UNIVERZA V MARIBORU

FAKULTETA ZA ELEKTROTEHNIKO,

RAČUNALNIŠTVO IN INFORMATIKO

Sašo Kolac

Izračun donosnosti naložbe v sistem upravljanja identitet in pravic dostopa

Magistrsko delo

Maribor, julij 2020

Zahvala

Zahvala mentorju in somentorju za vodenje, pomoč
in predloge pri izdelavi magistrske naloge.

Posebna zahvala družini in punci za podporo.

Izračun donosnosti naložbe v sistem upravljanja identitet in pravic dostopa

Ključne besede: upravljanje dostopa, upravljanje identitet, One Identity Manager, izračun donosnosti

UDK: 004.451.4:004.777(043.2)

Povzetek

V tej magistrski nalogi pregledamo osnove upravljanja uporabniških pravic in identitet, ter se podrobneje spustimo v izračun donosnosti naložbe v takšne sisteme. Ugotovimo kje in kako pridobiti potrebne podatke in kako jih uporabiti pri izračunih. Opravimo dejanske izračune in primerjamo rezultate, s pomočjo katerih lahko ugotovimo, če se takšen sistem v našem okolju splača in v kolikšnem času se nam investicija povrne. Predstavimo tudi spletno aplikacijo, katera nam avtomatizira približek izračuna z le nekaj potrebnimi osnovnimi podatki.

Calculation of the return on investment in identity and access management system

Keywords: access management, identity management One Identity Manager, calculation of the return on investment

UDC: 004.451.4:004.777(043.2)

Abstract

In this master's thesis, we review the basics of managing user rights and identities, and go into more detail in calculating the return on investment in such systems. We find out where and how to get the necessary data and how to use the accumulated data in calculations. We perform actual calculations and compare the results, with the help of which we can determine if such a system is good for our environment and in what time the investment will pay off. We also present a web application that automates the approximation of the calculation with only a few basic data.

KAZALO SLIK

1. UVOD

V preteklih mesecih smo, ob ustavitvi delovnih procesov različnih podjetij, bili priča odgovorne in pomembne vloge varnostno-informacijskih sistemov. Zaradi Covid-19 so se čez noč ustavili ustaljeni delovni procesi ob odsotnosti urejenih varnih povezav in prirejenih sistemov za delo od doma.

Ena izmed rešitev je lahko upravljanje identitet in pravic dostopa z One Identity Manager-jem. Vendar takšni sistemi predstavljajo veliko začetno investicijo, upravljanje stroškov pa je v trenutnem času izjemnega pomena, saj je večina podjetij zaradi pandemije utrpela gospodarsko škodo. V večini manjših podjetij se takšen sistem finančno ne splača, v večjih podjetjih pa si lahko investicijo povrnemo v le nekaj letih in dolgoročno prihranimo zajetno vsoto.

V magistrskem delu se osredotočam na analizo donosnosti naložbe in s tem povezanimi izračuni. Torej, pogledali bomo kako izračunati donosnost takšne naložbe in na kaj moramo pri izračunih biti pazljivi. Ob koncu izračuna bomo lahko iz analize sklepali ali se takšna naložba splača in v kolikšnem času se morebiti povrne. Primerjali bomo stroške z in brez upravljanja identitet in pravic dostopa ter ugotovili katere vse podatke potrebujemo za izračun in kje pridobiti te podatke, da bodo čim bolj aktualni in ažurni. Prav tako bomo pogledali spletno aplikacijo za približek izračuna donosnosti (slika 7.3), ki smo jo razvili. Ta na podlagi vnosa osnovnih podatkov poda grob izračun donosnosti in izriše preprost graf za lažjo predstavitev stroškov.

Najprej bomo na kratko opisali problem tako s finančnega vidika kot tudi z vidika pravic dostopa in varnosti v oddaljenih sistemih. Slednji so v trenutnem času še kako aktualni. Za tem bomo pogledali predlagano rešitev s finančnega stališča in v naslednjem poglavju to rešitev bolje tehnično predelali. Pogledali bomo kaj je upravljanje identitet in pravic dostopa, kakšne so prednosti in slabosti in opisali priporočen oziroma uporabljen produkt za upravljanje identitet ter pravic dostopa. Na kratko bomo opisali dobre prakse pri upravljanju identitet in zakaj so pomembne. Sledilo bo poglavje o pridobivanju vseh potrebnih podatkov, o tem zakaj so pomembni ažurni podatki in zakaj je pomembno pravilno pridobivanje podatkov. Sledi poglavje o dejanskem izračunu stroškov, izračun

investicij potrebnih za implementacijo sistema in primerjava stroškov ter izračun časa donosnosti naložbe. Na koncu pa sledi še poglavje o opisu dejanske implementacije spletne aplikacije ter sklep oziroma zaključek.

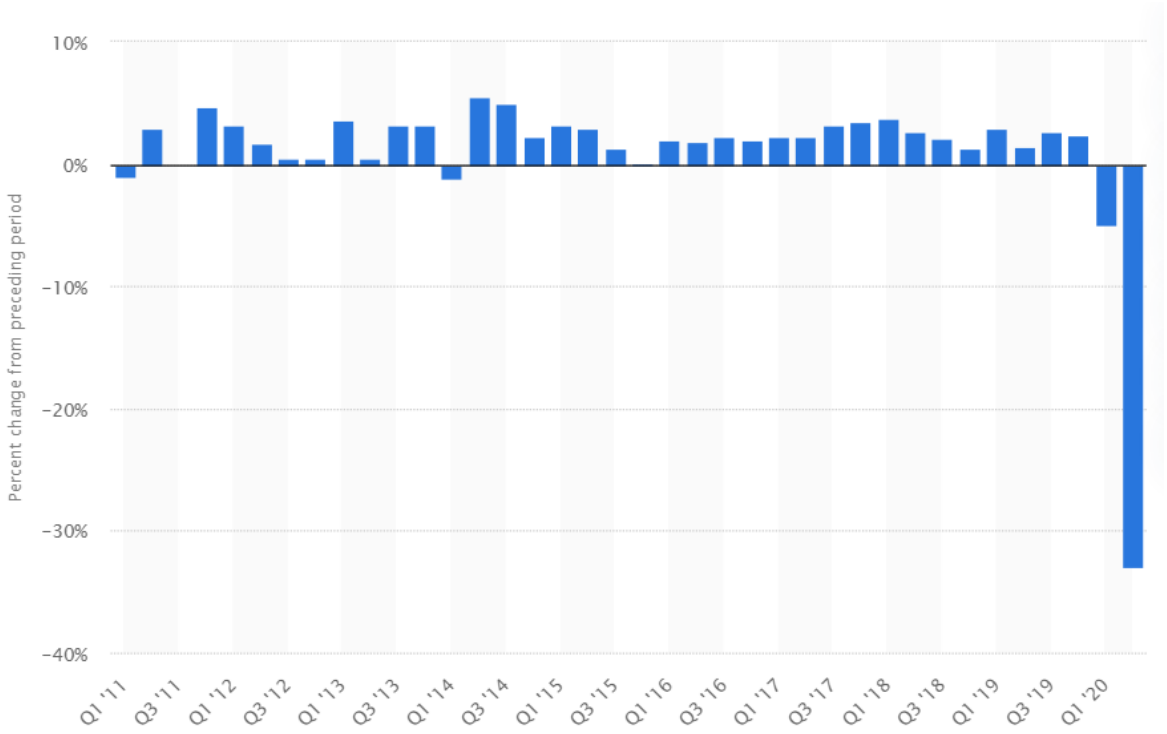
2. OPIS PROBLEMA

Vodstvo podjetja se mnogokrat ne zaveda kako velik strošek predstavlja upravljanje uporabniških identitet in pravic dostopov brez ustreznega sistema. V uvid moramo vzeti tudi porabljen čas, manjšo varnost in več vloženega truda. Vložek je navidezno manjši, ker je porazdeljen, vendar je tak način razmišljanja ekonomsko neupravičen zaradi neupoštevanja nefinančnih aspektov sprotnega dela in vlaganj.

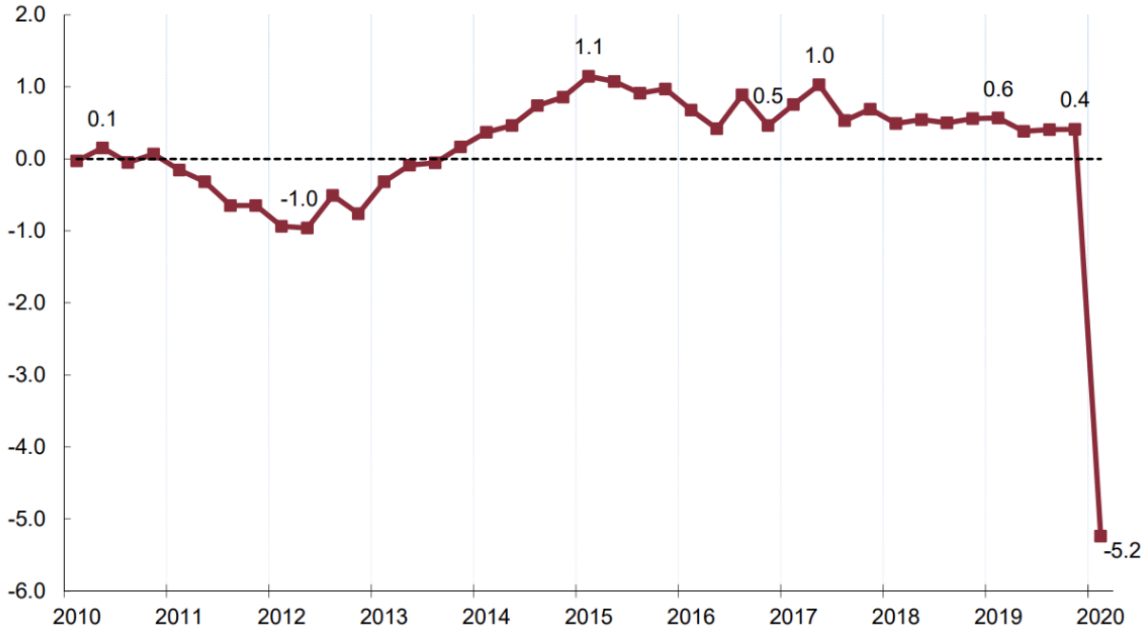
Mnoga podjetja s takšnim načinom razmišljanja po nepotrebnem zapravijo na tisoče evrov tedensko, namesto, da bi s tem povezane stroške precej omilili z ustreznim sistemom. Zaradi visokega prikaza začetne investicije so tudi tisti, ki aktivno razmišljajo o uvedbi sistema za upravljanje uporabniških pravic in dostopov, zelo hitro odvrnjeni in posledično hitro opustijo idejo o spremembah »statusa-quo« brez natančnih analiz. Obstajajo tudi manjša podjetja, ki takšnih sistemov ne potrebujejo ali pa jim ne predstavljajo dodane vrednosti.

Kako veliko podjetje pa mora biti, da se uvedba takšnega sistema splača? O koliko stroških govorimo? Kaj se z vpeljavo takšnega sistema spremeni? So spremembe potrebne? Vprašanj je veliko.

V času trenutne krize ima večina podjetij precej manj sredstev za nove naložbe, saj so imeli upočasnjene ali pa celo ustavljene poti dohodkov. Sredstva so morali prerazporediti tako, da lahko nemoteno poslujejo in prebrodijo težave. Države so podjetjem zagotovile precej pomoči, vendar se ta v večini primerov ne more primerjati z izgubo dohodkov. Da je kriza občutna lahko vidimo na spodnji sliki (slika 2.1), ki prikazuje razliko v bruto domačem proizvodu Združenih držav Amerike od leta 2011 do 2020, porazdeljeno kvartalno.[13] Podobno situacijo lahko vidimo tudi za Evropsko Unijo, kot je na prikazano na sliki od leta 2010 do prve četrtine leta 2020 (slika 2.2).[15]



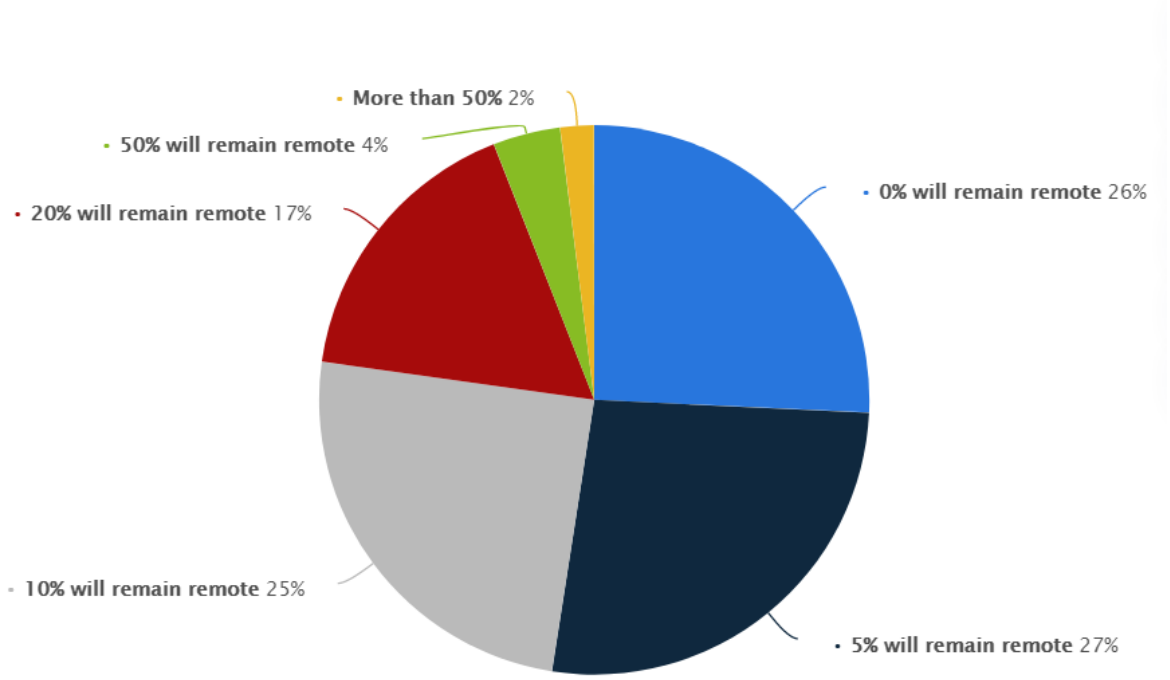
Slika 2.1: Razlika v bruto domačem proizvodu Združenih držav Amerike



Slika 2.2: Razlika v bruto domačem proizvodu Evropske Unije

Zaradi zagotavljanja varnosti svojih zaposlenih je bilo precej podjetij primoranih zapreti svoja vrata in omogočiti zaposlenim, v največji možni meri, delo od doma oziroma povsod, kjer je bilo mogoče. Na tej točki je veliko podjetij ugotovilo, da za takšno vrsto dela nimajo

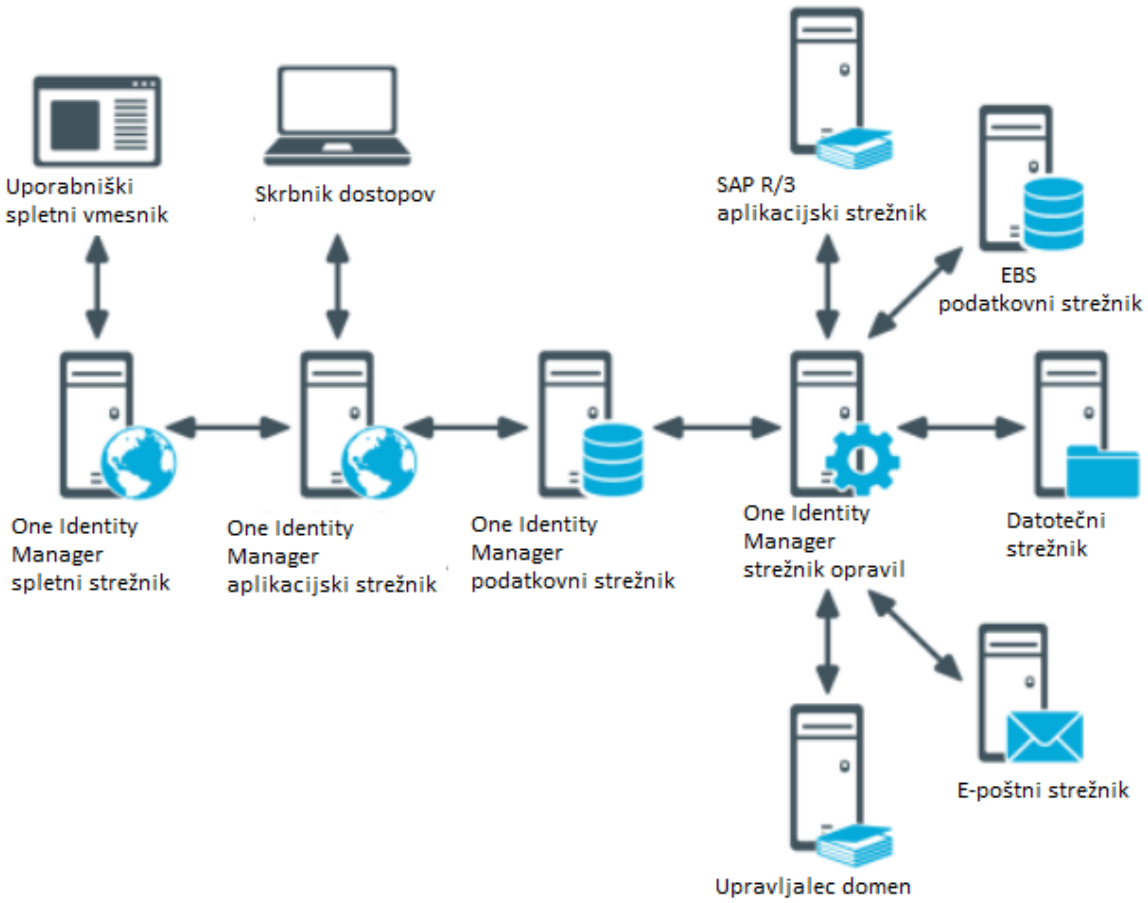
urejenih pravic dostopov. Ker predhodno niso imeli pravilno urejene arhitekture, so sedaj morali na silo uveljaviti začasne rešitve, ki so imele negativen vpliv na sredstva v podjetjih. Po nekaj mesecih uporabe drugačne arhitekture je mnogo podjetij ugotovilo, da je delo od doma prednost in ne slabost. Na spodnji sliki (slika 2.3) lahko vidimo koliko podjetij bo ohranilo kolikšen odstotek ljudi pri delu od doma tudi po koncu krize (vprašalnik je izveden na več sto naključnih ameriških podjetjih).



Slika 2.3: Koliko podjetij bo po krizi ohranilo delo od doma za kolikšen odstotek zaposlenih

3. PREDLAGANA REŠITEV PROBLEMA

Odločili smo se, da razvijemo na videz preprosto aplikacijo, ki na podlagi osnovnih podatkov izračuna približek realnega stanja z in brez sistema za upravljanje identitet in pravic dostopa. V našem primeru je predlagana rešitev sistem za upravljanje identitet in pravic dostopa One Identity Manager, ki nudi vse potrebno za uspešno upravljanje identitet in dostopov. Na spodnji sliki (slika 3.1) lahko vidimo primer arhitekturne postavitve z produktom One Identity Manager.



Slika 3.1: Primer arhitekture postavitve sistema

Sistem je zelo prilagodljiv potrebam posameznega podjetja. Vpeljava takšnega sistema za upravljanje identitet in pravic dostopa predstavlja kar zajetno začetno naložbo, vendar pa se takšna naložba lahko povrne v precej kratkem času. Ker želimo povračilo naložbe v najkrajšem možnem času, je smiselno najprej narediti analizo in izračune, s katerima lahko ugotovimo kdaj in do katere mere bo naložba donosna. Najpomembnejši del rešitve je

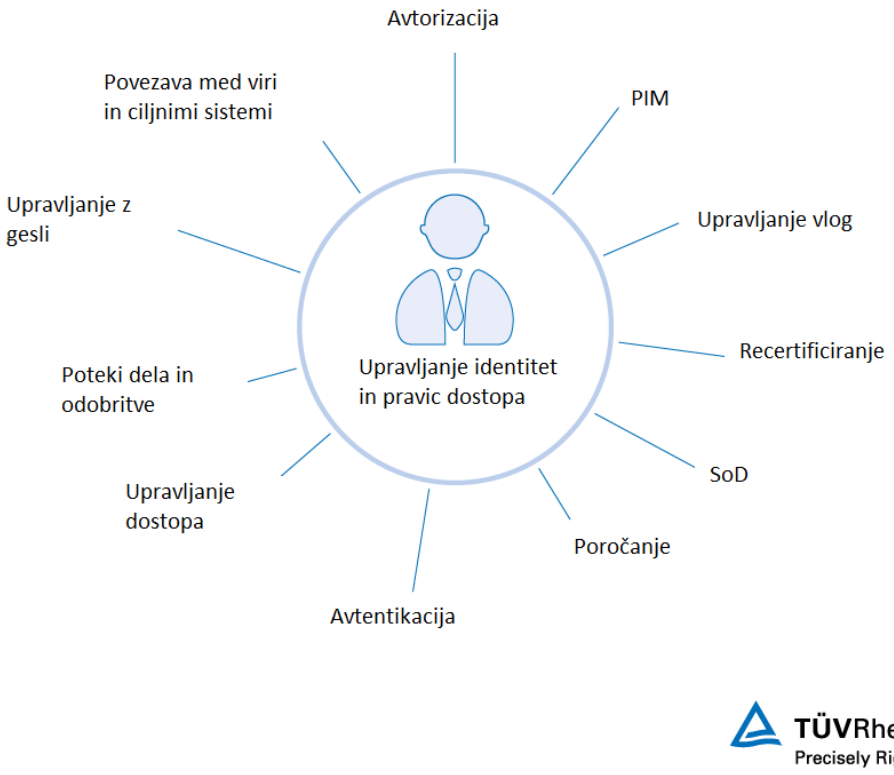
ravno izračun. Potrebujemo ažurne, aktualne in pravilne podatke, saj bo le tako analiza pravilna. Prostora za prirejanje podatkov in izmišljevanje boljšega stanja, kot je dejansko, pri takšnih izračunih ni. Najbolj kvalitetni so realni podatki. Če pri vnosu naletimo na zaplet in realnega podatka ne moremo pridobiti, je potrebno vzeti »slabši« približek, ki nam sicer zviša stroške, vendar poda natančnejšo projekcijo donosnosti naložbe.

Bolje je če projeciramo slabšo donosnost, saj s tem zavajamo sami sebe in se lahko takšen sistem hitro iz poskusa optimizacije spreobrne in nam prinese škodo.[5]

4. UPRAVLJANJE UPORABNIŠKIH PRAVIC IN IDENTITET

4.1.Splošno

Najprej razjasnimo kaj sploh je upravljanje uporabniških pravic in identitet. Gre se za določitev in upravljanje vlog in privilegijev dostopa posameznih uporabnikov omrežja ter okoliščin, kjer so uporabnikom dodeljeni ali odvzeti privilegiji. Glavni cilj je imeti eno digitalno identiteto na posameznika, saj lahko tako vsakemu posamezniku določamo privilegije in dostope. Digitalno identiteto pa je, po vzpostavitvi, potrebno vzdrževati, spreminjati in spremljati skozi celoten življenjski cikel za vsakega posameznika. Splošni cilj upravljanja uporabniških pravic in identitet je omogočiti dostop do ustreznih sredstev podjetja pravim uporabnikom v pravem kontekstu, od pridružitve h podjetju pa vse do odhoda iz podjetja. Grobo rečeno, upravljanje identitet zahteva vsa spodaj prikazana področja (slika 4.1). [1]



Slika 4.1: Zajem upravljanja identitet

Sistemi za upravljanje uporabniških pravic in identitet oskrbujejo skrbnike sistemov z orodji in tehnologijami za lažje spreminjanje vlog posameznikov, spremljanje dejavnosti in dejanj posameznikov ter sprotno uveljavljanje varnostnih politik. Sistemi so zasnovani tako, da omogočajo dostop do uporabnikov v celotnem podjetju in zagotavljajo skladnost tako s politikami podjetja kot tudi z vladnimi predpisi. Takšni sistemi so zgrajeni z mnogimi tehnologijami in funkcionalnostmi, ki jih lahko vidimo na sliki (slika 4.2) in vključujejo tudi bolj prepoznavne, ki so naštete spodaj:

- Vmesnik za programiranje aplikacij je funkcionalnost varnosti, ki omogoča upravljanje identitet za veleprodajno usmerjena podjetja in trgovine, ki temeljijo na mikro storitvah. Prav tako omogoča integracijo z oblakom. Največ se uporablja za tako imenovano enojno prijavo v aplikacije, kjer skrbi za upravljanje avtorizacije z internetom stvari in tako pridobiva podatke o privilegijih posameznika.

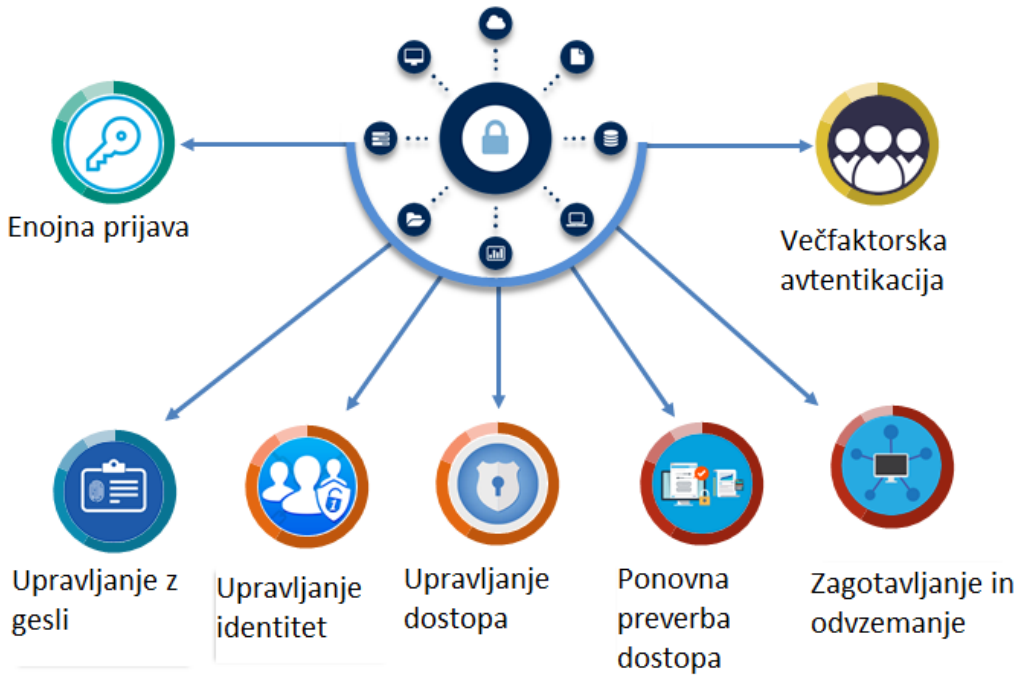
- Analitika identitete, ki nam omogoča detekcijo tveganega obnašanja posameznikov. S pomočjo strojnega učenja, statističnih algoritmov in nastavljenih pravil prepreči tvegano delovanje posameznika tako, da mu v primeru tvegane zaznave, odvzame privilegije, s katerimi bi lahko uporabnik povzročil kakršnokoli škodo podjetju ali drugim posameznikom.

- Upravljanje identitet in dostopov stranke nam omogoča avtentikacijo in celovito upravljanje uporabnikov. Sem sodi tudi upravljanje odnosov s strankami, načrtovanje virov in povezovanje do podatkovnih baz.

- Avtentikacija na podlagi tveganja, pri kateri sistem sam, s pomočjo pravil generira oceno tveganja, na podlagi katere se določi vrsta posameznikove avtentikacije. V primeru visokega tveganja je dober primer obvezna uporaba več faktorske avtentikacije.

- Identiteta kot storitev je funkcionalnost, ki ponuja enojno prijavo v aplikacije in rezervacije uporabniških računov.

- Upravljanje in načrtovanje identitet, ki omogoča avtomatiziranje in ponavljanje procesov za urejanje življenjskega kroga identitet



Slika 4.2: Funkcionalnosti sistema za upravljanje identitet

Če želimo imeti učinkovit sistem za upravljanje uporabniških identitet in pravic dostopov, moramo sistemu podati ažurne, celovite in usklajene podatke. Na podlagi prejetih podatkov lahko sistem izvaja razne aktivnosti in procese, ki lahko upravljajo z vsemi viri v organizaciji ter odvzemajo, dodajajo in urejajo pooblastila dostopa posameznikov.[14]

Če poskusimo obrazložiti izraz upravljanje identitet in pravic dostopov v eni povedi, bi rekli, da je to izraz, ki se nanaša na upravljanje posamezne identitete znotraj nekega sistema (podjetje, država, omrežje, ipd.). Uporablja se znotraj podjetja za vzpostavitev in upravljanje vlog ter pravic dostopov posameznih uporabnikov v omrežju. Sistem za upravljanje zagotavlja odgovornim orodja in tehnologije za nadzor dostopov uporabnikov do določenih virov organizacije. Glavna funkcionalnost sistema je povečanje varnosti in produktivnosti in zmanjšanje stroškov ter pohitritev ponavljajočih se nalog povezanih z upravljanjem pravic dostopov. Te med drugim vključujejo uporabnikovo ustvarjanje, brisanje, zaklepanje, odklepanje, kot tudi odobritev in preklic dostopov. [18] Uporabniki s preveč pravicami v sistemu lahko privedejo do varnostnih incidentov znotraj podjetja.

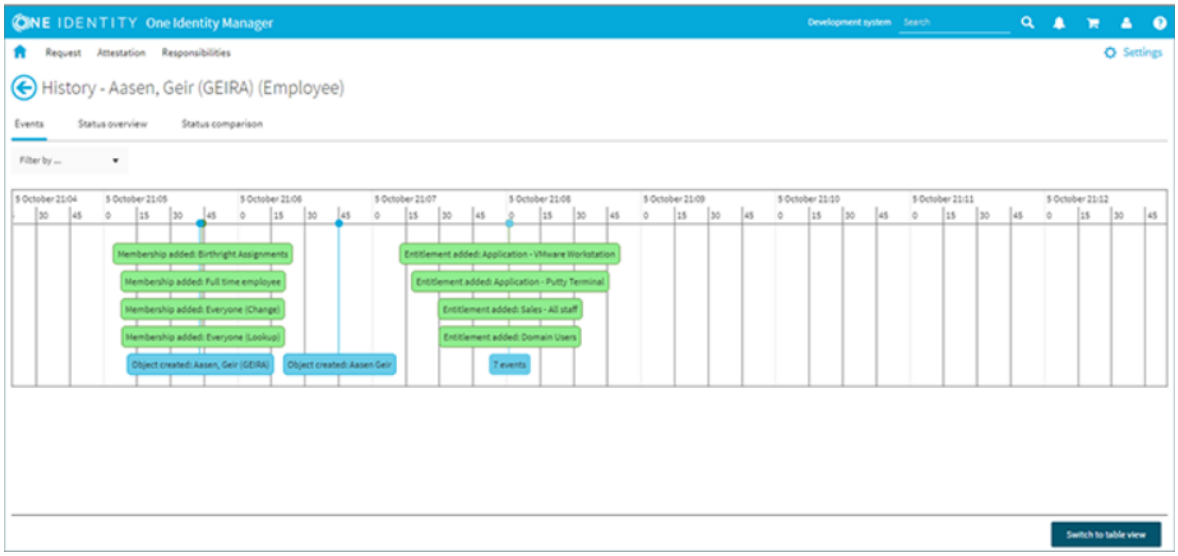
Izboljšana varnost, s pomočjo sistema za upravljanje identitet, zagotavlja pristnost dostopa uporabnika do virov in informacij in pravilno uporabo le-teh. [19]

Zaradi vedno večje potrebe uporabnikov in organizacij po prepoznavanju in upravljanju identitet, so se funkcionalnosti upravljanja bile primorane razširiti iz osnovnih namenov, kot so avtorizacija, storitve imenikov, overjanje in zagotavljanje dostopa. Nove funkcionalnosti zajemajo enotne prijave, spremljanje odgovornosti, avtomatizacijo potekov dela, storitve repozitorijev, enotne spletne prijave, nadzore dostopov na podlagi varnostnih politik, samodejno zaznavanje goljufij, ponastavitev podatkov in še mnogo drugih. [20]

4.2. Izzivi

Potreba po robustni strategiji upravljanja identitet postaja vedno večji del podjetniške informatike. Dobre rešitve lahko podjetjem omogočajo večjo produktivnost zaposlenih in okrepijo splošno varnost v podjetju. Upravljanje identitet in pravic dostopov je zaradi računalništva v oblaku in mobilnega dela vedno bolj kompleksno, kar pomeni, da je lahko brez ustreznega sistema upravljanje identitet zelo zapleteno. Dober sistem takšno upravljanje precej olajša.

Ekipe v podjetju, ki skrbijo za preverjanje uporabniških identitet in upravljanje dostopov do virov podjetja morajo precizno delovati, saj skrbijo za varnostni nadzor podjetja med racionalizacijo postopkov za povečanje produktivnosti uporabnikov informacijskega sistema. Upravljanje identitet in pravic dostopov je bistven del zagotavljanja spodbude uporabnikov pri zagotavljanju vrednosti podjetja, saj preprečuje škodovanju podjetja in skrbi za osnovno varnost tako podjetja kot uporabnikov. Zaradi takšnih razlogov morajo podjetja dobro premisliti o spremembi strategije upravljanja uporabniških pravic in identitet. Preden se odločijo, da bodo spremenili strategijo ali uporabili kakšen sistem, ki je posvečen upravljanju identitet, se morajo podjetja zavedati nekaterih najpomembnejših trendov v pristnosti identitet in upravljanju dostopa do korporativnih aplikacij ter virov podjetja. Splošna varnost informacijskega sistema postaja iz dneva v dan bolj zapletena, s tem pa tudi strategija in sistem za upravljanje identitet, ki se morata še naprej razvijati z napredovanjem varnostnih groženj in izzivov. To podjetju pomaga pri soočanju in reševanju problematik, kar omogoča dinamično rast.[11]



Slika 4.3: Pregled zgodovine dogajanja uporabnika

Dinamična rast podjetja pa je še kako zelo pomembna, saj je potreba po agilnih sistemih vedno večja in se podjetja morajo prilagajati nenehno se razvijajočim izzivom ter novim priložnostim. Hitrost prilagoditve je najpomembnejši faktor pri informacijskih sistemih, kar pomeni, da obstaja večen pritisk na informatiko podjetja, da hitro in brezhibno zagotavlja informacijske vire podjetja vsem uporabnikom, ki jih v določenem času potrebujejo. Potreba po hitrosti pa mnogokrat prinese večja varnostna vprašanja, ki so zaradi vedno večjega izkoriščanja sistemov (pa naj bo zaradi specializiranega hekerskega napada, zaradi prepočasnega odvzemanja privilegijev ali pa zaradi česa tretjega) skoraj najbolj pomemben del podjetja. Če se podjetje želi soočiti s takšnimi napadi, je začetna strategija strogo urejen in varen dostop do podatkov in virov podjetja. Strategije upravljanja privilegijev pogosto delujejo v sklopih, pri čemer je posamezen sklop nameščen v posameznem oddelku podjetja. Vsak sklop mora skrbeti za varnost informacij, odgovornost dostopa do virov in skladnostjo s predpisi. Ker pa vsak oddelek pogosto prilagaja privilegije dostopa s tem, da najbolje ustrezajo poslovanju in ciljem, zahteve ostanejo neizvršene. Takšen pristop lahko hitro pripelje do neskladnosti varnosti in izgube produktivnosti. Postavljanje in uveljavljanje celovite strategije upravljanja privilegijev je lahko bolj zapletena in dražja kot enostavna uvedba tehnologije, vendar pa lahko podjetja, če je strategija pravilno izvedena, dosežejo večjo operativno učinkovitost, poenostavljeno skladnost s predpisi in posledično tudi večje zadovoljstvo uporabnikov. Za uspešno izvedbo sistema za upravljanje identitet se je tako potrebno soočiti s kar nekaj izzivi:

- Vedno bolj razpršeno delovno silo. Eden izmed načinov kako lahko organizacije zaposlijo in obdržijo dober kader je odprava geografske omejitve in ponudba prilagodljivega delovnega okolja. Takšna delovna sila podjetju omogoča povečanje produktivnosti, omogoča nadzor stroškov in zaposlene povezuje z lokalnimi pisarniškimi nastavitvami okolja. Podjetje pa se z oddaljenim načinom dela trudi, poleg ohranjanja dobre izkušnje za zaposlene, ohranjati tudi varnost. Vendar pa rast mobilnega računalništva pomeni, da ima podjetje manjšo vidnost in nadzor nad delovnimi praksami zaposlenih. Celovita in centralno vodena rešitev upravljanja identitet in pravic dostopov podjetju vrača vidnost in nadzor za vsakega zaposlenega posameznika, ne glede na to kje in kdo je.

- Porazdeljene aplikacije. Z rastjo aplikacij v oblaku in programske opreme kot storitve, se uporabniki vedno bolj pogosto prijavljajo v kritične poslovne aplikacije (npr. Office365), v katere se lahko prijavijo kadar koli, od koder koli in s katero koli napravo. Takšne aplikacije povečajo zapletenost upravljanja identitet, saj brez upravljanja žrtvujemo varnost, z upravljanjem pa nam naraščajo stroški podpore frustriranih uporabnikov. Zato je pomembno, da je rešitev celovita in pravilno vzpostavljena, saj nam le tako pomaga pri nadzoru in poenostavitvi privilegijev dostopa, ne glede na to ali se gre za aplikacije v podatkovnih centrih, zasebnih oblakih, javnih oblakih ali pa hibridni kombinaciji.

- Produktivno upravljanje. Brez ustreznega sistema za upravljanje pravic dostopov mora osebje informatike dostope dodeljevati in odvzemati ročno. Dlje kot traja dodeljevanje dostopov uporabniku, manj je uporabnik produktiven. V primeru, da uporabnik zapusti organizacijo ali je premeščen na drug oddelek, lahko pride do resnih varnostnih posledic, če pravice dostopa niso pravočasno odvzete oziroma prilagojene. Za reševanje tega izziva se mora okno med odločbo in dejansko izvedbo o spremembi pravic dostopa zmanjšati na minimum. Na žalost v mnogih organizacijah to poteka tako, da mora iti ekipa informatike skozi vsak račun uporabnika, pogledati do katerih virov lahko dostopa in do katerih ne sme ter nato ročno prirediti dostop. Ročno upravljanje pravic dostopa je delovno intenzivno in nagnjeno k človeškim napakam. To velja zlasti za velike organizacije, pri katerih takšno upravljanje ne pride v poštev, saj ni učinkovito in trajnostno. Takšnem izzivu

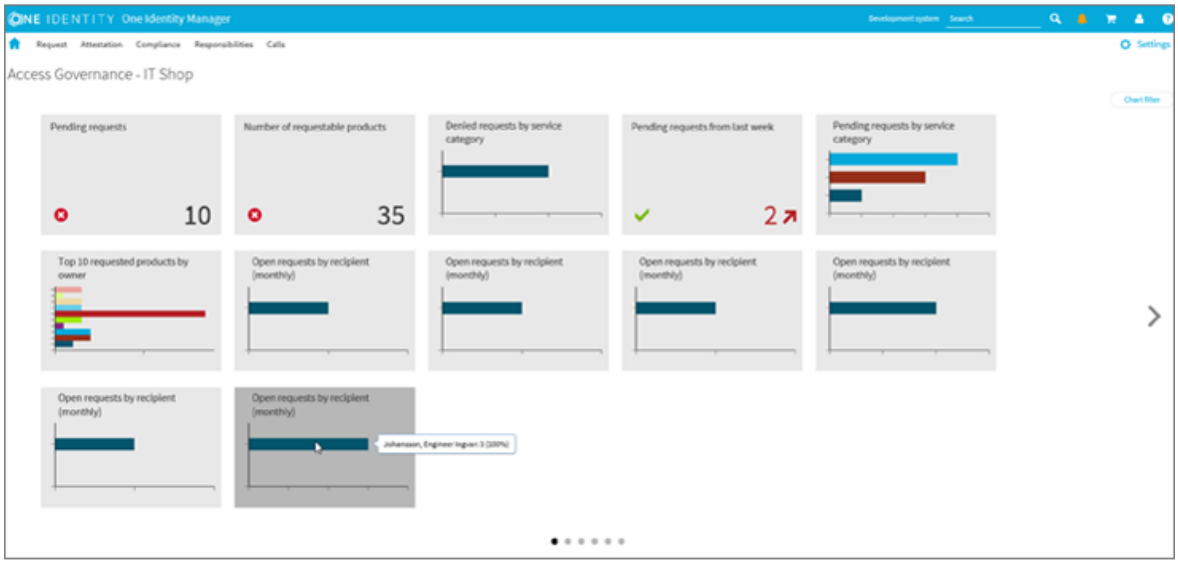
zadosti robustnost sistema za upravljanje identitet in pravic dostopov, saj lahko v celoti avtomatizira postopek zagotavljanja in odstranjevanja pravic in s tem poda ekipi za informatiko celostno moč pri pregledu nad uporabniki in organizacijo. Samodejno zagotavljanje in odstranjevanje pohitri izpopolnjenje močnih varnostnih politik in hkrati pomaga pri preprečevanju človeških napak.

- Uporaba lastniških naprav. Podjetja se danes soočajo tudi z izzivom osebnih naprav zaposlenih in z odločitvijo ali morajo te naprave biti upravljane ali ne. Zaposleni, partnerji, gosti in drugi vnašajo osebne naprave in se z njimi povezujejo v omrežje podjetij iz poklicnih in osebnih razlogov. Izziv ni v preprečitvi povezovanja v omrežje organizacije, ampak ali se lahko organizacija dovolj hitro odzove in zaščiti poslovna sredstva, ne da bi pri tem trpela storilnost, produktivnost in svoboda uporabnikov omrežja. Nekatera podjetja že imajo varnostno politiko za osebne naprave, ki uporabnikom omogočajo dostop do varnih virov znotraj podjetja, je pa takšna politika lahko precej bolj težavna in zapletena, kot običajen dostop na upravljanih mobilnih napravah in delovnih postajah. Podjetja morajo ravno iz tega razloga razviti strategijo, ki omogoča hitro, varno in enostavno dodeljevanje in odvzemanje pravic dostopa do organizacijskih aplikacij in virov. Ves promet znotraj organizacijskega omrežja mora biti skladen z varnostno politiko in vladnimi predpisi. Poleg mobilnih naprav, je tukaj tudi internet stvari, ki je vedno bolj v uporabi in ga je prav tako treba upravljati in omejevati.

- Gesla. Rast aplikacij v oblaku pomeni, da si morajo zaposleni zapomniti vedno večje število gesel za dostop do raznih aplikacij in sistemov. Ta gesla imajo pogosto različne standarde, zahteve in protokole za overjanje in delitev atributov. Zadovoljstvo uporabnikov je tako vedno manjše, saj posledično porabijo veliko časa za upravljanje gesel. Nekatere aplikacije zahtevajo spreminjanje gesel vsakih 30 dni. Podjetje lahko kot rešitev uporabi združevanje identitete uporabnika in razširijo zmogljivost z enojno prijavo. Enojna prijava integrira upravljanje z geslom na več domenah ter v različnih standardih in protokolih za avtentikacijo.

- Skladnost s predpisi. Skrb glede skladnosti in organizacijskega upravljanja so še naprej med glavnimi vzroki za uporabo sistema za upravljanje identitet in pravic

dostopov. Zagotavljanje podpore za postopke, kot so določitev privilegijev za dostop za določene zaposlene, sledenje odobritev poslovodstva za razširjen dostop in dokumentiranje, kdo je dostopal do katerih podatkov in kdaj je dostopal, lahko precej olajšajo breme skladnosti s predpisi in zagotavljajo nemoten revizijski postopek in revizijsko sled. Ustrezni sistemi za upravljanje identitet in pravic dostopov podpirajo skladnost z regulativnimi standardi in standardi varnosti podatkov. Prav tako omogočajo avtomatizirano revizijsko poročanje, kar močno poenostavi postopke za skladnost s predpisi in pomaga pri ustvarjanju celovitih poročil, potrebnih za dokazovanje skladnosti.



Slika 4.4: Pogled neskladij z določenimi politikami

Vidimo lahko da tradicionalna zaščita ni več dovolj. Podjetja, ki iščejo rešitve za upravljanje identitet in pravic dostopov, morajo upoštevati resničnost vedno bolj mobilne delovne sile in visoko porazdeljene ter zapletene mreže aplikacij. Močen sistem za upravljanje identitet podjetju znatno olajša težave pri upravljanju, poenostavi zagotavljanje in odpravljanje rezervacij in poveča produktivnost uporabnikov, hkrati pa znižuje stroške, zmanjšuje zahteve za informacijsko pomoč v podjetju in zagotavlja izčrpne podatke za pomoč pri izpolnjevanju regulativ in standardov. Podjetja tako zagotovijo varnost z uvajanjem rešitev več faktorske avtentikacije, z zagotavljanjem enojne prijave pa odpravijo določene težave uporabnikov. Dobra rešitev za upravljanje identitet omogoča odločitve glede na identiteto

posameznega uporabnika, lokacijo, napravo in zahtevani vir. Tako podjetju omogoči hiter dostop, kar pomeni da lahko podjetje enostavno loči med nepooblaščenim in pooblaščenim dostopom. [2]

4.3.Prednosti in slabosti

Z izjemo znatnega začetnega stroška in načrtovanja, sistem za upravljanje identitet in pravic dostopov nima prevelikih slabosti. Generalno gledano nam omogoči bližnjice pri upravljanju, avtomatizaciji in lepšem ter lažjem pregledu. Ker pa omogoča precej veliko različnih funkcionalnosti, imajo določene svoje prednosti in slabosti.

Ena izmed takšnih funkcionalnosti je enojna prijava. Brez enojne prijave vsako spletno mesto ali aplikacija vzdržuje svojo bazo uporabniških imen in gesel. Običajno, ko se uporabnik prijavi, se najprej izvede povpraševanje o že obstoječi prijavi. Če prijava že obstaja je uporabniku odobren dostop, v nasprotnem primeru pa se uporabnika pozove k prijavi. Po vpisu prijavnih podatkov sistem preveri ali poverilnice ustrezajo tistim, ki so shranjene v bazi in potrdi ali zavrne prijavo. Sistem v primeru uspešne prijave shrani status prijave tako, da lahko potujejo z uporabnikom, kar se lahko dogaja v obliki piškotkov, sej ali pa strežniškega spremljanja. V primeru enojne prijave pa se overitev uporabnika opravlja s pomočjo zaupanja med različnimi spletnimi storitvami. Bolj znan, vsakdanje uporabljan podoben primer enojne prijave je, ko nas spletna stran ali aplikacija vpraša ali se lahko v aplikacijo prijavimo z Google računom. V tem primeru sistem omogoča prijavo s pooblastili drugega sistema, kateremu zaupa pri preverjanju uporabniške identitete. Torej, enojna prijava nam omogoča, da se podatki o preverjanju pristnosti uporabnika pomikajo med več prijavnimi sistemi skupaj z uporabnikom. Podatki enojne prijave potujejo prek žetonov, kar omogoča zadostno varnost, hitrost in zmogljivost. Kot dober primer enojne prijave je rešitev Active Directory, ki omogoča obisk novih domen, povezanih z enim ponudnikom prijave, ne da bi se morali še enkrat prijavljati. Torej, kakšne so prednosti in slabosti enojne prijave?

Prednosti:

- Število gesel. Če si mora uporabnik zapomniti samo eno geslo je veliko bolj zadovoljen, kot pa v primeru da si mora zapomniti vsa gesla, ki imajo še povrhu več

različnih zahtev in varnostnih politik. S tem se rešimo tudi ponavljanja gesel na različnih storitvah, kar ustvarja veliko varnostno tveganje.

- Moč gesla. Ker si uporabnik mora zapomniti samo eno geslo je velika verjetnost, da bo to geslo močnejše in bolj varno.

- Poenostavitev upravljanja uporabnikov. Ko moramo uporabniku odvzeti pravice, mu lahko z enim odvzemom odstranimo vse poverilnice do celotne organizacijske strukture.

- Krepitev varnosti identitete. Z uporabo večfaktorske avtentikacije je identiteta varnejša.

- Poveča hitrost in produktivnost. Manjša verjetnost pozabljenih gesel ter ponastavitev in manjše število prijav povečata produktivnost pri vsakemu uporabniku.

- Manjša podpora uporabnikom. Ker uporabniki redkeje prijavljajo težave z gesli, se ekipa za informatiko lahko lažje osredotoči na ostala dela.

- Zmanjšanje uporabe zunanjih sistemov prijave. Ker za vse prijave skrbimo sami, je za varnost poskrbljeno in nismo odvisni od tretjih oziroma zunanjih sistemov.

Kljub vsem prednostim pa nekaterim organizacijam takšna funkcionalnost ne pride v poštev, saj ima tudi slabosti:

- Močna gesla. Spoštovati je treba postopke za izbiro močnih gesel, saj lahko pride do kaskade kršitev če se razkrije en niz poverilnic enojne prijave.

- Če se strežnik enojne prijave poruši in postane nedostopen, se dostop do vseh povezanih storitev ustavi. Zato je treba pri izbiri biti pazljiv in izbrati zanesljiv in robusten sistem ter pripraviti načrte odzivov v primeru morebitnih težav.

- Če se poruši sistem za upravljanje identitet in pravic dostopov, se z njim poruši tudi povezana rešitev enojne prijave.

- Za pravilno postavitev arhitekture je potrebnega precej časa in priprav. Ker je vsako okolje drugačno, ne obstaja splošni načrt, ampak je treba le-tega pripraviti posamično. Načrt mora biti premišljen in vsebovati vse možne scenarije napak in težav ter odzive na te težave.

- Enojna prijava ni idealna rešitev za več uporabniške delovne postaje.

- V nekaterih okoljih je mogoče potrebna zmanjšana prijava, kar privede do večjih stroškov. Če ima podjetje uporabnike z različnimi stopnjami dostopa, je potrebno vzpostaviti dodatne strežnike za preverjanje pristnosti poverilnic.

Sistem za upravljanje identitet in pravic dostopa je lahko tudi v oblaku, kar pa ima posledično spet svoje prednosti in slabosti. Funkcionalne prednosti so podobne kot pri lokalno postavljeni rešitvi, torej enojna prijava, enostavno in učinkovito upravljanje vlog in dostopov, samopostrežna ponastavitev gesel, olajšano zapisovanje in sledenje, opažanje morebitnih tveganih trendov in prenos tveganja na ponudnika storitev. Slabost pa je to da nimamo nadzora nad samim sistemom, saj so vsi podatki (podatki o zaposlenih, strankah, organizacijah, gesla, telefonske številke…) na strežniku ponudnika storitve. Prav tako je težava v tem, da smo odvisni od ponudnikov storitev in v primeru izpada, ne moremo narediti nič razen počakati, da ponudnik storitve reši težave. Pride lahko tudi do nepooblaščenega izliva podatkov, saj ne moremo vedeti kako ponudnik skrbi za varnost, zato je takšen pristop zgrajen na zaupanju ponudniku storitve.[3][12]

4.4.One Identity Manager

Eden bolj priznanih rešitev za upravljanje identitet in pravic dostopa, je produkt One Identity Manager [16]. Produkt ponuja večino potrebnih funkcionalnosti in je primeren za veliko večino podjetij. Podjetje One Identity, s tem produktom zagotavlja zmanjšanje tveganj, zaščito podatkov in informacij, robustnost brez izpadov in skladnost z uredbami (slika 4.4). Glavna prednost takšnega produkta je, da uporabniku omogoči dostop izključno do tistih sistemov in virov, ki jih uporabnik potrebuje. Z One Identity Manager-jem lahko podjetje poenoti varnostno informacijske politike in izpopolni ter avtomatizira potrebe po upravljanja identitet in pravic dostopa. Produkt izpolnjuje zahteve skladnosti in revizijske

zahteve, ponuja možnost avtomatizirano upravljanje katerega koli sistema, platforme in aplikacije, ima možnost vključitve raznih varnostnih politik za uporabnike (tako privilegirane, kot tudi za tiste brez dovoljenj), omogoča podjetju investicije zunaj lokalnih aplikacij in sistemov, zagotavlja popolno in podrobno revizijsko sled (slika 4.3) in poročila v realnem času, poenotenje politik iz več virov za zmanjšanje tveganja izpostavljenosti, in še mnogo več. Z neprestanimi nadgradnjami in posodobitvami, je One Identity Manager prejel tudi številne nagrade.[5] Med katere spadajo tudi slednje:

- CRN 2020 kot hitro rastoči ponudnik storitve upravljanja identitet

- KuppingerCole 2020, je produkt imenoval za vodilnega na seznamu upravljanja privilegiranega dostopa

- KuppingerCole 2020, je produkt imenoval za vodilnega tudi na seznamu upravljanja identitet in administracije

- Ameriška zvezna vlada, je produkt označila kot skladnega s varnostnimi merili, kar pomeni da je produkt pripravljen prenesti najstrožje varnostne zahteve vladnih in podjetniških organizacij

- Starlingova platforma, je produkt certificirala po sledečih ISO / IEC standardih: 27001:2013, 27017:2015 in 27018:2019. Takšen certifikat izraža infrastrukturo ustrezno za stroge varnostne standarde

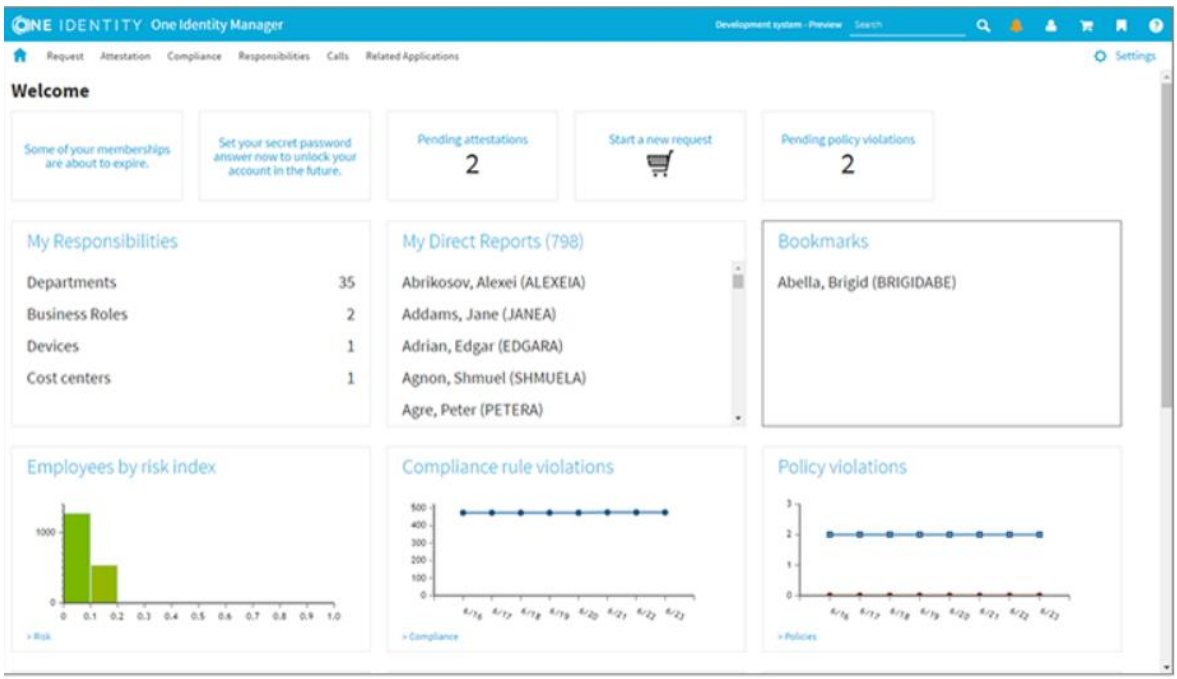
- CRN, je produkt označil z 5 zvezdicami in zmagovalcem leta 2020 v priročniku za partnerske programe

- Info Security, je produktu namenilo srebrno nagrado v kategoriji upravljanja identitet in pravic dostopa 2020

- Info Security, je produktu prav tako namenilo bronasto nagrado v kategoriji upravljanja privilegiranega dostopa in varnosti

- Gartner, je podjetje postavilo med vodilna podjetja pri upravljanju identitet in pravic dostopa, v svojem magičnem kvadrantu za leto 2019

Produkt One Identity Manager ima veliko dobrih lastnosti. Produkt je SAP certificiran, kar pomeni da omogoča globoko napredno integracijo s sistemom SAP z natančno definiranimi zmogljivostmi. Z združevanjem varnostnih informacij in pravilnikov iz več virov, zmanjšamo izpostavljenost in odstranimo tako imenovane podatkovne silose, zaradi česar zmanjšamo tveganje informacij. S pomočjo sistema Starling Connect, se produkt lahko razširi z aplikacijami v oblaku. Na voljo so podrobna revizijska poročila o upravljanju v realnem času, ki vključujejo informacije o tem kakšne vire ima podjetje v okolju, kdo lahko dostopa do njih ter kdaj in zakaj je bil dostop odobren oziroma ukinjen. S avtomatiziranimi sistemi, produkt pomaga odpraviti ročno vnesene napake in zagotavlja, da v katerem koli sistemu, platformi ali aplikaciji ostajajo samo pravilni podatki. S privilegiranim upravljanjem, lahko uporabniki sami zahtevajo dostop do virov, ki je lahko potem na podlagi potreb, odobren ali zavrnjen. Z pregledno vizualno reprezentacijo podatkov, omogoča vidnost in lažji nadzor nad podatki (slika 4.5).



Slika 4.5: Pozdravna stran produkta One Identity Manager

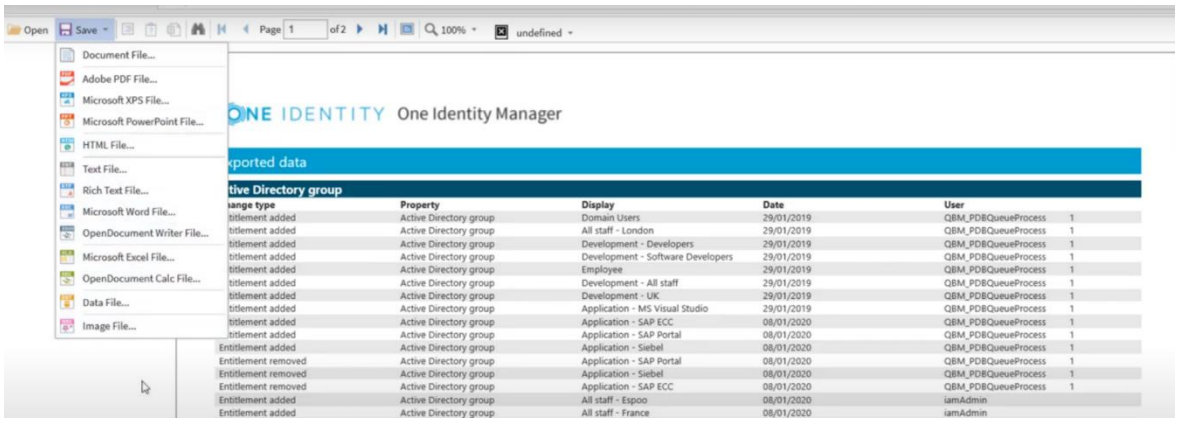
Produkt ima vgrajeno nadzorno ploščo za potrjevanje zahtev, kjer je vidno stanje v jasnem prikazu in kjer se lahko pripravijo podrobna naročila za odkrivanje skladnosti. Ponastavitve gesel in uporabniških računov so mogoče z uporabo nastavitvenih pravil, ki omogočajo

skladnost z več pravilniki o geslih in vlogah uporabnikov. Za večjo varnost pri prijavah v sistem, produkt omogoča integrirano več faktorsko avtentikacijo. Vsak uporabnik (bodisi gost, študent, zaposleni, zunanji izvajalec, partner, stranka, vodja, direktor..) ima dostop izključno samo do podatkov, ki jih potrebuje, s čemer se dolgoročna varnost sistema precej poveča. Za uporabnike produkt omogoča tudi portal do samopostrežnih storitev, kjer lahko uporabniki zahtevajo dostop do omrežnih virov, fizičnih sredstev, skupin in distribuiranih seznamov ter nadzirajo življenjski cikel svoje identitete, kar znatno razbremeni informacijski sektor podjetja.[5]

4.5. Dobre prakse pri upravljanju identitet

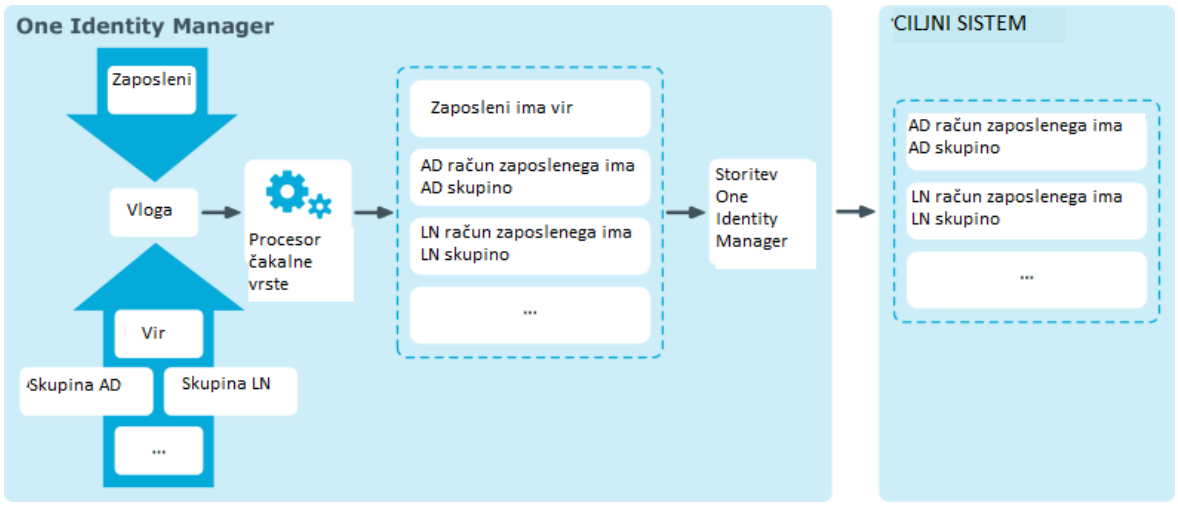
Upravljanje identitet in pravic dostopa ni enkratno opravilo, ampak je tekoči postopek in kritični del organizacijske infrastrukture. Tudi če podjetje že ima obstoječ sistem upravljanja, je pravilno da se spremljajo spreminjajoče se dobre prakse.

Določitev delovne sile je ena izmed pomembnejših dobrih praks. Znotraj organizacije je namreč osebje, ki upravlja ostale zaposleni. Temu oddelku pogosto pravimo oddelek za človeške vire. Upravljati morajo podatke o zaposlenih, gostih, strankah, študentih… Praktično vseh, ki smejo ali ne smejo imeti dostopa do organizacijskih virov. Priporoča se uporaba sistemov za upravljanje s človeškimi viri za pridobivanje podatkov, saj je to najbolj verodostojen vir podatkov znotraj organizacije. S tem se podjetje izogne ponavljajočemu delu, napakam, nedoslednosti in drugim težavam povezanim z rastjo organizacije ter hkrati sistema za upravljanje identitet in pravic dostopa. Najboljše je imeti nekakšen spletni vmesnik, ki nam vizualno zagotovi dostop do kakovosti uvoženih podatkov v sistem, kjer jih lahko preverimo in po potrebi popravimo oziroma prilagodimo. Poleg osebja, ki ureja sistem, je dobra praksa zagotoviti potrebno znanje in nadzor tudi vodstvu organizacije. Preko spletnega vmesnika lahko vodstvo dobi vpogled v realno časovne organizacijske podatke in poročila (slika 4.6).



Slika 4.6: Primer izvoza poročila

Določiti je potrebno tudi različne vrste in obsege identitet. Najboljša praksa je uporabiti enoten integriran sistem, ki samodejno upravlja osnovne identitete in jih onemogoča, ko pride čas za to. Običajno se na začetku uporabijo tri različne vrste identitet. Storitev primarnega imenika, sistem sporočanju in komunikacije ter primarni sistem za načrtovanje virov. Po implementaciji teh treh vrst, lahko po potrebi še dodajamo druge oziroma nove, vendar je potrebno pravilno in natančno načrtovanje pred implementacijo novih vrst sistemov. Ti začetni trije sistemi so nepogrešljivi, dokler ne ugotovimo katere vse ostale sisteme potrebujemo, saj jih uporabniki uporabljajo na dnevni ravni in so najbolj vidni. Vsak ločen sistem bo imel svoje uporabniške račune, katere integriran sistem poveže z identitetami s pomočjo procesov preslikave. Procese preslikav lahko urejamo preko spletne aplikacije, katera nam omogoči grafični pregled nad preslikavami. V večini organizacij, se pojavi kakšna identiteta, katere sistem ne zna preslikati avtomatično in mora to ročno popraviti odgovorna oseba, preko prej omenjena spletnega vmesnika.[4]



Slika 4.7: Potek dela pri ugotavljanju privilegijev glede na vlogo uporabnika

Med bolj pomembne dobre prakse spada tudi implementacija poteka dela. Vedno napredujoča tehnologija spodbuja spremembe, vendar pa lahko ne upravljane spremembe povzročijo precej težav. Implementacija poteka dela o zahtevi in odobritvi, zagotavlja učinkovit način upravljanja in dokumentiranja določenih sprememb. Uporabimo lahko uporabniški vmesnik, ki je običajno v obliki spletne aplikacije, in z njim omogočimo uporabniku samopostrežno storitev, s katero lahko zaprosi za dostop do določenega vira. Skrbnik teh virov se na to prošnjo odzove in s tem zagotovi primerno raven dostopa, hkrati pa razbremeni ekipo informatike v podjetju. Pametno je določiti različne stopnje dovoljenj (slika 4.7), pri čemer vsaka stopnja dobi svoj potek dela. S tem pristopom razbremenimo posameznike in smiselno razdelimo delo. Stopnje dovoljenj so seveda odvisne od sektorja in občutljivosti virov. Pri razbremenjevanju osebja, je smiselno pogledati tudi v avtomatsko upravljanje dostopa. Takšno upravljanje je smiselno na primer, ko podjetje pridobi novega uporabnika ali pa uporabnik zapusti podjetje. Za vsako takšno osnovno spremembo je potrebno storiti veliko manjših stvari (povezave v razne sisteme, e-pošta, dostopi do osnovnih baz podatkov), za kar bi ročno porabili precej časa, za to lahko takšne stvari prepustimo avtomatizaciji.

Posebej je treba izpostaviti tudi skladnost z vladnimi predpisi in uredbami. Dober sistem upravljanja z identitetami in pravicami dostopa lahko precej olajša pot k skladnosti. Vse kar potrebujemo je dobro in jasno definiranje ter dokumentiranje delovnih vlog in dobro definirati delovne vloge, ki nadzirajo te podatke. Potrebna je podrobna določitev pravil skladnosti, pri čemer za vsak korak definiramo tudi odgovorno delovno vlogo. Po določitvi

pravil, je priporočljiva tudi integracija teh pravil v sistem za upravljanje identitet in pravic dostopa, saj nas bo potem sistem sam opozarjal in pomagal preprečiti napake. S tem znatno izboljšamo doslednost, varnost in skladnost.

Že prej smo omenili da je sistem upravljanja identitet tekoče opravilo in ne enkratno. Za dobro in varno okolje, moramo vsake toliko preveriti in prilagoditi pravila dodeljevanja. Pogosto se zgodi, da določene delovne vloge ne potrebujejo enakih virov in dostopov, kot so jih potrebovale v preteklosti. Ne obnavljanje pravil lahko pomeni varnostno tveganje. Običajno takšne preglede in prilagoditve opravljajo skrbniki podatkov ali pa varnostni inženirji v organizaciji. Torej, dovoljenja dodeljujemo delovnim vlogam, v katere potem spadajo posamezniki. Dolgoročno gledano je najbolje določevanje vlog glede na dejanske naloge, ki jih posamezniki opravljajo.[11]

5. PODATKI POTREBNI ZA IZRAČUN

5.1. Pomembnost

Najpomembneje je da so podatki ustrezni in ažurni. Karkoli analiziramo z neustreznimi podatki, lahko pelje do neželenih rezultatov in težav. Ustrezni podatki so nesporni, kar pomeni da organizacije sprejema nove odločitve na podlagi dejstev in ne špekulacij. Ustrezni podatki nam omogočajo, da odgovorimo na vsa vprašanja o teh podatkih. Ustrezni podatki, o katerih se poroča pravilno, niso sporni ali subjektivni. Pri načrtovanju in odločanju o spremembah v organizaciji, so hipoteze, ki temeljijo na ustreznih podatkih, neizpodbitni del za snovanje nove strategije. Strukturirana merila z ustreznimi podatki so ključni del izvajanja strategije, takšna merila pa je pravilno redno primerjati med izvajanjem strategije in v kolikor pride do odstopanj, prilagoditi izvajanje tako, da je odstopanje čim manjše.

Brez ustreznih podatkov, organizacija ne more delati nikakršnih sprememb, niti ne ve kje je potrebna optimizacija. Če želimo nekaj optimizirati pa moramo najprej testirati in tako pridobiti merljive hipoteze, ki temeljijo na ustreznih podatkih (slika 5.1). Pogosto ljudje zamešajo testiranje in optimizacijo. Testiranje je del optimizacije, ki nam omogoča preverbo kakovosti, zmogljivosti in zanesljivosti nekega sistema. Optimizacija pa pomeni, da nek vir izrabimo boljše kot v preteklosti, s pomočjo merljivih hipotez, katere smo pridobili v postopku testiranja. Ustrezni podatki so nezmotni in prav ta nezmotnost nam onemogoči zavračanje rezultatov, pa naj bodo ti še tako slabi. S pomočjo nezmotnih podatkov lahko na primer, ugotovimo katere aktivnosti v organizaciji so bolj donosne od drugih in čas preusmerimo v donosnejše.

Slika 5.1: Primer izrisa in pregleda podatkov

Ustrezni podatki so prav tako pomembni za transparentnost in zaupanje, ter nam pomagajo pri zaščiti organizacije same. Z beleženjem ustreznih podatkov, smo precej bližje skladnosti z raznimi pravili in politikami.[6]

5.2. Opis potrebnih podatkov

Pri izračunu v tej magistrski nalogi, bomo potrebovali kar precej različnih podatkov. Najprej moramo vedeti o kakšnih podatkih govorimo in kaj vsak od teh podatkov pomeni. Najprej bomo podatke ločili na dve vrsti:

- Spremenljive, oziroma tiste, ki jih organizacija vnese v vnosna polja za izračun in so preprosti podatki, katere pozna vsako vodstvo podjetja, brez dodatnih analiz

- Nespremenljive, oziroma tiste, ki temeljijo na povprečjih in ne spadajo pod preproste podatke

Med spremenljive podatke tako štejemo število zaposlenih, oziroma osebe, ki so v podjetju zaposlene na podlagi pogodbe o zaposlitvi (interni zaposleni). Osebe bodisi uporabljajo storitve informatike ali pa se za njih vodi dostop do ne informacijskih virov (npr. mobilni

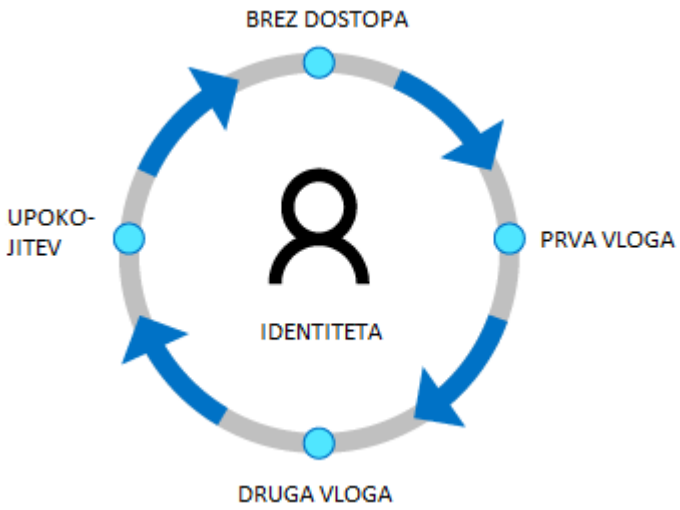
telefon, prenosni računalnik, dostop do prostorov). Število zunanjih uporabnikov sistema, oziroma osebe, ki s podjetjem sodelujejo na podlagi drugega pogodbenega razmerja (na primer zunanji svetovalci in izvajalci storitev, študentje…). Število vseh aplikacij v informacijskem sistemu, kot so Office 365, SharePoint, SAP in ostale. Ocena stroškov za licence za programsko opremo na leto, kar šteje strošek podjetja za nakup in vzdrževanje licenc za programsko opremo letno. Zadnji potreben spremenljiv podatek pa je povprečno število aplikacij v informacijskem sistemu na uporabnika, torej koliko od prej naštetih aplikacij uporablja uporabnik v povprečju.

Pri nespremenljivih podatkih, pa imamo precej večje število podatkov. Te podatke delimo na pod različice:

- Stroški zaposlenih
- Kadrovske spremembe
- Informacijski sistem
- Pomoč uporabnikom
- Revizija in kibernetska varnost

V kategorijo stroški zaposlenih spadajo podatki, ki nam povedo koliko ima organizacija stroškov z zaposlenimi. Tukaj spadajo podatki o mesečni povprečni plači in povezanimi stroški informacijsko sistemskega inženirja, to je postavka, ki vsebuje bruto plačo zaposlenega informacijsko sistemskega inženirja, strošek delodajalca (davek na plače, stroški prevoza in prehrane) ter drugi povezani stroški delovnega mesta (osnovna sredstva). Prav tako nas zanima mesečna povprečna plača in povezani stroški zaposlenega, ki ni informacijsko sistemski inženir. Ta postavka vsebuje bruto plačo zaposlenega, ki ni informacijsko sistemski inženir, v podjetju in strošek delodajalca (davek na plače, stroški prevoza in prehrane) ter drugi povezani stroški delovnega mesta (osnovna sredstva). Zanima nas tudi število delovnih ur na mesec ter urna postavka zaposlenega, tako v informacijskem sektorju, kot izven sektorja, torej mesečna povprečna plača in povezani stroški zaposlenega, deljeno s povprečnim številom mesečnih delovnih ur.

V kategorijo kadrovskih sprememb, uvrščamo podatke spremembah delovnih razmerij zaposlenih (slika 5.2), torej o ocenjenem odstotku novih zaposlitev na letni ravni, glede na prejšnja leta. Prav tako potrebujemo odstotek internih premestitev, torej ocenjen odstotek prerazporeditev na drugo delovno mesto znotraj oddelka ali v drugem oddelku, drugem pridruženem podjetju ali poslovni enoti letno. Prav tako tudi prekinitve delovnega razmerja, oziroma odstotek odhodov na letni ravni, ter spremembe zunanjih uporabnikov sistema, katere prav tako ocenimo v odstotkih. Glede na te odstotke, lahko potem izračunamo ocenjeno število vsake postavke, torej število novih zaposlitev, internih premestitev, odhodov in sprememb zunanjih uporabnikov letno.



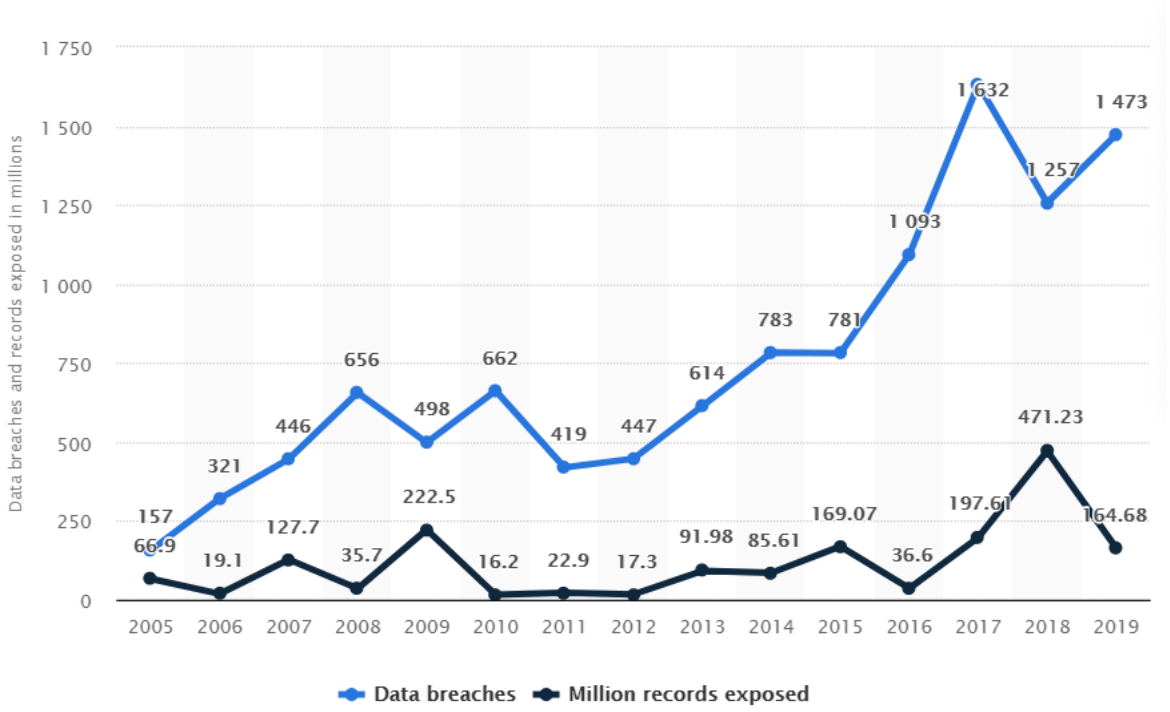
Slika 5.2: Življenjski cikel identitete glede na delovno razmerje

Znotraj kategorije o informacijskih sistemih imamo podatek o povprečnem številu uporabnikov posamezne aplikacije, številu novo uvedenih aplikacij na letni ravni, povprečen čas potreben za dodelitev, odvzem ali spremembo pravice dostopa, povprečno ceno licenc na uporabnika na leto, ter ocenjen odstotek nepotrebnih licenc, ki niso pravočasno ukinjene.

Za pomoč uporabnikom smo uvedli novo kategorijo, ki vsebuje število podpornih zahtevkov za urejanje pravic na uporabnika letno, to je povprečno število klicev ali podpornih zahtevkov za ureditev informacijskih pravic na zaposlenega. Tukaj spadata tudi čas trajanja reševanja zahtevka, v zvezi z urejanjem pravic, s strani informacijskega sistemskega

inženirja v urah, kot tudi čas trajanja čakanja zaposlenega na rešitev zahtevka, torej koliko časa čaka zaposleni na rešitev zahtevka za ureditev pravic.

Zadnja kategorija podatkov pa so podatki povezani z revizijo in kibernetsko varnostjo, ki so vedno pomembnejši, saj se število nepooblaščenih dostopov do podatkov v zadnjih letih znatno povečuje (slika 5.3). Potrebujemo število letnih pregledov informacijskega sistema in povezanih dostopov s strani zunanjih revizijskih hiš. Oceniti moramo čas trajanja priprave podatkov za zunanjega revizorja, torej čas, ki ga zunanji revizor potrebuje za pripravo končnega poročila. Vedeti moramo število letnih pregledov informacijskega sistema in povezanih dostopov, ki jih podjetje izvede interno za zaposlene in zunanje uporabnike. Pregled izvajajo vodje zaposlenih, lastniki aplikacij in podatkov ali interni revizorji. Glede na pretekle izkušnje, moramo ugotoviti čas trajanja, ki ga udeleženi znotraj podjetja potrebujejo za pripravo podatkov, izvedbe pregleda in končnega usklajevanja dostopov z realnim stanjem. Oceniti moramo stroške varnostnega incidenta, povezanega s pravicami uporabnikov, ter število takšnih varnostnih incidentov na letni ravni. Navsezadnje pa potrebujemo tudi odstotek zmanjšanja tveganja za varnostni incident, povezan s pravicami dostopa, po uvedbi sistema za upravljanje identitet in pravic dostopa.[7]



Slika 5.3: Število nepooblaščenih dostopov do podatkov v Združenih državah Amerike v milijonih od leta 2005 do 2019

5.3.Pridobivanje potrebnih podatkov

Vir najbolj relevantnih podatkov je organizacija sama, saj so podatki le tako čisto pravilni, ažurni in realni. Podatkom, katere v organizaciji zbiramo sami, pravimo primarni podatki. Primarni podatki so informacije, pridobljene neposredno iz vira in smo prvi, ki jih uporabljamo. Primarni podatki se lahko precej razlikujejo od sekundarnih, pridobljenih s pomočjo drugih organizacij, saj so sekundarni podatki lahko prečiščeni, urejeni ali pa celo prirejeni. Ker primarni podatki prihajajo direktno iz našega sistema, smo lahko zelo zaupljivi in lahko verjamemo v natančnost in ustreznost podatkov. Prav zaradi tega razloga so primarni podatki temelj naše podatkovne baze.

Primarne podatke delimo na kvantitativne in kvalitativne. Kvantitativni podatki so v obliki števil, količin in vrednosti. Stvari opisuje konkretno in lahko merljivo. Ker so kvantitativni podatki numerični in merljivi, se dobro podajajo analitiki in analizam. Ko analiziramo kvantitativne podatke, lahko odkrijemo vpoglede, s katerimi bolje in lažje razumemo organizacijo in stranke. Ker se tovrstni podatki ukvarjajo s številkami, so zelo objektivni in zanesljivi. Kvalitativni podatki so opisni in ne numerični, kar pomeni da so manj konkretni in težje merljivi kot kvantitativni podatki. Ti podatki pogosto vsebujejo opisne besedne

zveze in mnenja. Kvalitativni podatki pomagajo pri razlagi zakaj so kvantitativni podatki, takšni kot so. Zaradi tega je koristno dopolnjevanje količinskih podatkov, ki so temelji organizacijske podatkovne strategije. Ker so količinski podatki tako temeljni, jih je potrebno zbrati čim več. Med tem ko je strategij za zbiranje podatkov veliko, se pri vseh strategijah uporablja pet osnovnih korakov.

Najprej moramo ugotoviti, katere vse podatke želimo zbirati, torej katere podrobnosti potrebujemo. Odločiti se moramo, katere teme bodo informacije morale zajemati, o kom bomo zbirali podatke in koliko podatkov potrebujemo. Opredeliti je treba cilje, s pomočjo katerih dobimo vprašanja, na katera lahko odgovorimo ali pomagamo odgovoriti s pomočjo podrobnosti podatkov, ki jih bomo zbirali. Ko vemo katere podatke iščemo, moramo določiti časovni okvir v katerem bomo zbirali podatke. Določiti moramo kako dolgo bomo zbirali katere podatke in v kakšnih intervalih. Na tej točki vemo katere podatke zbiramo in v kakšnem časovnem okviru jih zbiramo, ne vemo pa še kako jih bomo zbirali. Določitev načina zbiranja podatkov je jedro strategije zbiranja podatkov. Da izberemo pravi način zbiranja podatkov, moramo upoštevati vrsto informacij, ki jih želimo zbirati, časovni okvir, v katerem jih bomo zbirali, in vse ostale določene vidike ter pravila. Sedaj pa nastopi dejansko zbiranje podatkov. Torej, ko imamo dokončno oblikovan načrt, lahko strategijo zbiranja podatkov izvedemo. Podatke zberemo, potem pa jih organiziramo in uporabimo pri analizah ter s tem pridobimo ugotovitve. Faza analize je ključna, saj pretvori surove podatke v uporabne vpoglede, katere lahko potem uporabimo.[8]

Če primarnih podatkov nimamo dovolj, jih moramo dopolniti s podatki drugih organizacij in raziskav. Takšnim podatkom pravimo sekundarni podatki. Pri pridobivanju sekundarnih podatkov je najbolj pomembno zaupanje v organizacijo, od koder pridobivamo podatke, saj je njihova dolžnost, da so podatki ažurni in niso prirejeni. Mi bomo v tej magistrski nalogi večino sekundarnih podatkov pridobili s pomočjo podjetja Gartner in njihov raziskav.

Gartner je svetovno priznano raziskovalno in svetovalno podjetje, ki ponuja informacije, statistične vpoglede, nasvete in orodja za vodstvo podjetij na več različnih področjih. [9] Da je podjetje Gartner vredno zaupanja, nam pove to, da se med njihovimi strankami nahajajo velike korporacije, vladne agencije, velika tehnološka podjetja in precej investicijskih skupnosti. Delujejo že od leta 1979 in imajo več kot 15 tisoč zaposlenih v več kot sto

pisarnah po celem svetu. V kolikor ustreznega podatka ne najdemo pri podjetju Gartner, ga lahko poiščemo pri ostalih bolj znanih podjetjih s statističnimi raziskava, kot je na primer Statista, kjer lahko najdemo grafe, povprečja, statistike in opise o vseh vrstah različnih tem.[9]

Podatek	Vrednost
Število zaposlenih	**500**
Število zunanjih uporabnikov sistema	**100**
Število vseh aplikacij v IT sistemu	**4**
Ocena stroškov za licence za programsko opremo na leto	**100.000,00 €**
Povprečno število aplikacij na uporabnika	**4**

Slika 5.4: Spremenljivi podatki

Sedaj pa poglejmo kje smo pridobili podatke, katere potrebujemo za izračun v tej magistrski nalogi. Spremenljive podatke dobimo ob vnosu v vnosna polja na začetni strani, pred izračunom, v našem primeru so to podatki srednje velikega podjetja (slika 5.4). Nespremenljive podatke o stroških zaposlenih smo pridobili iz primarnih podatkov v našem podjetju in jih podkrepili s podatki nekaterih podjetij, s katerimi poslujemo. Število delovnih ur na mesec smo izračunali z odštevanjem vikendov in praznikov. Urno postavko smo izračunali na podlagi povprečne mesečen plače in povezanih stroškov in delili s številom mesečnih ur. Naši podatki so vidni spodaj (slika 5.5)

Podatek	Vrednost
Stroški zaposlenih	
Mesečna povprečna plača in povezani stroški IT sistemskega inženirja	5.000,00 €
Mesečna povprečna plača in povezani stroški zaposlenega	4.000,00 €
Število delovnih ur na mesec	174
Urna postavka IT sistemskega inženirja	28,74 €
Urna postavka zaposlenega	22,99 €

Slika 5.5: Podatki o stroških zaposlenih

Podatke o kadrovskih spremembah smo pridobili na podlagi izkušenj z obstoječimi strankami, pri katerih smo uveljavljali sistem upravljanja identitet in pravic dostopa. Podatke smo preračunali v odstotke in povprečili. Te podatke potem preračunamo v številke, glede na vnesene podatke o številu zaposlenih (slika 5.6).

Kadrovske spremembe	
Odstotek novih zaposlitev letno	10,00%
Odstotek internih premestitev letno	20,00%
Odstotek odhodov letno (ocenjeno v %)	5%
Odstotek sprememb zunanjih uporabnikov sistema (ocenjeno v %)	25%
Število novih zaposlitev letno	50
Število internih premestitev letno	100
Število odhodov letno	25
Število sprememb zunanjih uporabnikov	25

Slika 5.6: Podatki o kadrovskih spremembah

Podatke o informacijskih sistemih (slika 5.7) smo pridobili s pomočjo lastnih preteklih meritev in opazovanj. Povprečno število uporabnikov se izračuna glede na vnesene podatke, število novo uvedenih aplikacij smo povprečili glede na ostale stranke, povprečen čas za spremembo pravice pred uvedbo sistema upravljanja identitet in pravic dostopa smo povprečili glede na različne stranke. Povprečno ceno licence na uporabnika smo izračunali s pomočjo vnosa o skupnih stroških licenc in o številu uporabnikov. Odstotek nepotrebnih licenc, pa je prav tako bil ocenjen glede na pretekla opazovanja in povprečen glede na več strank.

Informacijski sistem	
Povprečno število uporabnikov posamezne aplikacije	500
Število novo uvedenih aplikacij letno	1
Povprečen čas, potreben za dodelitev/odvzem/spremembo pravice	0,25
Povprečna cena licence na uporabnika letno	200,00 €
Ocenjen odstotek nepotrebnih licenc	10,00%

Slika 5.7: Podatki o informacijskem sistemu

Za podatke o pomoči uporabnikom, smo uporabili podatke podjetja Gartner, ki prikazujejo kako samopostrežni vmesnik pripomore k hitrejši in lažji pomoči uporabnikom. Podatki so usmerjeni na srednje veliko podjetje in povprečeni (slika 5.8).

Pomoč uporabnikom	
Število podpornih zahtevkov za urejanje pravic na uporabnika letno	8
Čas trajanja reševanja zahtevka s strani IT sistemskega inženirja (v urah)	0,5
Čas trajanja za zaposlenega (čakanja) na rešitev zahtevka (v urah)	0,75

Slika 5.8: Podatki o pomoči uporabnikom

Nazadnje pa imamo še podatke o reviziji in kibernetski varnosti (slika 5.9). Za število letnih pregledov (internih in zunanjih), smo uporabili globalne smernice in priporočila. Za čas trajanja priprave na pregled, smo uporabili lastne izkušnje glede na srednje veliko podjetje in z ustreznimi orodji. Za oceno stroška varnostnega incidenta smo uporabili podatke, glede na srednje veliko podjetje, s strani podjetja Gartner. Letno število varnostnih incidentov smo ocenili z povprečenjem lastnih izkušenj s strankami v preteklih letih. Prav tako smo, z povprečenjem lastnih izkušenj v preteklih letih, ocenili zmanjšanje tveganja z uvedbo sistema za upravljanje identitet in pravic dostopa.

Revizija in kibernetska varnost	
Število letnih pregledov s strani zunanjih revizorjev	2
Čas trajanja priprave podatkov za zunanjega revizorja (v urah)	40
Število internih letnih pregledov IT dostopov s strani vodij, lastnikov podatkov/aplikacij (število)	2
Čas trajanja za pripravo na interni pregled, izvedbe in odprave napak (v urah)	40
Ocena stroška varnostnega incidenta, povezanega s pravicami uporabnikov	7.000,00 €
Število IT varnostnih incidentov letno	10
Zmanjšanje tveganja za varnostni incident po uvedbi IAM sistema	50%

Slika 5.9: Podatki o reviziji in kibernetski varnosti

6. IZRAČUN STROŠKOV

Investicijo smo računali za dobo petih let, ker smo iz lastnih izkušenj ugotovili, da je to povprečna čakalna doba povratka investicije oziroma donosnosti investicije znotraj katere je stranka pripravljena investirati. Če je doba donosnosti investicije večja od pet let, se stranka zlahka ustraši in izgubi voljo za takšno investicijo, ter se raje poda v optimizacijo drugega dela arhitekture, sistema ali procesov. V največ primerih se za takšno optimizacijo odločajo stranke, katerim se investicija povrne v roku treh let. Pri vnosnih podatkih smo uporabili povprečje podatkov, glede na pretekle izkušnje, ki se nam je zdelo realno in optimalno. Tako smo za število uporabnikov uporabili vrednost 500, za število zunanjih uporabnikov sistema vrednost 100, število informacijskih sistemov smo določili na 4, letni strošek licence smo postavili na 100.000,00€, število aplikacij na uporabnika pa smo prav tako postavili na 4.

6.1. Brez upravljanja uporabniških pravic in identitet

Najprej smo za vsak del investicije izračunali letne stroške. V našem primeru je strošek ureditve pravic za novo zaposlene pred uvedbo sistema za upravljanje uporabniških pravic, znašal 2.586,21€. Znesek smo dobili z množenjem povprečnega časa potrebnega za dodelitev pravice s številom zaposlenih, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili s seštevkom urnih postavk obeh vrst zaposlenih, kot vidimo v (6.1). Strošek ureditve pravic ob premestitvah je znašal 5.172,41€. Znesek smo dobili z množenjem povprečnega časa potrebnega za spremembo pravice s številom premestitev letno, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili s seštevkom urnih postavk obeh vrst zaposlenih, kot vidimo v (6.2). Strošek za ukinitev pravic ob prenehanju delovnega razmerja je znašal 718,39€. Znesek smo dobili z množenjem povprečnega časa potrebnega za spremembo pravice z številom prenehanj delovnih razmerij letno, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili z urno postavko informacijskega inženirja.

$$z = dpp \cdot stz \cdot aup \cdot (upit + up) \tag{6.1}$$

Tu je:

z – znesek

dpp – povprečni čas potreben za dodelitev pravic (h)

stz – število zaposlenih

aup – povprečno število aplikacij na uporabnika

upit – urna postavka zaposlenega v informacijskem sektorju

up – urna postavka drugih zaposlenih

$$z = spp \cdot stz \cdot aup \cdot (upit + up) \tag{6.2}$$

Tu je:

z – znesek

spp – povprečni čas potreben za spremembo pravic (h)

stz – število zaposlenih

aup – povprečno število aplikacij na uporabnika

upit – urna postavka zaposlenega v informacijskem sektorju

up – urna postavka drugih zaposlenih

Eden izmed večjih stroškov je zaradi trajanja reševanja podpornih zahtevkov. Da smo dobili strošek trajanja reševanja podpornega zahtevka s strani informacijsko sistemskega inženirja, smo množili njegovo povprečno urno postavko s številom zaposlenih in povprečnim številom podpornih zahtevkov na uporabnika letno, ter vse skupaj še z časom trajanja reševanja posameznega zahtevka, kot vidimo v (6.3), ter tako dobili vrednost 57.471,26€. Še večji strošek pa je izguba časa, med tem ko zaposleni čaka na rešitev zahtevka oziroma odgovor informacijsko sistemskega inženirja, saj ta čas v povprečju traja tri četrt ure, med tem ko čas reševanja traja pol ure. Da smo dobili željeni podatek, smo množili povprečno urno postavko zaposlenega s številom zaposlenih in povprečnim številom podpornih zahtevkov na uporabnika letno, ter vse skupaj še z časom trajanja čakanja na odgovor oziroma rešitev posameznega zahtevka, kot vidimo v (6.4), ter tako dobili vrednost 68.965,52€.

$$s = up \cdot sz \cdot spz \cdot cr \tag{6.3}$$

Tu je:

s – strošek trajanja reševanja podpornega zahtevka s strani informacijsko sistemskega inženirja

up – povprečna urna postavka

sz – število zaposlenih

spz – število podpornih zahtevkov na uporabnika

cr – čas reševanja zahtevka (h)

$$s = up \cdot sz \cdot spz \cdot cc \tag{6.4}$$

Tu je:

s – strošek trajanja reševanja podpornega zahtevka s strani informacijsko sistemskega inženirja

up – povprečna urna postavka

sz – število zaposlenih

spz – število podpornih zahtevkov na uporabnika

cc – čas čakanja na odgovor(h)

Za pripravo podatkov za zunanjega revizorja je ocenjen porabljen čas štirideset ur. Če to število pomnožimo z urno postavko informacijsko sistemskega inženirja in številom letnih pregledov, dobimo 2.298,85€. Skoraj dvakrat tolikšen pa je strošek pri porabljenem času za interne revizijske preglede, saj za to porabimo čas tako informacijsko sistemskega inženirja, kot tudi drugega zaposlenega, saj morata biti v pripravo vključeni obe osebi. Kar pomeni da, ko pomnožimo število ur potrebnih za pregled, izvedbo in odpravo napak z številom pregledov ter seštevkom obeh urnih postavk, dobimo 4.137,93€. Največji strošek pri kategoriji kibernetske varnosti je z veliko razliko, ocena stroška varnostnega incidenta, povezanega s pravicami uporabnikov. Namreč, če pomnožimo ocenjen povprečen strošek varnostnega incidenta s ocenjenim letnim številom incidentov, dobimo kar 70.000,00€.

Največji letni strošek pri našem izračunu pa je ocena stroškov za licence za programsko opremo. To oceno nam uporabnik vnese v vnosno polje, preden zažene izračun in v našem primeru znaša 100.000,00€. Skupni stroški so tako 311.350,57€ (slika 6.1).

Leto	Strošek brez IDM
1	311.350,57 €
2	622.701,15 €
3	934.051,72 €
4	1.245.402,30 €
5	1.556.752,87 €

Slika 6.1: Letni stroški brez upravljanja identitet in pravic dostopa

6.2. S upravljanjem uporabniških pravic in identitet

Strošek ureditve pravic za novo zaposlene je po uvedbi sistema za upravljanje uporabniških pravic, znašal 1.034,48€. Znesek smo dobili z množenjem povprečnega časa potrebnega za dodelitev pravice po uvedbi sistema s številom zaposlenih po uvedbi sistema, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili s seštevkom urnih postavk obeh vrst zaposlenih. Strošek ureditve pravic ob premestitvah je znašal 2.068,97€. Znesek smo dobili z množenjem povprečnega časa potrebnega za spremembo pravice po uvedbi sistema s številom premestitev letno, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili s seštevkom urnih postavk obeh vrst zaposlenih. Strošek za ukinitev pravic ob prenehanju delovnega razmerja po uvedbi sistema je znašal 287,36€. Znesek smo dobili z množenjem povprečnega časa potrebnega za spremembo pravice po uvedbi, z številom prenehanj delovnih razmerij letno, kar smo množili z povprečnim številom aplikacij na uporabnika, ter vse skupaj množili z urno postavko informacijskega inženirja.

Strošek zaradi trajanja reševanja podpornih zahtevkov je po uvedbi sistema precej manjši in znaša 7.183,91€. Da smo dobili strošek trajanja reševanja podpornega zahtevka s strani informacijsko sistemskega inženirja po uvedbi sistema, smo množili njegovo povprečno urno postavko s številom zaposlenih in povprečnim številom podpornih zahtevkov na uporabnika letno, ter vse skupaj še z časom trajanja reševanja posameznega zahtevka po uvedbi sistema. Prav tako je strošek za izgubo časa, med tem ko zaposleni čaka na rešitev

zahtevka oziroma odgovor informacijsko sistemskega inženirja, precej manjši. Strošek smo dobili z množenjem povprečne urne postavke zaposlenega s številom zaposlenih in povprečnim številom podpornih zahtevkov na uporabnika letno, ter vse skupaj še z časom trajanja čakanja na odgovor oziroma rešitev posameznega zahtevka po uvedbi sistema, in znaša 11.494,25€.

Za pripravo podatkov za zunanjega revizorja, po uvedbi sistema, porabimo le šestnajst ur, kar je precej manj kot štirideset ur, potrebnih pred uvedbo. Če to število pomnožimo z urno postavko informacijsko sistemskega inženirja in številom letnih pregledov, dobimo 919,54€, torej manj kot polovico zneska pred uvedbo. Strošek pri porabljenem času za interne revizijske preglede, pa je pred uvedbo sistema bil precej večji od stroška za zunanjega revizorja, po uvedbi, pa je ta strošek še manjši od stroška za zunanjega revizorja po uvedbi, in znaša le 827,59€. Za interni pregled po uvedbi potrebujemo le osem ur, namesto štiridesetih pred uvedbo sistema. Podatek dobimo, če enako kot prej, pomnožimo število ur potrebnih za pregled, izvedbo in odpravo napak z številom pregledov ter seštevkom obeh urnih postavk, in dobimo 827,59€. Ocena stroška varnostnega incidenta, povezanega s pravicami uporabnikov se je po uvedbi sistema prepolovila in sedaj znaša 35.000,00€.

Letni strošek za licence za programsko opremo pa lahko s pomočjo partnerstva zmanjšamo za deset odstotkov, torej na 90.000,00€. Skupni stroški po uvedbi sistema so le 148.816,09€ (slika 6.2).

Leto	Strošek z IDM2
1	427.850,57 €
2	652.041,67 €
3	876.232,76 €
4	1.100.423,85 €
5	1.324.614,94 €

Slika 6.2: Letni stroški z upravljanjem identitet in pravic dostopa

6.3. Izračun investicije

Investicija pomeni implementacija in vzdrževanje dejanskega sistema za upravljanje identitet in pravic dostopa. Glede na pridobljene podatke, lahko grobo ocenimo količino dela, potrebnega za implementacijo, ter stroške vzdrževanja (slika 6.3).

Leto	Skupna vrednost investicije	Skupna vrednost prihranka
1	116.500,00 €	0,00 €
2	191.875,00 €	162.534,48 €
3	267.250,00 €	325.068,97 €
4	342.625,00 €	487.603,45 €
5	418.000,00 €	650.137,93 €

Slika 6.3: Skupna letna vrednost investicije v sistem upravljanja identitet in pravic dostopa

Za pripravo takšnega podjetja bi porabili 60 dni, kar pri povprečnem strošku 250,00€ na dan, znaša 15.000,00€. To je strošek podjetja za pripravo in sodelovanje v sklopu takšnega projekta. Dnevni strošek se izračuna na podlagi povprečne mesečne plače informacijsko sistemskega inženirja, deljeno s povprečno 20 dnevi mesečno. Izvedbo analize in načrtovanje smo ocenili na 10 dni, vendar pa je tukaj strošek na dan 700,00€ in znaša skupaj 7.000,00€, saj je to strošek zunanjega izvajalca priprave in načrtov. Kar 31.500,00€ bi znašal strošek nakupa licenc za sistem upravljanja identitet in pravic dostopa, ker v tem primeru potrebujemo petsto licenc. Za dejansko implementacijo oziroma uvedbe sistema, smo ocenili 30 dni, kar skupaj znaša 21.000,00€, vključuje pa namestitev in konfiguracijo sistema, uvoz podatkov, namestitev spletnega portala in izobraževanje uporabnikov. Poleg osnovnega sistema, je potrebno integrirati tudi uporabniške aplikacije. Za vsako aplikacijo je ocenjen strošek 10.500,00€ in ker imamo v našem primeru štiri aplikacije, se strošek zmnoži na 42.000,00€. Skupna implementacija torej stane 116.500,00€.

Povprečno vzdrževanje sistema na letni ravni, je v sledečih letih cenejše, od začetne implementacije. Vzdrževanje zajema licence, popravke, nadgradnje, nove funkcionalnosti, analize, načrtovanja, dodaten razvoj in vključevanje novih uporabniških ciljnih sistemov. Za vsako sledeče leto smo tako izračunali povprečen strošek 75.375,00€ (slika 6.4).

Investicija 1. leto			
Priprava projekta - interno (dni)	60	250,00 €	15.000,00 €
Izvedba analize in načrta - blueprint (dni)	10	700,00 €	7.000,00 €
Nakup licenc za IAM programsko opremo (št. Licenc)	500	63,00 €	31.500,00 €
Uvedba IAM rešitve v podjetje - storitve izvajalca (dni)	30	700,00 €	21.000,00 €
Vključevanje upravljanih ciljnih sistemov - storitve izvajalca (število sistemov)	4	10.500,00 €	42.000,00 €
		SKUPAJ:	**116.500,00 €**
Investicija 2. leto			
Vzdrževanje IAM programske rešitve (popravki, licence)			7.875,00 €
Vzdrževanje in nadgradnja IAM rešitve, nove funkcionalnosti (št. Dni/mesec)	5	3.500,00 €	42.000,00 €
Sodelovanje pri analizi, načrtovanju, razvoju IAM sistema - interno (dni/mesec)	5	250,00 €	15.000,00 €
Vključevanje novih upravljanih ciljnih sistemov (število sistemov)	1	10.500,00 €	10.500,00 €
		SKUPAJ:	**75.375,00 €**

Slika 6.4: Izračun investicije za implementacijo in vzdrževanje sistema

6.4. Primerjava in izračun vračila naložbe

Kot lahko vidimo, smo pri vseh izračunih z uvedbo sistema za upravljanje identitet in pravic dostopa, stroške zmanjšali. Skupni letni strošek smo zmanjšali za kar 52 odstotkov. Strošek ureditve pravic za novo zaposlene, ob premestitvah in ob prenehanju delavnega razmerja je po uvedbi sistema manjši za 60 odstotkov. Strošek reševanja zahtevka s strani informacijsko sistemskega inženirja je po uvedbi manjši za kar 88 odstotkov, med tem ko je strošek zaposlenega pri čakanju na rešitev zahtevka manjši za 83 odstotkov.

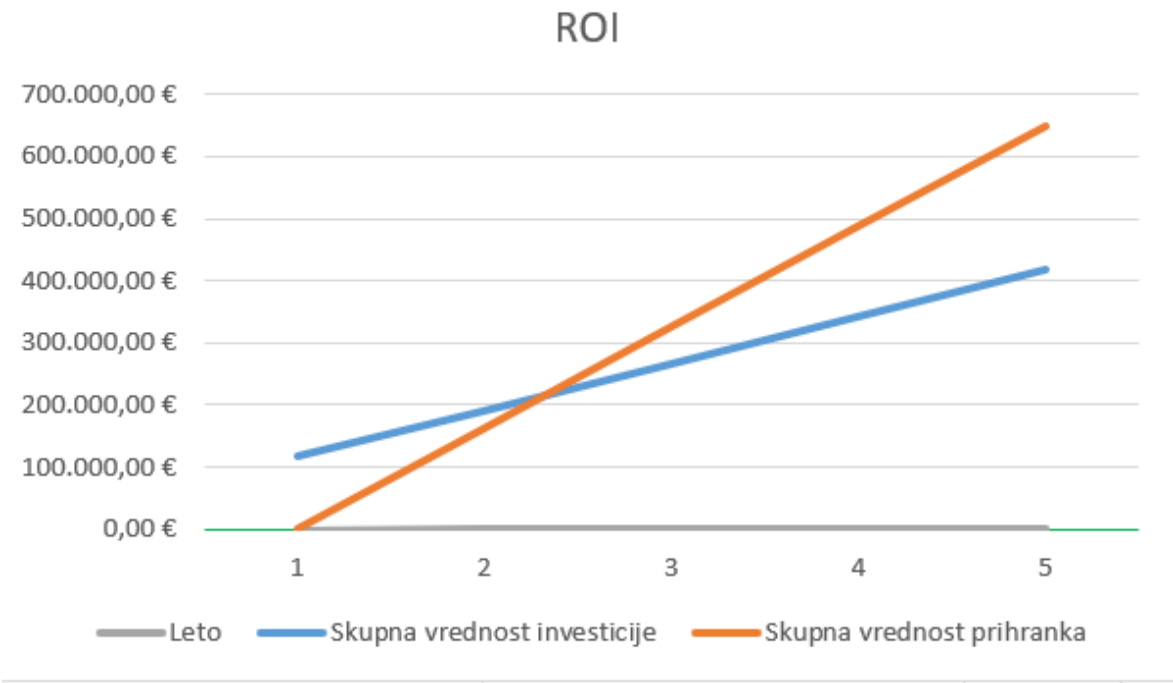
Strošek pripravi podatkov za zunanjega revizorja je po uvedbi manjši za 60 odstotkov. Strošek internega varnostnega pregleda se je med tem zmanjšal za 80 odstotkov. Prav tako se je razpolovilo ocenjeno število varnostnih incidentov, kjer so zaradi tega stroški za 50 odstotkov manjši. Licence po uvedbi sistema znašajo 10 odstotkov manj, kot pred uvedbo.

Poleg manjših stroškov, se je po uvedbi sistema za upravljanje identitet in pravic dostopa, zmanjšalo tudi trajanje več procesov (slika 6.5). Tako se je potrebni čas za ureditev sprememb pravic, skrajšal za 60 odstotkov. Prav tako za 60 odstotkov, se je skrajšal čas potreben za pripravo poročil za revizorje. Za kar 75 odstotkov se je zmanjšalo ocenjeno število podpornih zahtevkov za urejanje pravic. Za 50 odstotkov se je skrajšal čas trajanja zahtevka s strani informacijskega oddelka organizacije. Prav tako pa se po uvedbi, tveganje za informacijski varnostni incident zmanjša za kar 50 odstotkov.

Prihranki	% prihranka
Strošek ureditve pravic za nove zaposlitve ali ob premestitvah	60,00%
Zmanjšanje potrebnega časa, potrebnega za ureditev sprememb pravic	60,00%
Zmanjšanje podpornih zahtevkov za urejanje pravic	75,00%
Zmanjšanje časa trajanja reševanje zahtevka s strani IT	50,00%
Zmanjšanje tveganja za IT varnostni incident	50,00%
Zmanjšanje časa trajanja priprave poročil za revizorje	60,00%

Slika 6.5: Pomembnejši prihranki

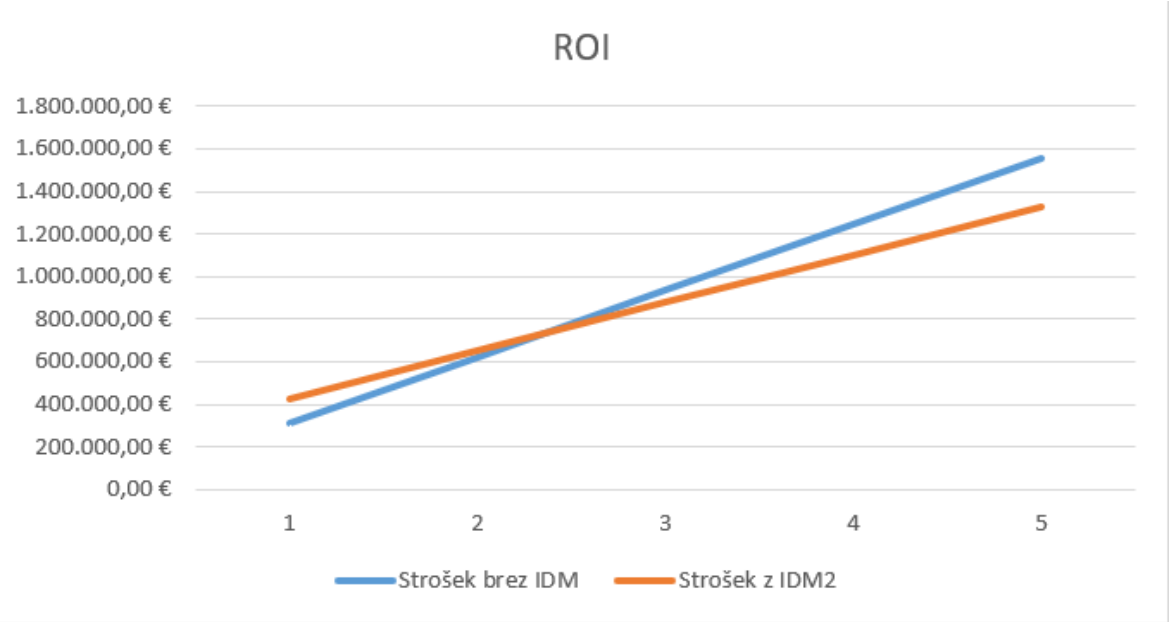
Ker moramo, da dobimo realen znesek letne porabe, znesku po uvedbi prišteti še dejansko naložbo, ki v našem primeru znaša 116.500,00€ v prvem letu in 75.375,00€ vsako naslednje leto. S temi podatki lahko izračunamo, da se bo investicija obrestovala v dveh letih in pol. Na prikazanem grafikonu lahko vidimo kako hitro raste vrednost skupnega prihranka z uporabo sistema za upravljanje identitet in pravic dostopa (slika 6.6).



Slika 6.6: Razlika v investiciji

Te podatke pa lahko predstavimo tudi na drugačen način. Namesto z uporabo skupne vrednosti investicije in skupne vrednosti prihranka, lahko podatke prikažemo kot skupni strošek brez sistema za upravljanje identitet in pravic dostopa in z uvedbo takšnega sistema. V sledečem grafikonu lahko vidimo prikaz, kako je z uporabo sistema za upravljanje identitet in pravic dostopa daljica, ki prikazuje skupni strošek v časovnem obdobju petih let

bolj položna od tiste, ki prikazuje skupni strošek brez vpeljave sistema in kje se daljici sekajo, tam se namreč prične donosnost investicije(slika 6.7).

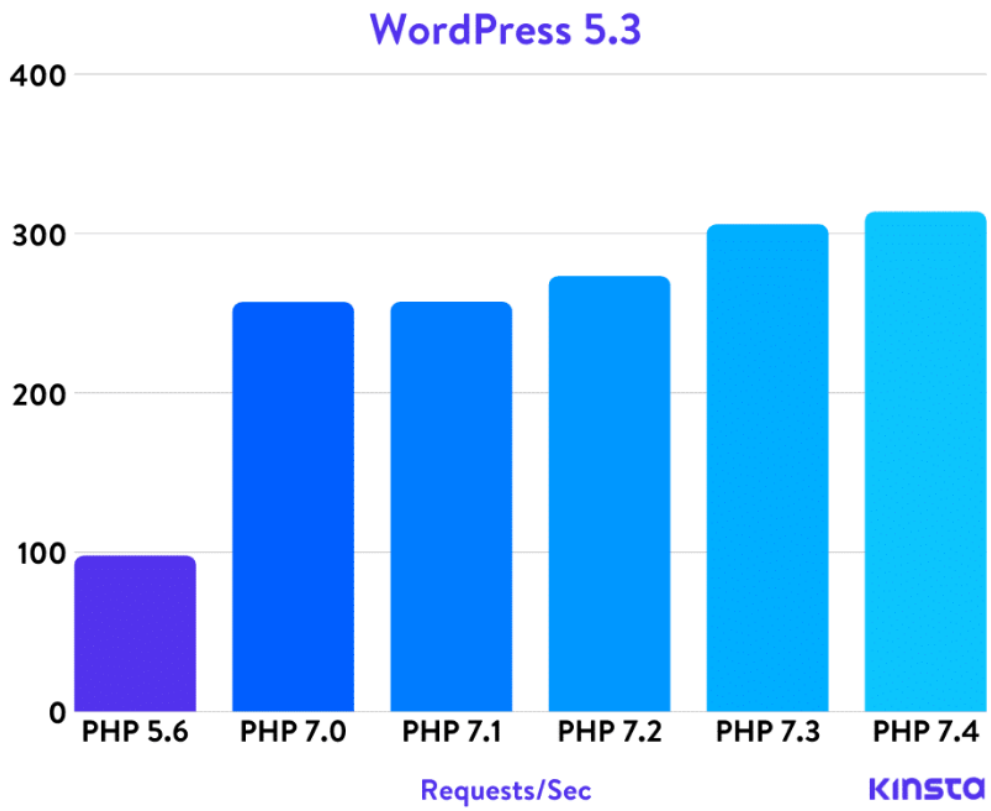


Slika 6.7: Razlika v stroških z in brez uporabe sistema za upravljanje identitet in pravic dostopa

7. IMPLEMENTACIJA SPLETNE APLIKACIJE ZA IZRAČUN VRAČILA

7.1. Izbira okolja in orodij

Po zaključku načrtovanja, izračunov in analize, smo se morali določiti v katerem okolju in s katerim programskim jezikom naj implementiramo spletno aplikacijo za izračun. Po premisleku in primerjavi različnih okolij, smo se odločili za programski jezik PHP in ogrodje PhpStorm. Za PHP smo se odločili predvsem zaradi tega, da bi bilo na strani uporabnika narejenega čim manj dela. Ker je PHP strežniški jezik, se odjemalcu oziroma uporabniku pošlje samo že generirana spletna stran in se na uporabniški strani ne dogajajo nobeni izračuni ali dodatne funkcionalnosti. Ker vemo, da se ne bo izračunavalo veliko izračunov v istem trenutku, nimamo težav z zmogljivostjo strežnika, pa čeprav del strežnika na katerem je ta aplikacija nima dodeljenih veliko virov. Z zmogljivostjo še posebej ni težav po posodobitvi oziroma nadgradnji različice PHP, saj je različica 7.4 približno dvakrat hitrejša od različice 5.6, kar lahko lepo vidimo na spodnji sliki (slika 7.1), kjer je prikazana primerjava zmožnosti istega strežnika, pri poganjanju platforme WordPress različice 5.3. [10]



Slika 7.1: Primerjava zmogljivosti istega strežnika pri poganjanju WordPress 5.3

Programski jezik PHP prav tako nima težav z izvajanjem na različnih operacijskih sistemih in napravah. Jezik prav tako že v osnovi podpira povezavo do podatkovnih baz in nam s tem prihrani precej razvojnega časa. Če potrebujemo kaj takšnega, da jezik ne podpira v osnovi, pa lahko brez težav dodamo tretje osebne module in knjižnice, katere moramo za uporabo samo vključiti in jih že lahko uporabljamo. Tretje osebne knjižnice se največkrat uporabljajo za poenostavitev in pohitritev programiranja. V našem primeru smo uporabili samo eno knjižnico, in sicer Phpmailer, katera nam omogoča enostavno pošiljanje e-poštnih sporočil z naprednimi nastavitvami. Programski jezik PHP je odprto koden in obstaja že več kot 24 let, tako da o stabilnosti in zaupanju ni več vprašanj. Prav tako je eden izmed bolj uporabljenih in prepoznavnih programskih jezikov na svetu, kar pomeni da je veliko težav, na katere lahko potencialno naletimo, že rešenih in veliko odgovorov na vprašanja, ki jih imamo, že odgovorjenih. Uporablja sintakso podobno programskemu jeziku C in se ga je dokaj enostavno privaditi.

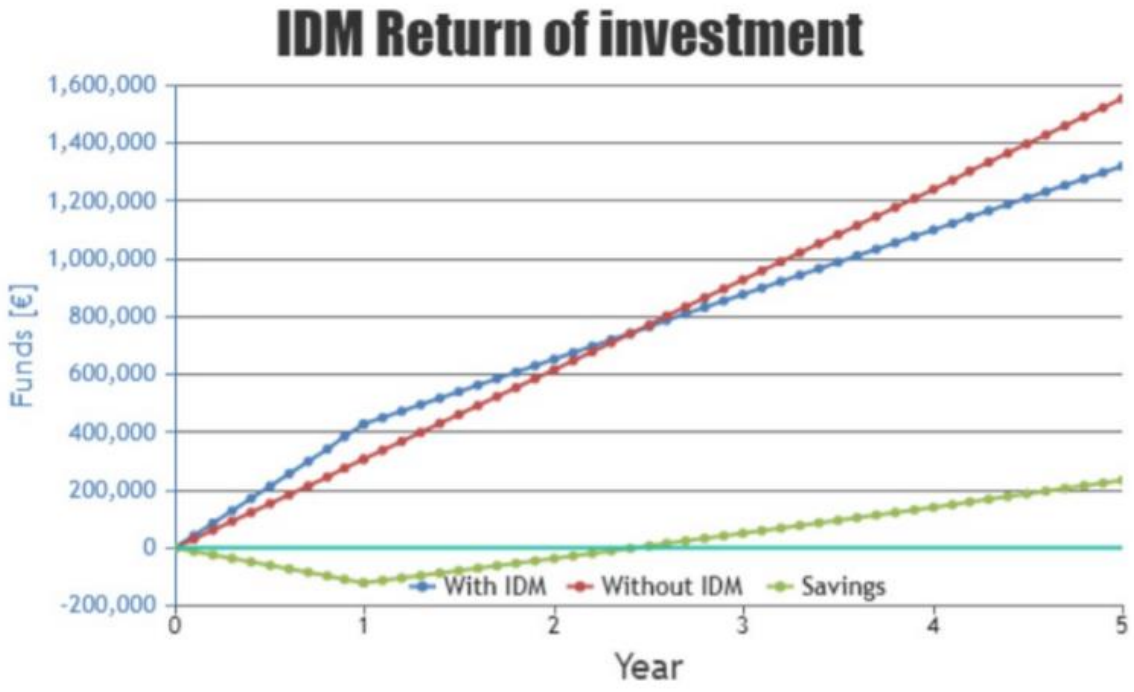
Za razvojno okolje smo si izbrali PhpStorm. Le ta je integrirano razvojno okolje za programski jezik PHP, izdelano s strani češkega podjetja JetBrains in je na voljo na različnih operacijskih sistemih. [17] Vgrajeno ima urejevalnik jezikov PHP, HTML in JavaScript s sprotnim analiziranjem kode, preprečevanjem napak in samodejnim obnovitvami kode. Samodejno dokončanje kode podpira zadnjo različico (7.4) pa vse do različice 5.3, kar nam omogoča tudi urejanje zapuščenih in starejših projektov. Za vse podprte različice vsebuje tudi generatorje, sorodne postopke, določene ključne besede, sezname znotraj zank, imenske prostore, sintakso kratkega niza in še mnoge druge bližnjice. Orodje prav tako vključuje popoln SQL urejevalnik z možnostjo urejanja rezultatov poizvedb. Orodje je napisano v jeziku Java in podpira razne vtičnike, ustvarjene posebej za PhpStorm, katere lahko ob obsežni dokumentaciji, napišejo tudi uporabniki sami.

7.2. Dejanska implementacija

Najprej smo pripravili vnosno masko (slika 7.3), za katero se uporablja preprost in osnoven HTML in CSS, s katero prejmemo na strežnik vnosne podatke uporabnika in zahtevo za izračun. Ob prejetju vnosnih podatkov, smo uporabniku vrnili potrditveno stran, na kateri smo potrdili prejem podatkov in napisali, da bo v kratkem na e-poštni naslov pridobil izračun. Vse pridobljene podatke smo shranili v bazo in pridobili implementirali spremenljivke z spremenljivimi in nespremenljivimi podatki, katere potrebujemo za

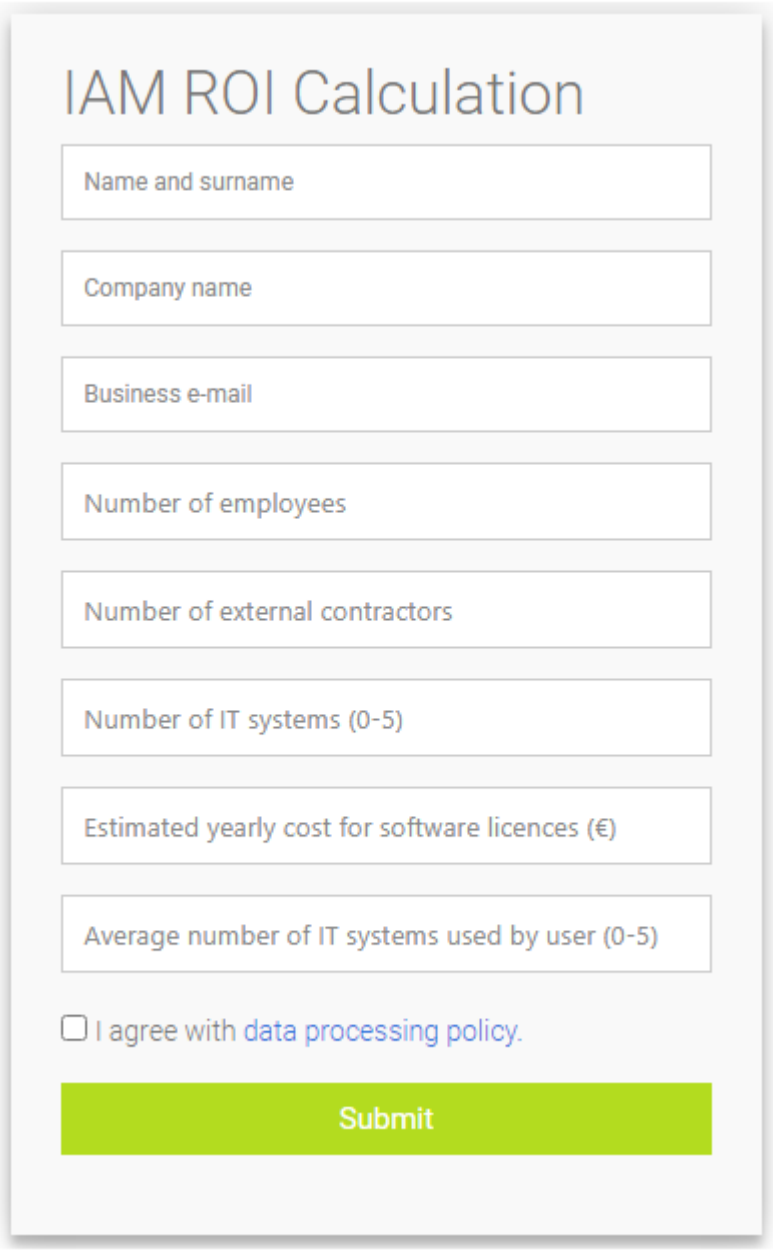
izračun. Pri implementaciji izračuna smo si pomagali z izračunom, ki smo ga med analizo in načrtovanjem pripravili z orodjem Microsoft Office Excel. Sam izračun je velik skoraj 300 vrstic kode, v katerih je vsaka izračunana vsaka potrebna spremenljivka, kot tudi pomožni podatki za hitrejše izračune. Najprej smo v spremenljivke shranili vse vhodne podatke in podatke, ki smo jih poznali (statistične in povprečne), nato smo najprej opravili pomožne izračune, kot je na primer dejansko število letnih novih zaposlitev. S tem nam ni bilo v vsakem izračunu množiti število zaposlenih z odstotkom novih zaposlitev, ampak smo samo uporabili že prej izračunano dejansko število novo zaposlenih. Takšne izračune smo opravili za število novo zaposlenih, premestitev, odhodov, sprememb zunanjih uporabnikov, povprečno število uporabnikov posamezne aplikacije, ceno letnih licenc na uporabnika, in še nekatere druge. Za tem smo opravili izračune stroškov in zneskov, kot opisano v poglavju 6, s tem da smo vse stroške in zneske delili še na par podkategorij, katere uporabljamo za interno rabo in v našem konkretnem izračunu niso pomembni. Ko smo imeli vse zneske, smo jih morali še sešteti in opraviti primerjavo z in brez sistema za upravljanje identitet in pravic dostopa.

Izračun smo poskusili čim bolj optimizirati in pohitriti, za lepši pregled pa veliko uporabljamo sezname in imenike. Ko smo imeli vse izračune pripravljene, smo z programskih jezikom JavaScript, poleg osnovne postavitve HTML, naredili graf v katerega smo napolnili izračunane podatke in prikazali stroške pred in po vpeljavi sistema za upravljanje identitet in pravic dostopa, ter prihranke (slika 7.2).



Slika 7.2: Graf z izračunanimi podatki

Na vrhu dokumenta se nahajajo podatki podjetja in kontakt, sledil je graf prikazan na zgodnji sliki (7.2). Za grafom smo napisali par besed o donosnosti upravljanja identitet in pravic dostopa, na kar so sledili vneseni podatki in razpredelnica, ki prikazuje razdelitev posameznih stroškov. Na dnu dokumenta pa je bila razpredelnica, v kateri smo videli opravila pri katerih smo prihranili največ. Vse skupaj je bilo generirano kot datoteka PDF in s pomočjo knjižnice Phpmailer, poslano uporabniku v e-poštnem sporočilu. Celotna aplikacija podpira dva jezika, in sicer slovenščino in angleščino. Jezik uporabnika je pred izbran glede na lokacijo naslova IP, s katerim je uporabnik prišel do vnosne maske, lahko pa se na začetni strani spremeni. Za najhitrejše delovanje smo pripravili dve datoteki, vsako v svojem jeziku, tako da se je izvajala samo ena datoteka, glede na izbrani jezik, zaradi česar smo uporabili samo en pogojni stavek in uporabili funkcijo odvisno od jezika, namesto preverjanja jezika pri vsaki pojavitvi potrebe po prevajanju.



Slika 7.3: Vnosna maska spletne aplikacije

8. SKLEP

V tem magistrskem delu smo pogledali kako opraviti analizo donosnosti naložbe v sistem upravljanja identitet in pravic dostopa. Torej, kako izračunati donosnost, na kaj moramo biti pri izračunu pazljivi, kakšne podatke potrebujemo in kje takšne pridobiti čim bolj relevantne podatke. Pri pregledu ali se takšna naložba splača in v kolikšnem času postane donosna, smo po precej poskusih opazili, da je največji atribut pri določanju donosnosti število zaposlenih in da je meja pri približno 80 uporabnikih sistema. Običajno se je donosnost večala z številom uporabnikov sistema, je pa to seveda odvisno od posamezne organizacije. Spoznali smo osnove upravljanja identitet in pravic dostopa, prednosti in slabosti, dobre prakse ter predlagan produkt. Opravili smo izračun s testnimi podatki in pregledali stroške ter potrebno investicijo in čas donosnosti naložbe. Na koncu smo pa opravili tudi kratek pregled dejanske implementacije aplikacije za izračun.

Težav pri izračunu in implementaciji nismo imeli, so pa bile potrebne kakšne prilagoditve pri izračunih in pridobivanju podatkov, pa čeprav je bilo to pričakovano, nam je povzročilo nekaj preglavic in dodatnega dela. Po ugotovitvi katere vse podatke potrebujemo za uspešen izračun, smo tudi dopolnili podatke, ki jih spremljamo pri strankah, tako da so lahko izračuni v bodoče še lažji, bolj relevantni in natančnejši.

9. VIRI

[1] Martin, A. J., Waters, J. K., What is IAM? Identity and access management explained, Dostopno na: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html [12. 07. 2020]

[2] F5, The Challenges and Benefits of Identity and Access Management, Dostopno na: https://www.f5.com/services/resources/white-papers/the-challenges-and-benefits-of-identity-and-access-management [14. 07. 2020]

[3] Cortes, M., SINGLE SIGN-ON (SSO): PROS & CONS, Dostopno na: https://www.cynexlink.com/2020/06/03/single-sign-on-pros-and-cons/ [19. 07. 2020]

[4] Aradhya, D., Identity Management (in the cloud): IDaaS, Dostopno na: http://www.divyaaradhya.com/2017/09/19/identity-management-in-the-cloud-idaas/ [24. 07. 2020]

[5] One Identity, Resources, Dostopno na: https://www.oneidentity.com/products/identity-manager/ [23. 07. 2020]

[6] DemandZen, 7 Reasons Why Relevant Data Is Important To Your Organization, Dostopno na: https://demandzen.com/7-reasons-why-relevant-data-important-your-organization/ [24. 07. 2020]

[7] Grow, WHY IS DATA IMPORTANT FOR YOUR BUSINESS?, Dostopno na: https://www.grow.com/blog/data-important-business [27. 07. 2020]

[8] Lotame, P., What Are the Methods of Data Collection?, Dostopno na: https://www.lotame.com/what-are-the-methods-of-data-collection/ [29. 07. 2020]

[9] Wikipedia, Gartner, Dostopno na: https://en.wikipedia.org/wiki/Gartner [02. 08. 2020]

[10] Jackson, B., The Definitive PHP 5.6, 7.0, 7.1, 7.2, 7.3, and 7.4 Benchmarks (2020), Dostopno na: https://kinsta.com/blog/php-benchmarks/ [05. 08. 2020]

[11] Zimšek A., Izkušnje pri uvajanju sistema uporabniških identitet. V: Javornik B., Jagodic M. (ur.), 23. mednarodna konferenca o revidiranju in kontroli informacijskih sistemov, Zreče, 22-23. september 2015, /: Slovenski odsek ISACA, 2015, str. 45-52.

[12] Zimšek A. Upravljanje identitet. Spletna revija SIR*IUS, (2013),

[13] Statista. Analize in primerjave. Dostopno na: https://www.statista.com/ [25. 07. 2020]

[14] Jamnikar E., Zimšek A. Vpliv upravljanja uporabniških pooblastil na varnost podatkov. V: Heričko M., Kous K. (ur.), OTS 2017 SODOBNE INFORMACIJSKE TEHNOLOGIJE IN STORITVE (ZBORNIK DVAINDVAJSETE KONFERENCE), Maribor, 13. junij 2017, Maribor: Univerzitetna založba Univerze v Mariboru, 2017, str. 2-9.

Dostopno na: http://press.um.si/index.php/ump/catalog/book/229 [08. 07. 2020]

[15] Nagarajan, S., Eurozone gdp sinks in first quater coronavirus 2020, Dostopno na: https://www.businessinsider.com/eurozone-gdp-shrinks-in-first-quarter-coronavirus-2020-4 [25.08.2020]

[16] Gartner. Magic Quadrant for Identity Governance and Administration. Stamford: Gartner Inc., 2018

[17] JetBrains. Produkt PhpStorm. Dostopno na: https://www.jetbrains.com/phpstorm/ [25.08.2020]

[18] Misra, S. C., Mondal, A. Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment, Mathematical and Computer Modelling, 2011, 53(3-4), str. 504–521.

[19] Chonka, A., Xiang, Y., Zhou, W., Bonti, A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks, Journal of Network and Computer Applications, 2011, 34(4), str. 1097–1107.

[20] Kumar, V., Bhardwaj, A. Identity Management Systems. International Journal of Strategic Decision Sciences, 2018, 9(1), str. 63–78.