biti i pružatelj usluge i pružatelj identiteta. Ukoliko je Salesforce pružatelj usluge, korisnici iz ostalih cloud-ova i aplikacija putem nekog pružatelja identiteta kojeg kompanija koristi (Microsoft's Active Directory Federation Services (ADFS), Ping Identity's PingFederate, open-source Shibboleth, ForgeRock's OpenAM, itd.), mogu pristupiti Salesforce-u. Dakle, korisnici se prijavljuju na temelju davatelja identiteta, a zatim se preusmjeravaju na Salesforce. U slučaju da je Salesforce pružatelj identiteta, on sadrži sve informacije o korisnicima te garantira ostalim cloud-ovima i aplikacijama da korisnik nije prijetnja te da se može jednostavno prebaciti na njih, bez ponovnog unošenja korisničkog imena

[6] Izvor: https://www.parallels.com/blogs/ras/oauth-vs-saml-vs-openid/ [Pristupano 6. prosinca 2023].

i lozinke. Time Salesforce pruža SSO značajku za povezivanje korisnika s različitim pružateljima usluga (Sharma, 2020).

Security Assertion Markup Language (SAML) protokol omogućuje da se korisnici jednostavno prebacuju iz jedne aplikacije u drugu bez ponovnog prijavljivanja. Takav protokol olakšava integraciju između različitih sustava i aplikacija koje podržavaju SAML. Pa tako jednom kada su korisnici već prijavljeni u Salesforce, oni unutar te platforme mogu kliknuti na link ili ikonu od neke aplikacije, npr. Gmail, bez ponovnog unošenja korisničkog imena i lozinke. Isto je moguće i kada se putem neke druge aplikacije želi pristupiti Salesforce-u (Buckbee, 2022).

OAuth (Open Authorization) 2.0 protokol omogućuje sigurno dijeljenje podataka između aplikacija. Koristi se u slučajevima gdje korisnici trebaju dati pristup ne povezanim aplikacijama u obrađivanju njihovim podacima bez otkrivanja lozinki. Na taj način, korisnik radi u jednoj aplikaciji, ali vidi podatke iz druge aplikacije. U slučaju Salesforce-a, korisnici su npr. ulogirani u Salesforce mobilnu aplikaciju te iz nje vide podatke koji se inače nalaze na Salesforce desktop verziji (Salesforce Security Guide, 2020).

OpenID Connect Protocol (OIDC) šalje informacije o identitetu korisnika s jedne aplikacije na drugu. Upravo taj protokol omogućuje ulaženje u sustav Salesforce-a putem drugih aplikacija. OIDC omogućuje korisnicima korištenje Single sign-on (SSO). Salesforce ugrađuje podršku za nekoliko glavnih pružatelja društvenih identiteta, a to su: Google, Facebook i LinkedIn. Na taj način korisnici ne moraju za Salesforce raditi novi korisnički račun, kreirajući novu lozinku i korisničko ime, već se jednostavno povežu klikom na ikonu ili link društvene mreže koja koristi OpenID Connect Protocol (Salesforce Security Guide, 2020).

5. Revizija i nadzor podataka u Salesforce-u

Osim kontrolama pristupa na temelju uloga (roles), profila i dopuštenja (permission sets), sigurnost podataka u Salesforce-u ostvaruje se kontinuiranim nadzorom i revizijom. Nadzor nad podacima omogućuje praćenje aktivnosti korisnika u stvarnom vremenu, dok se revizijom prate sve promjene i konfiguracije unutar platforme (Johan i Ahmad, 2023).

Spremić (2012) ističe da uspješne organizacije upravljaju IT-om na isti način na koji upravljaju i ostalim procesima i strateškim funkcijama. Ističe kako mnogi drugi poslovni procesi ovise o IT-u te da bi bez IT-a aktivnosti organizacije došle do zastoja. IT rizici nastaju intenzivnim korištenjem IS-a i IT-a što može izazvati neočekivanu ili neželjenu štetu. Postupak procjene IT rizika se izračunava na temelju imovine (sve što kompanija posjeduje i za što ima poslovnu vrijednost), prijetnje (mogućnost ili namjera neke osobe da iskoristi ranjivost organizacije), ranjivosti (učinkovitost kontrola unutar dijelova informacijskog sustava) (Spremić, 2012). Rizici se ne mogu potpuno ukloniti, ali se mogu smanjiti. Da bi do toga došlo, upravljanje rizicima mora biti na razini cijele organizacije te točno mora postojati plan kako upravljati rizicima. Plan upravljanja rizicima je sljedeći: identifikacija i klasifikacija IT rizika, procjena IT rizika, strategija odgovora na IT rizik, provedba i dokumentiranje odabrane protumjere, definiranje načina otklanjanja šteta te nadzor, revizija i prilagodba plana (Spremić, 2012).

Spremić (2017b) opisuje reviziju kao postupak kojim se provjerava uspješnost informacijskog sustava, odnosno u kojoj mjeri su njegove kontrole učinkovite za sigurno poslovanje na svim hijerarhijskim razinama. Revizijom se procjenjuju rizici i daju se preporuke za njihovo smanjenje. Do danas su se dogodili mnogi hakerski napadi na velike i zvučne kompanije koje su boljom zaštitom informacijskog sustava mogle spriječiti takve napade. Neke od velikih kompanija čiji su informacijski sustavi do nedavno griješili su: Sony, gdje su hakeri dobili pristup osobnim podacima korisnika, podacima povijesnih kupnji te brojevima kreditnih kratica; eBay, bili su kompromitirani podaci koji su uključivali imena, adrese, datume rođenja i šifrirane zaporke njihovih korisnika; JP Morgan Chase, gdje su ukradeni podaci uključivali osobne podatke korisnika te interne podatke banke; Target, krađa 40 milijuna brojeva kreditnih kartica, preko 70 milijuna adresa, brojeva telefona i ostalih povjerljivih podataka kupaca; itd (Spremić, 2017b).

Napadi mogu biti usmjereni na bilo koju kompaniju, bilo na privatna ili javna poduzeća. Hakeri danas raspolažu naprednim tehnologijama i znanjem te je veća vjerojatnost da će provesti

isplanirani i sofisticirani napad koji će biti teški za detektiranje te će se teško moći upravljati nad njime. Kao što je već i spomenuto, hakeri mogu napasti bilo koji dio informacijskog sustava i u bilo koje vrijeme. Najčešća meta današnjih hakerskih napada su zaposlenici kompanije koji predstavljaju „ulaznicu“ hakeru da dođe u sustav i tako našteti nekoj organizaciji. Hakerskim napadima najčešće se nastoji izvući novac od oštećene strane. Stoga je važno često provoditi reviziju sustava koja će ocijeniti u kojoj mjeri su trenutne kontrole učinkovite u prevenciji hakerskih napada.

Neki od napada koji se događaju putem interneta su: phishing (slanje lažnih poruka kojim se nasamare ljudi da daju svoje podatke), društveni inženjering (lažnim predstavljanjem se manipulira osobama kako bi se izvuklo čim više podataka), keyloggers (bilježenje svakog udarca na tipkovnici kako bi se sumirali prikupljeni podaci i iskoristili na štetu uhvaćene žrtve), razni zloćudni računalni programi poput ransomware-a (računalni virus kriptira podatke koji su nužni za nastavak poslovanja, gdje za njihovo dekriptiranje hakeri traže neku odštetu), itd. Tu su još i mnogi drugi poput: Sniffing-a, napad lozinkama, skeniranje portova, Session hijacking, DDoS napadi, itd (Spremić, 2017b).

Koliko god sigurnosne mjere bile snažne, na neke potencijalne ranjivosti i rizike je teže utjecati. Greške korisnika su jedan od najvećih rizika ne samo za Salesforce, već i za bilo koji sustav. Korisnici mogu ne namjerno izložiti osjetljive podatke, mogu kreirati slabe lozinke ili nasjesti na phishing napade, ugrožavajući na taj način sigurnost svojih i organizacijskih podataka. Stoga je važno raznim prijenosom znanja i treninzima educirati radnu snagu na svim razinama hijerarhije kako bi opreznije postupali sa osjetljivim podacima, kreirali jake lozinke te na vrijeme identificirali kibernetičke napade. Jallow (2022) naglašava da treba biti oprezan s integracijama trećih strana poput drugih sustava i aplikacija koje zbog svojih sigurnosnih propusta mogu naštetiti i Salesforce sustavu. Stoga korisnici Salesforce sustava trebaju biti oprezni s kim žele dijeliti podatke te provjeriti da li posluju sa pouzdanom i sigurnom trećom stranom. Johan i Ahmad (2023) stavljaju poseban naglasak na unutarnje mjere koje zbog svojih mogućih zaostataka mogu zakazati u identificiranju potencijalnih prijetnji što na kraju može naštetiti Salesforce instanci. Naime, nezadovoljni i zlonamjerni zaposlenici mogu naštetiti sustavu i ukrasti podatke. Da bi se zaštitila od takvih prijetnji, kompanija treba raznim ograničenjima nad podacima putem kontrola pristupa i stalnom revizijom i nadzorom nad podacima pratiti, kako bi se na vrijeme uočile neke sumnjive aktivnosti te identificirali potencijalni rizici i ranjivosti. Kompanija također treba imati unaprijed postavljen plan kojima će ublažiti nastalu štetu, ukoliko dođe do nje (Johan i Ahmad, 2023).

5.1. Revizija informacijskih sustava na temelju studije slučaja

Mnoge današnje kompanije se zbog učinkovitosti i smanjenja troškova odlučuju za pohranu svojih podataka na cloud okruženje. Kompanije nemaju svoje servere za pohranu podataka već koriste za to servere drugih kompanija koje ulažu velik dio svojih sredstava za održavanje takve infrastrukture. Postavlja se pitanje koliko su zaštićeni i sigurni sustavi dobavljača koji pružaju usluge računalstva u oblaku. Chen i Zhao (2012) istaknuli su neke od većih incidenata koji su se dogodili kod velikih pružatelja cloud usluga poput Amazon's Simple Storage Service, gdje su 2009. godine procurili podaci korisnika koji su bili na Amazon-ovom serveru. Isto tako i Microsoftova platforma za računalstvo u oblaku Azure je bila žrtva hakerskog napada zbog čega su njezine usluge morale biti zatvorene 22 sata. Stoga pružatelji cloud usluga moraju imati sigurnosne mjere, održavati integritet podataka te imati backup opciju, kako podaci njihovih korisnika ne bi bili narušeni i zauvijek izgubljeni. Vodeći pružatelji cloud usluga današnjice poput Salesforce.com, Amazon, Google i Microsoft, da bi imali povjerenje od svojih klijenata, moraju omogućiti privatnost i sigurnost podataka te trebaju biti usklađeni s regulativama i pravilima koje izdaju zakonodavna tijela (Chen i Zhao, 2012).

Salesforce je danas jako popularna platforma za pružanje cloud usluga. Ukupno gledajući, ona je jako sigurna za pohranu privatnih podataka te se upravo radi toga, sve više i više kompanija odlučuje za korištenje njezinih usluga. Isto tako, hakeri će pokušati naći način kako da naštete kompanijama i izvuku maksimalnu korist za sebe. Povećanjem klijenata i profitabilnosti neke kompanije, sigurno je za očekivati da će se povećati i pokušaji hakerskih napada. Dokaz tome je i napad na kompaniju Hanna Andersson 2019.godine koja se bavi prodajom dječje odjeće. Tim napadom narušena je privatnost podataka takve kompanije te je Salesforce zasigurno osjetio udarac na svoju reputaciju u to vrijeme (Jallow, 2022).

Kako opisuje Epiq (2020), hakeri koji su prodrli u Salesforce bazu podataka putem Hanna Andersson kompanije, ukrali su oko 10 tisuća podataka od strane kupaca Hanna Andersson kompanije te ih prodali kriminalcima na dark web-u. Ljudi koji su bili žrtve, su oni ljudi čiji su podaci bili pohranjeni u bazu podataka zbog provođenja transakcija s kompanijom. Time su bili ukradeni osobni podaci i podaci o plaćanju od strane kupaca. Hakeri su nekako uspjeli ugraditi malware na mrežu Salesforce-a putem Hanna Andersson kompanije koja očito nije imala dobre sigurnosne mehanizme. No, isto tako i Salesforce je zakazao u pogledu zaštite jer je prodor u bazu podataka tek otkriven tri mjeseca nakon. Tako i Salesforce i Hanna Andersson nisu uspjele

zaštiti privatne podatke kupaca. Zakazali su u zaštiti nad podacima zbog korištenja neadekvatne sigurnosne prakse, dosta su kasno otkrile prodor te nisu na vrijeme javile kupcima za povredu njihovih podataka (Epiq, 2020).

Kontrole koje su mogle spriječiti ovaj kibernetički napad su: bolja kontrola nad sustavom za plaćanje, korištenje višestruke provjere autentičnosti (MFA), bolji nadzor nad sustavom, kvalificirano stručno osoblje koje se razumije u zaštitu sustava, enkripcija podataka, bolji nadzor mrežnog prometa, podizanje svijesti zaposlenih o cyber sigurnosti, ažurirani anti-malware softver te segregacija mreže.

Sljedeći primjer napada je na Uber 2022.godine, odnosno na tvrtku koja pruža usluge prijevoza. Uber koristi Salesforce-ovu Slack aplikaciju za razmjenjivanje poruka. Kod ovog slučaja, problem nije bio u nedostatku sigurnosti hardvera, softvera ili enkripcije podataka na mreži, već zbog nepažnje zaposlenika od strane Uber-a. Napad se dogodio na način da su napadači došli do lozinke jednog od zaposlenika. Kada je napadač želio ući u sustav putem tog zaposlenikovog računa, zaposlenik je nesvjesno prihvatio zahtjev za dvofaktorsku autentifikaciju te time omogućio hakerima pristup Uber-ovom sustavu. Jednom unutra, napadači su ušli u Salesforce-ovu Slack aplikaciju koju koristi Uber. Unutar Slack-a, napadači su preuzeli neke poruke koje su zaposlenici Uber-a razmjenjivali međusobno (Novet, 2022).

Vidljivo je da je u ovom slučaju korištena hakerska tehnika društvenog inženjeringa gdje su napadači uvjerili zaposlenika da prihvati zahtjev za dvofaktornu autentifikaciju. Kontrole koje su mogle spriječiti ovaj kibernetički napad su: korištenje multi faktorske umjesto dvofaktorske autentifikacije korisnika, podizanje svijesti zaposlenika o društvenom inženjeringu te bolje praćenje neuobičajenih aktivnosti.

Sličan gornje navedenom napadu, dogodio se baš na Salesforce platformu 2007.godine, kada je jedan od zaposlenika Salesforce-a postao žrtva phishing prijevare. Berlind (2007) pojašnjava da je analizom od strane Salesforce-a naknadno utvrđeno da je napadač uspio prevariti zaposlenika same platforme da mu otkrije svoju lozinku, što je omogućilo napadaču da dođe u bazu podataka i kopira kontakte korisnika Salesforce-a. Berlind (2007) dalje navodi kako su kopirani podaci uključivali imena, prezimena, nazive tvrtki, adrese e-pošte, telefonske brojeve korisnika, itd. Hakerima su najvažnije bile email adrese koje su iskoristili kako bi slali phishing mailove klijentima od kompanija koje koriste cloud rješenja od Salesforce-a. Na kraju se nekoliko ljudi uspjelo „upecati“ na phishing napade, dajući hakerima svoje lozinke. Email adrese su izgledale poput nekih Salesforce-ovih računa radi kojih su se ljudi lagano dali

nasamariti. Jedna od kompanija koja je bila žrtva, čiji su klijenti dobili lažne email poruke je i Automatic Data Processing Inc, odnosno tehnološka kompaniju koja pruža cloud rješenja koja su bazirana na upravljanje ljudskim kapitalom (engl. human capital management - HCM) poput: ljudskih resursa, obračun plača, poreza, itd (Berlind, 2007).

Na temelju svega gore vidljivo je da upad nije proizašao iz nedostatka sigurnosti Salesforce platforme ili nedostatka baze podataka, već radi neopreznosti njezina zaposlenika. Ono što je moglo spriječiti napad je podizanje svijesti i obrazovanje od strane zaposlenika Salesforce-a i njezinih korisnika da znaju prepoznati phishing poruke, ograničiti IP raspon prijave u Salesforce sustav i time dopuštajući pristup samo s korporativne mreže, korištenje tehnologije koja će automatski reagirati na phishing napade, korištenje multi faktorske identifikacije i praćenje neuobičajenih aktivnosti unutar sustava.

Iz gore navedenih primjera kibernetičkih napada, može se zaključiti da Salesforce, koliko god naprednu hardversku i softversku tehnologiju koristio, mora više osvijestiti svoje zaposlenike, korisnike i partnere kako da na bolji i efikasniji način implementiraju Salesforce-ovu tehnologiju. Platforma mora pružati obilan i lako dostupan skup resursa, uključujući dokumentaciju, vodiče i obuke koje će pomoći korisnicima razumjeti sigurnosne značajke i kako ih implementirati u svojim organizacijama. Skočnim prozorima (engl. pop-up windows) pružati svakojake savjete o dodatnoj zaštiti te obavijestima o sigurnosti i ažuriranjima kako bi obavijestili korisnike o novim prijetnjama ili sigurnosnim poboljšanjima. Ukoliko će se korisnici držati preporučene sigurnosne prakse od strane Salesforce-a, korisnici će se manje suočavati sa prijetnjama izvana. Također, ograničenja pristupa zaposlenicima unutar kompanije je isto ključno kako se ne bi omogućilo zaposlenicima kompanije da imaju veći pristup nečemu čemu ne bi smjeli imati. U sljedećem poglavlju će se pričati o dodatnim rješenjima koje Salesforce pruža, a tiče se nadzora nad podacima i zaposlenicima.

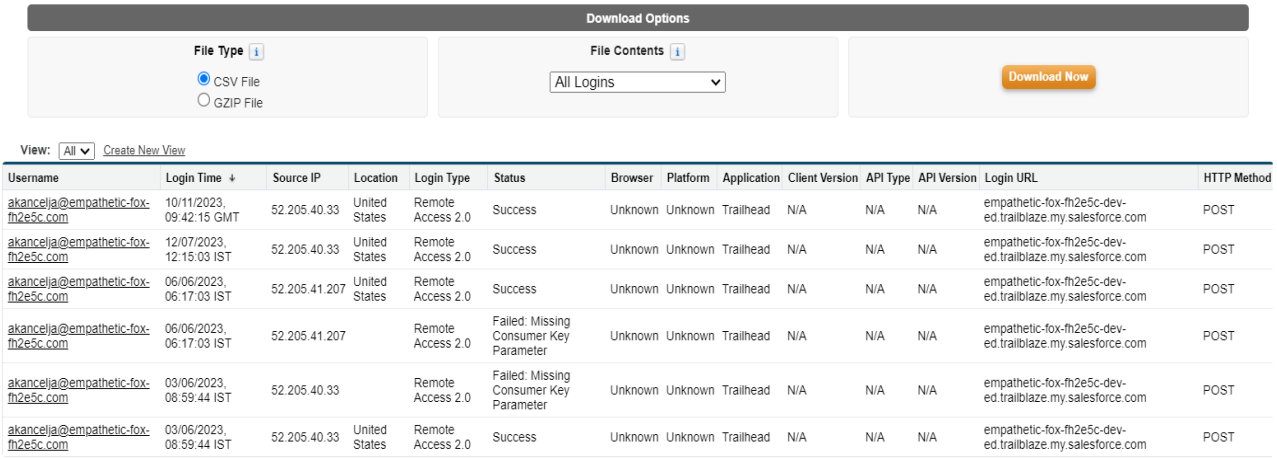
5.2. Načini provjere i praćenje sumnjivih radnji korisnika unutar Salesforce-a

Redovito praćenje Salesforce-ovog okruženja radi mogućih prijetnji i ranjivosti sustava, ključno je za održavanje privatnosti podataka i sprječavanje krađe podataka. Praćenje događaja odvija se u stvarnom vremenu te pruža uvid u aktivnost korisnika unutar platforme. Time se omogućuje administratorima lakše praćenje promjena nad podacima kako bi se na vrijeme uočile anomalije unutar sustava (Jahan i Ahmad, 2023).

U Salesforce-u je tako moguće pratiti sva zbivanja koja njezini korisnici naprave te na taj način pravovremeno otkriti neku sumnjivu radnju. Prati se tko je zadnji uredio neki zapis, može se pregledati popis uspješnih i neuspjelih pokušaja prijave u sustav, tko je promijenio neku vrijednost u polju, itd.

Praćenje događaja unutar Salesforce-a, omogućuje administratorima da budu poput detektiva koji će pratiti sve aktivnosti unutar sustava. Praćenje događaja (engl. Event Monitoring) jedan je od alata koji Salesforce nudi kako bi držao podatke zaštićenima. Alat daje mogućnost detaljnog nadzora nad korisnikovim aktivnostima unutar organizacije. Postoji 50 tipova događaja koji se mogu pratiti, a neki od njih su: prijave, odjave, klikovi unutar platforme, performanse sustava, pogreške (engl. errors), preuzeti sadržaji, itd. Dakle svaka aktivnost koja se dogodi na platformi, pohranjuje se te je nakon nekog vremena dostupna administratoru za pregled. Primjerice, sumnjiva radnja će biti ako se npr. na neki određeni dan ulazilo nekoliko stotina puta u sustav, dok kompanija broji samo desetak zaposlenika. Salesforce-ovim se alatom može vidjeti koji se je korisnik toliko puta prijavljivao u sustav te s koliko se različitih IP adresa korisnik prijavljivao (Salesforce Security Guide, 2020).

Slika 8. Povijest prijave (Izvor: vlastiti rad autora)



Download Options

File Type: CSV File / GZIP File

File Contents: All Logins

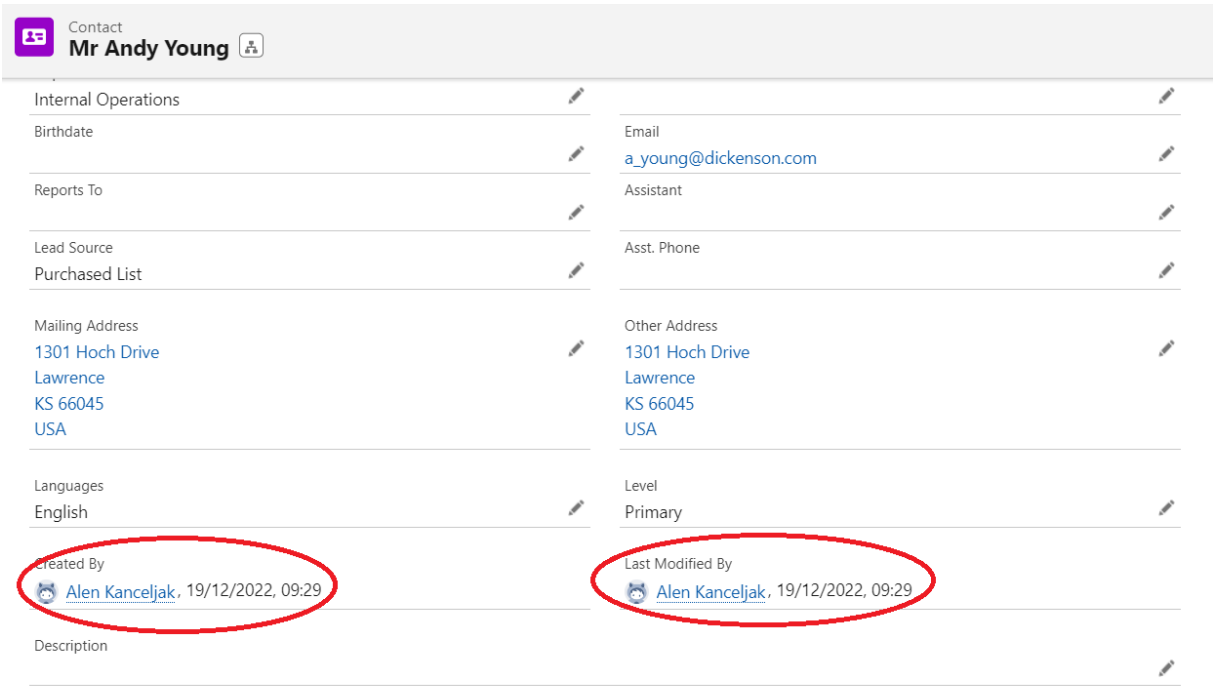
Download Now

View: All Create New View

Username	Login Time	Source IP	Location	Login Type	Status	Browser	Platform	Application	Client Version	API Type	API Version	Login URL	HTTP Method
akancelja@empathetic-fox-fh2e5c.com	10/11/2023, 09:42:15 GMT	52.205.40.33	United States	Remote Access 2.0	Success	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST
akancelja@empathetic-fox-fh2e5c.com	12/07/2023, 12:15:03 IST	52.205.40.33	United States	Remote Access 2.0	Success	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST
akancelja@empathetic-fox-fh2e5c.com	06/06/2023, 06:17:03 IST	52.205.41.207	United States	Remote Access 2.0	Success	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST
akancelja@empathetic-fox-fh2e5c.com	06/06/2023, 06:17:03 IST	52.205.41.207		Remote Access 2.0	Failed: Missing Consumer Key Parameter	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST
akancelja@empathetic-fox-fh2e5c.com	03/06/2023, 08:59:44 IST	52.205.40.33		Remote Access 2.0	Failed: Missing Consumer Key Parameter	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST
akancelja@empathetic-fox-fh2e5c.com	03/06/2023, 08:59:44 IST	52.205.40.33	United States	Remote Access 2.0	Success	Unknown	Unknown	Trailhead	N/A	N/A	N/A	empathetic-fox-fh2e5c-dev-ed.trailblaze.my.salesforce.com	POST

Kod praćenja prijava, administratori mogu pratiti sve pokušaje prijave kod svoje organizacije. Pa tako, slika iznad prikazuje koji član organizacije se htio prijaviti u sustav, datum i vrijeme prijave, uspješnost prijave, IP adresa, itd. Administratori mogu preuzeti povijest prijava u zadnjih 6 mjeseci u obliku CSV ili GZIP formata te time može biti prikazano do 20 000 zapisa.

Slika 9. Prikaz osobe koja je kreirala i zadnje uredila zapis (Izvor: vlastiti rad autora)



Contact

Mr Andy Young

Internal Operations

Birthdate

Email: a_young@dickenson.com

Reports To

Assistant

Lead Source: Purchased List

Asst. Phone

Mailing Address: 1301 Hoch Drive, Lawrence, KS 66045, USA

Other Address: 1301 Hoch Drive, Lawrence, KS 66045, USA

Languages: English

Level: Primary

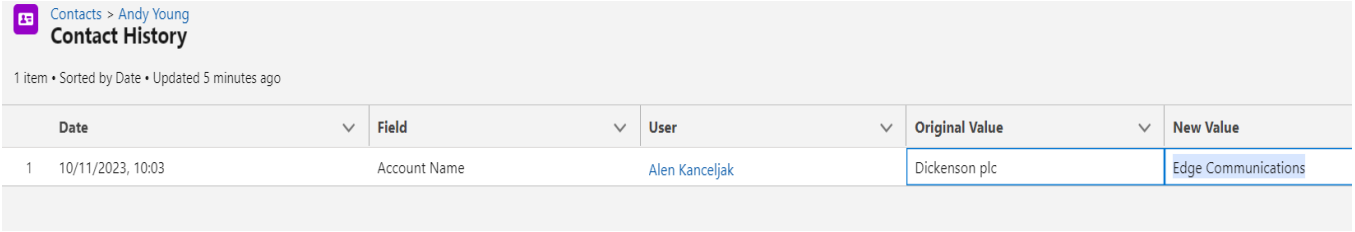
Created By: Alen Kanceljak, 19/12/2022, 09:29

Last Modified By: Alen Kanceljak, 19/12/2022, 09:29

Description

Praćenjem polja unutar nekog objekta, administratori mogu vidjeti modifikacije koje su se provodile nad poljima. Mogu vidjeti datum, vrijeme, tko je kreirao zapis te tko je napravio zadnju promjenu na zapisu.

Slika 10. Vidljivost nad promjenom vrijednosti polja (Izvor: vlastiti rad autora)

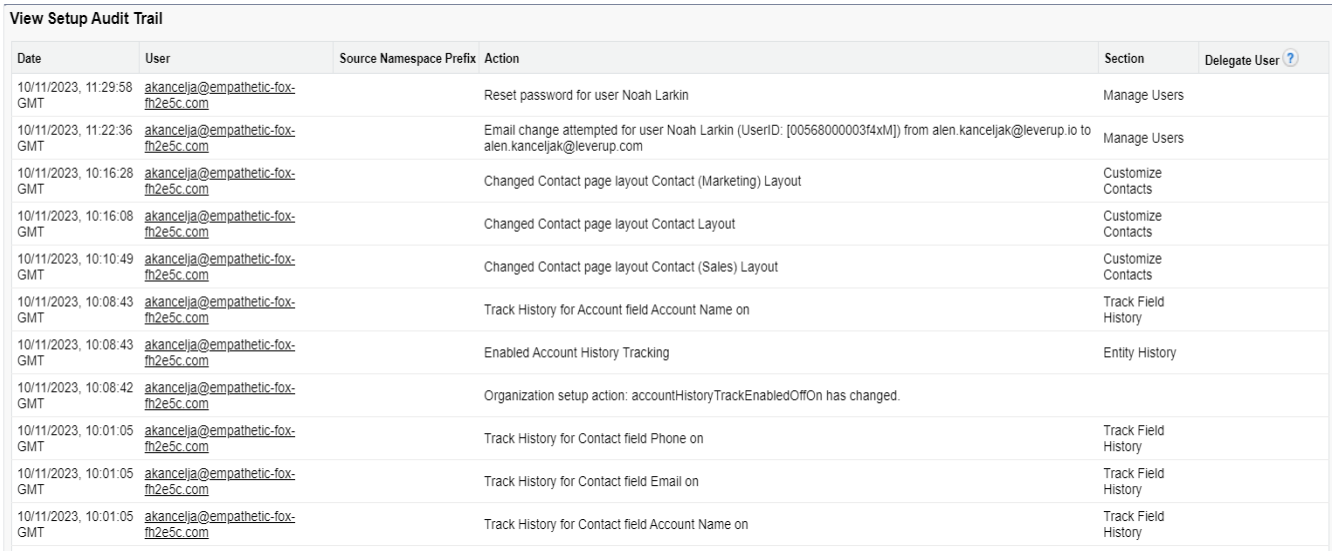


Administratori mogu vidjeti i promijenjenu staru vrijednost nekog polja u novu vrijednost. Na primjer, u gornje prikazanoj slici je navedena vrijednost „Account" polja koja je promijenjena iz „Dickenson plc" u „Edge Communications".

„Setup Audit Trail" je opcija koja prati nedavne promjene postavki unutar sustava. Uglavnom administratori imaju pravo promjene postavki te je ta značajka korisna kako bi se kontroliralo ako u organizaciji ima više od jednog administratora. Tom opcijom se mogu pratiti i najmanje promjene koje je korisnik s administratorskim ovlastima unutar neke organizacije napravio. Puno toga se „Setup Audit Trail" prati, no ovo su samo neke od promjena koje se prate: promjena jezika unutar sustava, resetiranje email adresa korisnika, resetiranje lozinke za korisnika, izvoz podataka, uvoz podataka te mnogo drugih promjena.[7] Slika ispod prikazuje neke od promjena koje su napravljene unutar Salesforce platforme. Pa tako slika prikazuje da je email adresa i lozinka nekog korisnika promijenjena od strane administratora. Tu su i ostale promjene poput omogućivanja ostalih značajki unutar Salesforce-a, poput: omogućivanje opcije praćenja promjene vrijednosti polja, promjene rasporeda unutar „Contact" objekta, itd., a koje su dio Event Monitoring-a.

[7] Izvor: https://help.salesforce.com/s/articleView?id=sf.admin_monitorsetup.htm&type=5 [Pristupano 7. prosinca 2023].

Slika 11. Praćenje promjena unutar sustava - Event Monitoring (Izvor: vlastiti rad autora)



View Setup Audit Trail

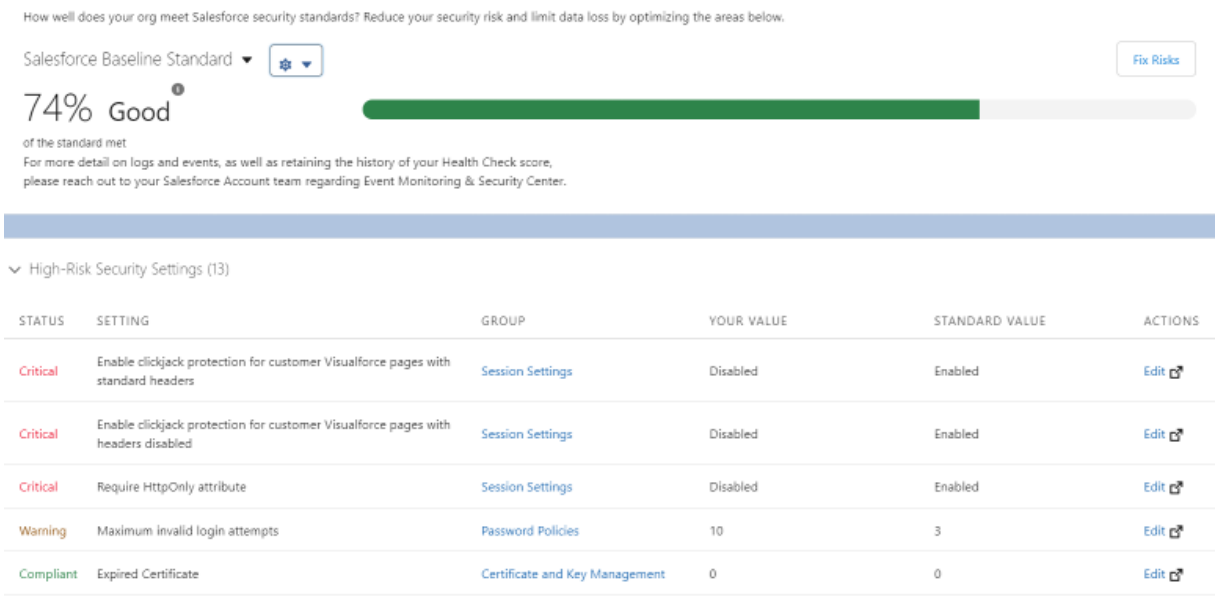
Date	User	Source Namespace Prefix	Action	Section	Delegate User
10/11/2023, 11:29:58 GMT	akancelja@empathetic-fox-fh2e5c.com		Reset password for user Noah Larkin	Manage Users	
10/11/2023, 11:22:36 GMT	akancelja@empathetic-fox-fh2e5c.com		Email change attempted for user Noah Larkin (UserID: [00568000003f4xM]) from alen.kanceljak@leverup.io to alen.kanceljak@leverup.com	Manage Users	
10/11/2023, 10:16:28 GMT	akancelja@empathetic-fox-fh2e5c.com		Changed Contact page layout Contact (Marketing) Layout	Customize Contacts	
10/11/2023, 10:16:08 GMT	akancelja@empathetic-fox-fh2e5c.com		Changed Contact page layout Contact Layout	Customize Contacts	
10/11/2023, 10:10:49 GMT	akancelja@empathetic-fox-fh2e5c.com		Changed Contact page layout Contact (Sales) Layout	Customize Contacts	
10/11/2023, 10:08:43 GMT	akancelja@empathetic-fox-fh2e5c.com		Track History for Account field Account Name on	Track Field History	
10/11/2023, 10:08:43 GMT	akancelja@empathetic-fox-fh2e5c.com		Enabled Account History Tracking	Entity History	
10/11/2023, 10:08:42 GMT	akancelja@empathetic-fox-fh2e5c.com		Organization setup action: accountHistoryTrackEnabledOffOn has changed.		
10/11/2023, 10:01:05 GMT	akancelja@empathetic-fox-fh2e5c.com		Track History for Contact field Phone on	Track Field History	
10/11/2023, 10:01:05 GMT	akancelja@empathetic-fox-fh2e5c.com		Track History for Contact field Email on	Track Field History	
10/11/2023, 10:01:05 GMT	akancelja@empathetic-fox-fh2e5c.com		Track History for Contact field Account Name on	Track Field History	

Zbog mnogih značajki, licenci i aplikacija koje Salesforce pruža, redoviti pregledi sigurnosnih postavki su neophodni. To je moguće zahvaljujući provjeri zdravlja sustava (engl. Health Check) koji daje sveukupnu ocjenu na temelju sigurnosnog stanja unutar Salesforce instance koju neka kompanija koristi. Pomaže kompanijama da identificiraju ranjivosti unutar svoje Salesforce instance te da ih riješe prije nego što mogu biti iskorištene od strane hakera. Health Check-om se identificiraju ranjivosti i nadzire se učinkovitost podešenih sigurnosnih postavki. Radi na principu da postotkom prikaže kolika je sigurnost unutar sustava. Pa tako 100% prikazuje najveći stupanj sigurnosti, dok 0% najmanji stupanj (Strongpoint.io, 2023). Ocjena se formira na temelju podešenih postavki unutar sustava, a može biti: 90% i iznad je odlično (engl. Excellent), 80%–89% je vrlo dobro (engl. Very Good), 70%–79% je dobro (engl. Good), 55%–69% je siromašno (engl. Poor) i 54% i ispod je jako siromašno (engl. Very Poor).[8] Postoje četiri kategorije rizika: Visoki rizik, Srednji rizik, Niski rizik i Informativni rizik. Svaki od rizika u sebi sadrži statuse: „critical“ kao najrizičniji, „warning“ kao upozoravajući te „compliant“ koji je blag i zanemariv. Visoki rizici poput zaštita od „clickjack“ i maksimalan broj nevažećih pokušaja prijave će najviše utjecati na postotak, srednji rizici nalik složenosti lozinke i vrijeme isteka lozinke će srednje utjecati, niski rizici poput postavljanja vremenskog perioda automatske odjave iz sustava nakon neaktivnosti ili postavljanje sigurnosnog pitanja prilikom prijave u sustav će najmanje utjecati, dok informativni rizici uopće neće utjecati na

[8] Izvor: https://help.salesforce.com/s/articleView?id=sf.security_health_check_score.htm&type=5 [Pristupano 5. rujna 2023].

postotak.[9] Tu je i mnogo ostalih sigurnosnih postavka koje administratori mogu prebaciti u bilo koju kategoriju, bilo visoko, srednje ili nisko rizičnu. Health Check daje preporuke koje stvari treba popraviti i na koji način, pa stoga može uvelike olakšati administratoru i skratiti mu vrijeme na traženje svih opcija koje nisu podešene na viši stupanj sigurnosti. Isto tako klikom na gumb „Fix Risks“ (hrv. Popravi rizike), automatski popravlja rizične postavke za administratora podešavajući postavke na preporučenu razinu. Neka uobičajena područja koja Health Check skenira su: postavke politike lozinke (maksimalan broj nevažećih pokušaja prijave i složenost lozinke), omogućavanje korisnicima da potvrde svoj identitet putem teksta (SMS), postavke isteka sesije, omogućenost zaštite protiv „clickjack“ (napad na korisnika tako da mu se podmetne neki nevidljivi element na stranicu, koji kad korisnik klikne, preuzima se zlćudni program na korisnikovo računalo), postavke za učitavanje/preuzimanje datoteka, itd (Strongpoint.io, 2023).

Slika 12. Provjera zdravlja sustava - Health Check (Izvor: vlastiti rad autora)



U primjeru iznad, Health Check je izmjerio da je stupanj sigurnost 74%, što je dobro. U primjeru su prikazane postavke sa visokim rizikom, odnosno one postavke koje najviše utječu na formiranje postotka. Vidljivo je da zaštita protiv „clickjack“ nije omogućena, isto kao što i nedostaje HttpOnly atribut (atribut dodan kolačiću preglednika koji sprječava dodavanje skripta na strani klijenta). Također, maksimalan broj nevažećih pokušaja prijave trenutno je postavljen

[9] Izvor: https://help.salesforce.com/s/articleView?id=sf.security_health_check_score.htm&type=5 [Pristupano 5. rujna 2023].

na 10, a preporučeno je 3. Ukoliko se te stvari poprave, postotak će se povećati te će se zelena boja na crti pored postotka pomaknuti udesno.

6. Zaključak

Sve više i više kompanija se okreće korištenju cloud tehnologija. Jednostavnije je i troškovno isplativije za kompanije da koriste usluge računalstva u oblaku od drugih kompanija koje imaju višegodišnje iskustvo bavljenja time te kojima je primarni cilj pružanje usluga u oblaku. Takvi pružatelji usluga cloud rješenja imaju vlastitu infrastrukturu i servere za pohranu velike količine podataka. Svjetski lider u pružanju takvih usluga je Salesforce koji pruža niz funkcionalnosti te pomaže kompanijama u upravljanju odnosima s klijentima.

Radom se pokazalo kakvu sve odgovornost nad podacima sudionici Salesforce platforme mogu imati. Takve ovlasti dodjeljuje administrator koji mora biti oprezan kakve sve uloge i dopuštenja dodjeljuje korisnicima kako se ne bi zloupotrijebili podaci. Istaknuta je i uloga Salesforce-a u pridržavanju regulatornih okvira i standarda koji osiguravaju transparentnost i zaštitu privatnosti korisnika. Međutim, svijest o regulativama i pridržavanje istih još uvijek predstavljaju izazov koji zahtijeva stalnu pažnju i prilagodbu.

Salesforce platforma pruža razne mehanizme zaštite od kibernetičkih prijetnji. Podaci se štite u 3 sloja, a to su fizički, mrežni i aplikacijski. Stabilnom i sigurnom infrastrukturom, Salesforce štiti fizičke uređaje koji služe za pohranu podataka od njihovog pokušaja krađe ili neke prirodne katastrofe. Mrežu također drži sigurnom, kriptirajući podatke, postavljanjem vatrozida te ograničavajući ulaz neovlaštenih korisnika u sustav. Također, raznim identifikacijskim i autorizacijskim kontrolama nastoji otkriti i spriječiti neovlašteno korištenje platforme. No ipak, uz sve te sigurnosne kontrole, incidenti vezani za Salesforce i dalje su se događali. Nedovoljno educirano radno osoblje platforme i kompanija koje koriste Salesforce zakazali su u otkrivanju napada poput phising-a i društvenog inženjeringa što je rezultiralo povredom podataka. Isto tako, neke kompanije i dan danas ne koriste preporučene mjere zaštite od strane Salesforce-a što također može rezultirati krađi podataka.

Sigurnost i zaštita privatnosti podataka od iznimne je važnosti za očuvanje povjerenja korisnika i klijenata. Njezino narušavanje može utjecati na reputaciju Salesforce platforme. Stoga su kontinuirana edukacija o potencijalnim kibernetičkim prijetnjama, proaktivna uloga korisnika, stalni nadzor nad podacima i stalno unaprjeđenje mjera sigurnosti ključni za održavanje visokih standarda sigurnosti i zaštite podataka unutar ove CRM platforme.

Popis literature

1. Bellovin, S.M. and Cheswick, W.R. (1994). Network firewalls. *IEEE Communications Magazine*, [online] 32(9), pp.50–57. doi:https://doi.org/10.1109/35.312843.
2. Berlind, D. (2007). *Phishing-based breach of salesforce.com customer data is more evidence of industry's need to act on spam. Now.* [online] ZDNET. Dostupno na: https://www.zdnet.com/article/phishing-based-breach-of-salesforce-com-customer-data-is-more-evidence-of-industrys-need-to-act-on-spam-now/ [3. rujna 2023].
3. Buckbee, M. (2022). *What is SAML and How Does it Work?* [online] Varonis.com. Dostupno na: https://www.varonis.com/blog/what-is-saml [16. listopada 2023].
4. Burger, M. (2022) Metrics and Insights to Help You Boost Login Security. Salesforce admins. Dostupno na: https://admin.salesforce.com/blog/2021/metrics-and-insights-to-help-you-boost-login-security [11. lipnja 2023].
5. Canavan, J., (n.d.). Fundamentals of Network Security. [online] Dostupno na: http://diglib.globalcollege.edu.et:8080/xmlui/bitstream/handle/123456789/1074/Fundamentals%20of%20Network%20Security.pdf.1.pdf?sequence=1&isAllowed=y [15. lipnja 2023].
6. Chaudhary, A. (2022). *Salesforce Shield Platform Encryption*. [online] Apex Hours. Dostupno na: https://www.apexhours.com/salesforce-shield-platform-encryption/ [9. studenoga 2023].
7. Chen, D. i Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. International Conference on Computer Science and Electronics Engineering. Dostupno na: https://www.researchgate.net/profile/Deyan-Chen-5/publication/254029141_Data_Security_and_Privacy_Protection_Issues_in_Cloud_Computing/links/568296bb08ae051f9aee6ab4/Data-Security-and-Privacy-Protection-Issues-in-Cloud-Computing.pdf [12. lipnja 2023].
8. Diligenski, A., Prlja, D. i Cerović, D. (2018). Pravo zaštite podataka GDPR. [online]. Institut za uporedno pravo. Beograd, Terazije 41. Dostupno na: http://ricl.iup.rs/222/1/2018%20-%20Pravo%20za%C5%A1tite%20podataka%20-%20Diligenski%2C%20Prlja.pdf [4. prosinca 2023].
9. Ebady Manna, M. (2018). A Cloud-Based Encryption for Document Storage UsingSalesforce.com [online]. Medwell Journals: Journals of Engineering and Applied Sciences 13 (Special Issue 1): 2382-2387. Dostupno na: https://medwelljournals.com/abstract/?doi=jeasci.2018.2382.2387 [16. lipnja 2023.]
10. Epiq (2020). Salesforce Data Breach: Consumers Fight Back. [online] Facebook App ID. Dostupno na: https://www.epiqglobal.com/en-us/resource-center/articles/salesforce-data-breach [2. rujna 2023].
11. Europa.eu. (2016). EUR-Lex - 32016R0679 - EN - EUR-Lex. [online] Dostupno na: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [23. listopada 2023.]

12. Fagin, R. (1978). On an authorization mechanism. *ACM Transactions on Database Systems* [online]. 3(3), pp.310–319. Dostupno na: https://dl.acm.org/doi/pdf/10.1145/320263.320288 [6. prosinca 2023].
13. Gong, C., Liu, J., Zhang, Q., Chen, H. and Gong, Z. (2010). *The Characteristics of Cloud Computing*. [online] Dostupno na: https://web.archive.org/web/20170811140221id_/http://www.qom.post.ir/_ITCenter/Documents/TheCharacteristicsofCloudComputing_20140722_154207.pdf [30. studenoga 2023.]
14. Gov.hr. (2018). Što je opća uredba o zaštiti podataka (engl. General Data Protection Regulation - GDPR) ? - gov.hr. [online] Dostupno na: https://gov.hr/hr/sto-je-opca-uredba-o-zastiti-podataka-eng-general-data-protection-regulation-gdpr/1868 [23. listopada 2023.]
15. Griffiths, P.P., i Wade, B.W. (1976). An authorization mechanism for a relational database system.ACM Trans. Database Syst. I, 3, 242-255.
16. Hajdarevic, K., Allen, P. and Spremić, M. (2016). Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Environments. Telecommunications Forum (TELFOR): IEEE. Dostupno na: https://ieeexplore.ieee.org/document/7818717 [25. listopada 2023.]
17. Hickman, Kipp E.B. (1994). *The SSL Protocol*. [online] Dostupno na: http://www.webstart.com/jed/papers/HRM/references/ssl.html [17 listopada. 2023].
18. Hrvatska enciklopedija (2021). Kibernetika. Hrvatska enciklopedija. [online] Dostupno na: https://www.enciklopedija.hr/Natuknica.aspx?ID=31381 [21 studenoga 2023].
19. Jahan, S. i Ahmad, F. (2023). Ensuring Data Security on Salesforce: A Comprehensive Review of Security Measures and Best Practices [online]. Integral University, Lucknow, Uttar Pradesh, India: International Journal of Engineering and Management Research. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4451453 [15. lipnja 2023.]
20. Jallow, M. (2022). Creating secure integrations: Case of Salesforce integrations. Završni rad. Jyväskylä: University of Jyväskylä, 2022, 109 p. Dostupno na: https://jyx.jyu.fi/bitstream/handle/123456789/83815/URN%3ANBN%3Afi%3Ajyu-202211085117.pdf?sequence=1 [10. studenoga 2023.]
21. Kristian Beckers, Stephan Faßbender, Maritta Heisel, Holger Schmidt, Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation, 2012 Seventh International Conference on Availability, Reliability and Security. pp. 242-248.
22. Leavitt, N.(2009). "Is cloud computing really ready for prime time?" Computer, vol. 42, no. 1, pp. 15–25. Dostupno na: https://ieeexplore.ieee.org/document/4755149 [10. studenoga 2023.]

23. Marańda, W., Poniszewska-Marańda, A. i Szymczy ´nska, M. (2022). Data Processing in Cloud Computing Model on the Example of Salesforce Cloud [online]. Information 2022, 13(2), 85. Dostupno na: https://www.mdpi.com/2078-2489/13/2/85 [16. lipnja 2023.]
24. Marinović, B. (2014). Zaposlenik je isključio struju, hrvatsko nebo bilo bez nadzora? [online] Vecernji.hr. Dostupno na: https://www.vecernji.hr/vijesti/zaposlenik-je-iskljucio-glavno-napajanje-struje-pa-nije-bilo-nadzora-letova-968165 [19 studenoga 2023].
25. Novet, J. (2022). *Salesforce co-CEO Benioff says there's 'no finish line when it comes to security' after Uber hack*. [online] CNBC. Dostupno na: https://www.cnbc.com/2022/09/20/marc-benioff-salesforce-will-keep-working-on-security-after-uber-hack.html [2. rujna 2023].
26. Okta.com. (2023). *Okta, Inc.* [online] Dostupno na: https://www.okta.com/identity-101/authentication-vs-authorization/ [10. listopada 2023].
27. Ometov, A., Bezzateev S., Mäkitalo N., Andreev, S., Mikkonen, T. i Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, [online] 2(1), pp.1–1. Dostupno na: https://doi.org/10.3390/cryptography2010001 [6. prosinca 2023].
28. Padmanabhan, R. (2021). *Salesforce Security Guide: Best Practices*. [online] Varonis.com. Dostupno na: https://www.varonis.com/blog/salesforce-security-guide [5. prosinca 2023].
29. Salesforce (2020). Salesforce Security Guide [online]. Salesforce. Dostupno na: https://resources.docs.salesforce.com/224/latest/en-us/sfdc/pdf/salesforce_security_impl_guide.pdf [12. lipnja 2023]
30. Salesforce (2023a). Salesforce Data Processing Addendum. Salesforce. Dostupno na: https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf [23. listopada 2023.]
31. Salesforce (2023b). Salesforce Services and other services and features1 Security, Privacy and Architecture. Salesforce. Dostupno na: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf [25. listopada 2023.]
32. Salesforce. (2023c). Salesforce Shield Platform Encryption Implementation Guide @salesforcedocs. Dostupno na: https://resources.docs.salesforce.com/latest/latest/en-us/sfdc/pdf/salesforce_platform_encryption_implementation_guide.pdf [17 listopada. 2023].
33. Salesforce (2014). *What is Salesforce?* [online] Dostupno na: https://www.salesforce.com/products/what-is-salesforce/ [20. studenoga 2023].
34. Salesforce (2022). Data privacy and security with Salesforce. Salesforce. [online]. Dostupno na: https://help.salesforce.com/s/articleView?id=000385172&type=1 [7. studenoga 2023].

35. Salesforce.com. (2022). Categories | Salesforce Compliance. [online] Dostupno na: https://compliance.salesforce.com/en [25. listopada 2023].
36. Sharma, A. (2020). Data security in Salesforce [online]. Jaypee University of Information Technology, Waknaghat: Department of Computer Science and Engineering. Dostupno na: http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/6746/1/Data%20Security%20in%20Salesforce.pdf [16. lipnja 2023.]
37. Shiang Hwang, M., Bayat M., Kusiak, A., et al. (2014). International Journal of Electronics and Information Engineering Vol. 1, No. 2 [online]. Jalaxy Technology Co., Ltd., Taiwan. Dostupno na: http://ijeie.jalaxy.com.tw/contents/ijeie-v1-n2/ijeie-v1-n2.pdf#page=29 [30. studenoga 2023.]
38. Sneha, M. S. i Krishna Prasad, K. (2018). Analysis of Business Strategies of Salesforce.com Inc. International Journal of Case Studies in Business, IT and Education (IJCSBE), 2(1), 37-44. [online]. Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184087 [20. studenoga 2023.]
39. Snisarenko, A. (2023). How Many Companies Use Salesforce? Total Customer Number. [online] Ascendix. Dostupno na: https://ascendix.com/blog/how-many-companies-use-salesforce/ [26. listopada 2023.]
40. Soni, K. & Vala, B. (2017). "Roadmap to salesforce security governance & salesforce access management," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-4, doi: 10.1109/ICECCT.2017.8117831.
41. Spremić, M. (2007). Metode provedbe revizije informacijskih sustava. Zbornik Ekonomskog fakulteta u Zagrebu, Vol. 5 No. 1, str. 295-312. Dostupno na: https://hrcak.srce.hr/26137 [25. listopada 2023.]
42. Spremić, M. (2012). Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks. [online] ResearchGate; publication - 261390322. Dostupno na: https://www.researchgate.net/publication/261390322_Corporate_IT_Risk_Management_Model_a_Holistic_view_at_Managing_Information_System_Security_Risks [15. lipnja 2023].
43. Spremić, M. (2013).Holistic Approach for Governing Information System Security. London, U.K.: Proceedings of the World Congress on Engineering 2013 Vol II,
44. Spremić, M. (2017a). Digitalna transformacija poslovanja.. Zagreb: Ekonomski Fakultet.
45. Spremić, M. (2017b). Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije. Zagreb: Ekonomski Fakultet.
46. Spremić, M. i Popovic, M. (2007). Towards a Corporate IT Risk Management Model. [online] ResearchGate: publication - 262173401. Dostupno na: https://www.researchgate.net/publication/262173401_Towards_a_corporate_IT_risk_management_model [12. lipnja 2023].

47. Spremić, M. i Šimunić, A, (2018). Cyber Security Challenges in Digital Economy. London, U.K.: Proceedings of the World Congress on Engineering 2018 Vol I.
48. Strongpoint.io. (2023). *Maintaining Org Security with the Salesforce Health Check*. [online] Dostupno na: https://www.strongpoint.io/en/blog/what-is-salesforce-health-check [5. rujna 2023].
49. Sun, Y. et al. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks: Hindawi Publishing Corporation. Dostupno na: https://journals.sagepub.com/doi/pdf/10.1155/2014/190903 [10. studenoga 2023.]
50. Szombathelyi, D. (2021). Kibernetička sigurnost. Završni rad. Osijek: Filozofski fakultet.
51. Tähtinen, Sami (2005). Järjestelmäintegraatio: Tarve, vaihtoehdot, toteutus. Talentum.
52. The Complete Guide to Salesforce Data Security - Keeping Salesforce Data Safe. (n.d.). Dostupno na: https://appexchange.salesforce.com/partners/servlet/servlet.FileDownload?file=00P4V00000u4drEUAQ [11. studenoga 2023.]
53. Varga, M. (2021) Upravljanje Podacima [online]. Zagreb: Ekonomski Fakultet. Dostupno na: https://books.google.hr/books?id=3HcpEAAAQBAJ&printsec=frontcover&hl=hr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [23. listopada 2023.]
54. Velte, A., Velte, T., Robert, N., York, C., San, F., Lisbon, L., Madrid, M., City, M., New, D., San, J. and Singapore (2010). *Cloud Computing: A Practical Approach*. [online] Dostupno na: https://ds.amu.edu.et/xmlui/bitstream/handle/123456789/9207/CloudComputing.pdf?sequence=1&isAllowed=y [30. studenoga 2023.]
55. Wayburn, J. (2023). Salesforce Security: Preventing Breaches and Malware Threats. [online] Perception Point. Dostupno na: https://perception-point.io/guides/cloud-storage-security/salesforce-security-should-be-concern/ [27. listopada 2023.]

Popis slika

Životopis

europass

Alen Kanceljak

Kućna : Družilovec 80, Veliko Trgovišće, 49214, Veliko Trgovišće, Hrvatska

E-adresa: alen.kanceljak1999@gamil.com **Telefonski broj:** (+385) 0999573543

Datum rođenja: 14/08/1999 **Državljanstvo:** hrvatsko

O MENI

Otvoren za promjene koje doživljavam kao priliku za unaprjeđenje poslovanja i samog sebe.

RADNO ISKUSTVO

[2022 – Trenutačno] **Junior Tehnical Salesforce Consultant**

LeverUP Consulting Adria d.o.o.

Mjesto: Zagreb | **Zemlja:** Hrvatska

Rješavanje tehničkih izazova i pružanje savjeta klijentima.

OBRAZOVANJE I OSPOSOBLJAVANJE

[2018 – Trenutačno] **Student**

EKONOMSKI FAKULTET ZAGREB https://www.efzg.unizg.hr/

Adresa: Trg John F. Kennedy 6, 10000, Zagreb, Zagreb |

[2014 – 2018] **Srednja stručna sprema**

Gimnazija Antuna Gustava Matoša Zabok http://www.gimagm.hr/

Adresa: prilaz Janka Tomića 2, 49210, Zabok |

JEZIČNE VJEŠTINE

Materinski jezik/jezici: Hrvatski

Drugi jezici:

Engleski

SLUŠANJE B2 **ČITANJE** B2 **PISANJE** B2

GOVORNA PRODUKCIJA B2 **GOVORNA INTERAKCIJA** B2

talijanski

SLUŠANJE A2 **ČITANJE** A2 **PISANJE** A2

GOVORNA PRODUKCIJA A2 **GOVORNA INTERAKCIJA** A2

njemački

SLUŠANJE A2 **ČITANJE** A2 **PISANJE** A2

GOVORNA PRODUKCIJA A2 **GOVORNA INTERAKCIJA** A2

Razine: A1 i A2: temeljni korisnik; B1 i B2: samostalni korisnik; C1 i C2: iskusni korisnik

DIGITALNE VJEŠTINE

Moje digitalne vještine

Certified Salesforce Administrator | Salesforce Certified Marketing Cloud Account Engagement Specialist | Salesforce Certified Marketing Cloud Account Engagement Consultant | Microsoft Office | Google Drive | - SQL – Basic | Internet user

VOZAČKA DOZVOLA

Automobili: B