Tampereen yliopisto

Emma Ikonen

KÄYTTÄJÄHALLINTAPROSESSIN SUUNNITTELU TEHOKKAAN KÄYTTÄ-JÄHALLINNAN TOTEUTTAMISEKSI

Diplomityö
Johtamisen ja talouden tiedekunta
Syyskuu 2022

TIIVISTELMÄ

Emma Ikonen: Käyttäjähallintaprosessin suunnittelu tehokkaan käyttäjähallinnan toteuttamiseksi
Diplomityö
Tampereen yliopisto
Tietojohtaminen
Syyskuu 2022
Tarkastajat: Yliopistonlehtori Ilona Ilvonen ja Yliopistonlehtori Pasi Hellsten

Käyttäjähallinta vaikuttaa yritysten tietoturvallisuuteen. Kyberrikollisuuden lisäännyttyä tietomurrot voivat koitua erittäin kalliiksi organisaatiolle ja vahingoittaa organisaation imagoa. Käyttäjien pääsyn seuraaminen identiteetin- ja pääsynhallinnan avulla on olennainen vaihe turvallisen tietoturvasuunnitelman kehittämisessä. Identiteetin ja pääsynhallinta on prosessi, jolla varmistetaan, että asianmukaisilla henkilöillä on pääsy asianmukaisiin resursseihin organisaation sisällä. Organisaatiot muuttuvat ja kasvavat. Tästä seuraakin, että käyttäjähallintaympäristöjä voidaan joutua suunnittelemaan uudelleen organisaatiomuutosten takia.

Tutkimuksen kohde yrityksellä havaittiin kaksi pääongelmaa käyttäjähallinnassa. Pääongelmina oli, että käyttäjällä on joko liikaa oikeuksia tai ei ollenkaan sekä, että käyttöoikeuksien antaminen on todella työlästä. Pääongelmien lisäksi käyttäjähallinnassa oli havaittu ongelmia käyttäjien poistamisessa. Tutkimustyön tavoitteena on luoda ymmärrys yrityksen tämänhetkisestä käyttäjähallinnasta ja sen epäkohdista. Tutkimuksen tulosten tavoitteena on selvittää yritykselle tehokas ja tietoturvallinen tapa hallita käyttäjiä eri järjestelmien välillä. Tavoitteena olisi hoitaa kaikki käyttäjähallinta Microsoftin Azure Active Directory ryhmien kautta usean paikan sijaan. Työn tarkoituksena oli tutkia miten käyttäjähallinta tulisi suunnitella ja toteuttaa, jotta voitaisiin välttyä vastaavilta ongelmilta.

Tutkimus jakaantui kahteen osaan. Ensimmäisenä tarkasteltiin aihetta teoriaosuudessa. Ensimmäisessä teorialuvussa käsiteltiin pilvipalveluita, identiteetin- ja pääsynhallintaa, tietoturvallisuutta ja kyberturvallisuutta, käyttäjähallinta osana kyberturvallisuutta sekä automatisoitu käyttäjähallinta. Toisessa teorialuvussa käsiteltiin käyttäjähallinnan työkaluja, Azure Active Directorya and Azure Active Directory ryhmiä. Empiirisessä osuudessa toteutettiin haastatteluita asiantuntijoille. Haastateltavat olivat käyttäjähallinnan asiantuntijoita, kehittäjiä tai kohde yrityksen edustajia. Haastatteluista tehtiin yhteenveto ja vertailtiin tuloksia teoriaan.

Tutkimuksen tulokseksi saatiin, että tehokkaan ja käyttäjäystävällisen käyttäjähallinnan toteuttamisessa täytyy käyttäjähallintaprosessin suunnitteluun käyttää paljon aikaa ja vaivaa. Suunnittelua ei tulisi laiminlyödä. Organisaation tulisi hahmottaa oman käyttäjähallinnan iso kuva, jotta saadaan prosessista kokonainen. Roolipohjainen käyttäjähallinta koettiin erittäin hyödylliseksi tavaksi toteuttaa käyttäjähallinta. Jotta roolipohjainen käyttäjähallinta voidaan toteuttaa ja suunnitella, on ymmärrettävä organisaation rakenne ja dokumentoida se selkeästi. Automatisoitu käyttäjähallinta vähentää työtä ja nopeuttaa prosessia, mikä kuitenkin vaatii hyvin suunnitellun prosessin.

Avainsanat: Käyttäjähallinta, pilvipalvelut, tietoturvallisuus, IAM

ABSTRACT

Emma Ikonen: Design process for effective user management
Master's thesis
Tampere University
Master's Degree Program in Information and Knowledge Management
September 2022
Examiner: University Lecturer Ilona Ilvonen and University Lecturer Pasi Hellsten

---

User management affects the information security of companies. With the increase in cybercrime, data breaches can be very expensive for an organization and damage the organization's image. Monitoring user access through identity and access management is an essential step in developing a secure information security plan. Identity and access management is the process of ensuring that the appropriate individuals have access to the appropriate resources within an organization. Organizations change and grow. User management environments may have to be redesigned due to organizational changes.

Two main problems in user management were observed at the company that was the subject of the study. The main problems were that the user either has too many rights or none, and that granting access rights is tedious. In addition to the main problems, there was also problems with deleting users. The goal of the research work is to create an understanding of the company's current user management and its shortcomings. The goal of the research results is to find an efficient and data-secure way for the company to manage users between different systems. The goal would be to manage all user management through Microsoft's Azure Active Directory groups instead of several places. The purpose of the work was to investigate how user management should be planned and implemented in order to avoid similar problems.

The study was divided into two parts. First, the topic was examined in the theory part. The first theory chapter discussed cloud services, identity and access management, information security and cyber security, user management as part of cyber security and automated user management. The second theory chapter discussed user management tools, Azure Active Directory and Azure Active Directory groups. In the empirical part, interviews were conducted with experts. The interviewees were user management experts, developers or representatives of the target company. The interviews were summarized, and the results were compared with the theory.

The result of the research was that in order to implement an effective and user-friendly user management, a lot of time and effort must be spent on planning the user management process. Planning should not be neglected. The organization should understand the big picture of its own user management in order to get a complete picture of the process. Role-based user management was perceived as a very useful way to implement user management. In order for role-based user management to be implemented and planned, the structure of the organization must be understood and documented clearly. Automated user management reduces work and speeds up the process, which requires a well-planned process.

Keywords: User management, Cloud services, Information security, IAM

ALKUSANAT

Tämä tutkimus on tehty diplomityönä Tampereen yliopiston tietojohtamisen koulutusohjelmaan. Iso kiitos CGI Suomi Oy:lle mahdollisuudesta tehdä tämä diplomityö. Aihe syntyi asiakkaan kokemien ongelmien pohjalta. Tutkimuksen tarkoituksena oli selvittää mitä ongelmia asiakkaalla on käyttäjähallinnassa ja miten niihin voitaisiin vaikuttaa. Käyttäjähallinta oli itselleni alkuun suhteellisen tuntematon aihe, mutta työtä tehdessä opin paljon uutta aiheesta. Iso kiitos työn ohjauksesta ja ongelma tilanteissa avun saamisesta Pasi Hellstenille ja Ilona Ilvoselle. Tämä työ sai ensimmäiset askeleensa Suomen Lapin kaamoksessa ja viimeiset hengenvedot Espanjan auringon alla.

Opiskeluajasta haluan kiittää kaikkia opiskelukavereita, joilta olen saanut tukea ja apua läpi opintojen. Näiden upeiden vuosien aikana on tullut tutustuttua todella moniin mahtaviin henkilöihin, joita toivottavasti tulee nähtyä vielä opiskeluidenkin jälkeen. Olen erittäin kiitollinen TTHP ry:lle, Tietojohtajakilta Man@ger ry:lle sekä NMKSV ry:lle kaikesta toiminnasta ja tapahtumista, missä on saanut olla mukana niin osallistuja kuin järjestäjänä. Ilman kyseisten järjestöjen toimintaa olisi opiskeluvuodet olleet huomattavasti tylsempiä.

Vaikka diplomityö onkin yksilösuoritus, tarvittiin tässäkin työssä seinän tullessa vastaan sparrailuapua. Iso kiitos Jasminille ja Vilhelmille ideoista ja sparrailuista.

Gandiassa, 4.9.2022

Emma Ikonen

SISÄLLYSLUETTELO

KUVALUETTELO

LYHENTEET JA MERKINNÄT

AD	Active Directory
API	Application programming interface
DRBAC	Dynamic role-based access control
IAM	Identity and access management
HR	Human resource
IT	Information technology
MFA	Multi-factor authentication
OLAP	Online analytical processing
RBAC	Role-based access control
SSO	Single sign-on
UI	User interface

1. JOHDANTO

1.1 Tausta

Tässä työssä käsitellään yrityksen käyttäjähallintaa. Työssä keskitytään käyttäjähallintaprosessin parantamiseen. Tutkimusosuus tehdään toimeksiantona yritykselle. Tutkimuksen aihe syntyi yrityksen toimesta. Yritys kokee käyttäjähallintansa monimutkaiseksi ja työlääksi ylläpitää. Työn tavoitteena on tutustua käyttäjähallintaan yleisesti ja kehittää ehdotus, miten yritys pystyisi rakentamaan toimivamman ratkaisun olemassa olevan käyttäjähallinnan tilalle.

Pilvipalveluympäristöissä infrastruktuurin jakamisessa esiintyy usein kaksi ongelmaa käyttäjähallinnan suhteen, käytettävyys ja tietoturva (Lin *et al.* 2010). Käytettävyyteen vaikuttaa käyttäjien hallinnan helppous. Tietojen jakamisessa pilviympäristöissä suurimpia ongelmia Ahmad *et al.* (2015) mukaan on hallita käyttäjien pääsyä.

Aikaisempia tutkimuksia käyttäjähallinnan menetelmistä löytyy paljon. Joillakin organisaatioilla on edelleen käytössä paikallisia Active Directoryja. Paljon kuitenkin organisaatioita on siirtynyt hybridijärjestelmään. (Rongstad & Zhang 2021) Pilviaikakauden myötä käyttäjähallintaa on siirretty paljon käyttäjähallintaan erikoistuneiden pilvipalveluiden pariin. Käyttäjähallintaan käytettäviä identiteettien hallintapalveluita tarjoavat muun muassa pilvi-infrastruktuuriyritykset Amazon Web Services (AWS), Microsoft Azure ja Google Cloud (Mohammed 2019a). Edellä mainitut palveluntarjoajat tarjoavat, jokainen oman hybridi ratkaisun, jolla voi yhdistää paikallisen käyttäjähallinnan pilvipalvelun käyttäjähallintaan. Palveluilla voi integroida paikallisen kirjaston datan pilvipalveluun. (Amazon Web Services 2015, Google Cloud 2019, Microsoft 2021) Työn yritys käyttää Microsoftin Azure Active Directory pilvipalvelua käyttäjähallinnassaan.

Azure Active Directory tai Azure AD on Microsoftin pilvipohjainen identiteetin ja pääsynhallintapalvelu, jonka avulla työntekijät voivat kirjautua sisään ja käyttää resursseja, kuten Office 365:tä, Azure-portaalia ja tuhansia muita ulkoisia ohjelmistoja palvelusovelluksina verkossa sekä sisäisiä sovelluksia ja intranettiä. (Rongstad & Zhang 2021)

Organisaatiot muuttuvat ja kasvavat. Tästä seuraakin, että käyttäjähallintaympäristöjä voidaan joutua suunnittelemaan uudelleen organisaatiomuutosten takia. Muutokset kannattaa tehdä mahdollisimman nopeasti, kun huomataan uuden rakenteen tarve. Mitä

myöhemmäksi muutosta lykätään, sitä kalliimpi ja monimutkaisempi muutostyöstä tulee. (Francis 2021)

Identiteetin- ja käyttäjähallinnan ydinprosessi sisältää käyttäjien, autentikoinnin, valtuuksien, pääsyn, käyttötietojen hallinnan sekä auditoinnin ja toiminnan seurannan. Käyttäjien hallinnan tavoitteena on organisaation käyttäjien identiteetin elinkaaren hallintatoiminnot. Käyttäjän identiteetin aitouden määritysprosessin tulee olla tehokasta ja virheetöntä. Organisaation on määritettävä resurssien käyttöoikeudet käyttäjille, joilla on oikeus käsitellä resurssia. Käyttäjähallinnan prosessin täytyy olla suunniteltu siten, että pääsyoikeuksien pyytäminen ja jakaminen toimii moitteettomasti ja tietoturvallisesti. Prosessin tulee käsitellä identiteetti- ja pääsytietojen oikeellisuuden välittäminen organisaation tietokomponenttien välillä. Vaatimustenmukaisuuden seuranta-, auditointi- ja raportointiprosesseilla varmistetaan, että käyttäjien käyttöoikeudet ovat organisaatiolle määriteltyjen tehokkaiden pääsyturvakäytäntöjen mukaisia. (Brad & Munteanu 2012)

Kyberturvallisuusratkaisun tavoitteena loppujen lopuksi on hallita kenellä ja millä on pääsy sovelluksiin ja tietoihin, mikä on identiteetin ja pääsynhallinnan ydin. Hallinnassa käytettävien toimenpiteiden tavoite on varmistaa, että oikeat henkilöt voivat käyttää oikeita resursseja oikeaan aikaan ja oikeista syistä. (Alhija 2020) Käyttäjähallinta on iso osa organisaatioiden kyberturvallisuutta. Sen takia onkin erittäin kannattavaa tutkia ja parantaa yrityksen käyttäjähallintaprosessia. Prosessia parantaessa pystytään tarkistamaan käyttäjähallintaprosessin tietoturvallisuus ja käytettävyys, mitkä olivatkin Lin *et al.* (2010) mukaan kaksi yleisintä ongelmaa käyttäjähallinnassa.

1.2 Tutkimuksen ongelmat, tavoitteet ja tutkimuskysymykset

Tutkimuksen kohdeyrityksen käyttäjähallinnasta on tunnistettu kaksi pääongelmaa. Ensimmäisenä ongelmana on, että käyttäjällä on joko liikaa oikeuksia tai ei ollenkaan. Käyttäjät ovat saattaneet päästä tarkastelemaan sellaistakin dataan mihin ei pitäisi olla oikeuksia tai heillä ei ole ollut oikeuksia ollenkaan. Konsernitasolla tukifunktioiden, esimerkiksi HR ja talous, ryhmien käyttöoikeuksien ryhmittely on ollut puutteellista tai sitä ei ole ollut ollenkaan. Mikäli tukifunktiolle on annettu oikeudet, on oikeudet myös saanut useammalle funktiolle. Konserni jakaantuu useampaan liiketoimintayksikköön. Liiketoimintayksikkö tasolla on ollut samaa ongelmaa kuin konserni tasolla. Käyttäjillä on ollut pääsy, joko näkemään koko liiketoimintayksikön data tai ei ollenkaan. Liiketoimintayksikön datassakin olisi tasoja, joita pitäisi pystyä ryhmittelemään eri käyttäjäryhmille.

Toisena pääongelmana on, että käyttöoikeuksien antaminen on todella työlästä. Yrityksen Active Directory-ryhmät ovat sekava sotku. Ryhmät haluttaisiin selkeämmäksi ja virtaviivaisemmaksi käyttää. Käyttäjille käyttöoikeuksien antaminen on vaikeaa ja raskasta. Käyttäjäryhmät ovat rakennettu aina yhdelle järjestelmälle ja liiketoimintayksikölle, joten käyttäjiä on jouduttu lisäämään useisiin ryhmiin, mikäli on ollut tarvetta antaa useampaan järjestelmään oikeuksia. Käyttäjän poistuttua organisaatiosta on haasteellista poistaa häneltä kaikki käyttöoikeudet, koska ei tiedetä varmasti missä kaikissa AD-ryhmissä käyttäjä on. Ryhmät ja järjestelmät täytyvät käydä yksi kerrallaan läpi ja selvittää mihin kaikkiin käyttäjä oli lisätty. Työssä tarkasteltavia yrityksen käytössä olevia järjestelmiä ovat Manual UI, OLAP kuutiot, Power BI ja käyttöön otettavat Sustainability Database ja Power Apps. Eri järjestelmillä on erilaiset käyttäjähallintaprosessit. Käyttäjä voidaan joutua lisäämään kolmesta eri paikasta, jotta voi päästä raportoimaan oman liiketoimintayksikkönsä toimintoja ja tutkimaan oman liiketoimintayksikkönsä raportteja. Käyttäjä jouduttaisiin tällaisessa tilanteessa lisäämään AD-ryhmään, Manual UI kantaan ja Power BI työtilaan, jotta hän pääsisi raportoimaan, tutkimaan raporttien tietoja ja katselemaan raportteja.

Lisäksi ongelma on ollut oikeuksien poistaminen. Koska oikeuksia on jouduttu jakamaan useasta eri paikasta, ei ole tiedetty mistä kaikkialta käyttäjä täytyisi poistaa. Käyttäjätilien poistamista ei ole pystytty hallinnoimaan millään järjestelmällisellä tavalla. Mikäli oikeusryhmistä on löytynyt jokin tunnettu käyttäjätili, esimerkiksi entinen johtoryhmäläinen, on käyttäjältä osattu poistaa oikeudet. Ongelmana on myös se, että kukaan ei oikein tiedä kuka oikeuksia tarvitsee ja mihin. Käyttäjän poistuessa organisaatiosta oikeuksien poistamisesta ei koidu ongelmia, koska käyttäjätili poistuu käytöstä työsuhteen loppuessa. Käyttäjän siirtyessä organisaation sisällä toisiin tehtäviin, on käyttäjälle jäänyt oikeuksia resursseihin, mihin hänellä ei jatkossa olisi enää tarvetta.

Tutkimustyön tavoitteena on luoda ymmärrys yrityksen tämänhetkisestä käyttäjähallinnasta ja sen epäkohdista. Tutkimuksen tulosten tavoitteena on selvittää yritykselle tehokas ja tietoturvallinen tapa hallita käyttäjiä eri järjestelmien välillä. Tavoitteena olisi hoitaa kaikki käyttäjähallinta Microsoftin Azure Active Directory ryhmien kautta usean paikan sijaan. Työn yritys haluaa toteuttaa käyttäjähallintansa systemaattisemmin. Toiveena olisi, että kaikki käyttäjähallinta olisi keskitetty konserni tasolle, ja liiketoimintayksiköt pystyisivät itse hallinnoimaan dataansa. Liiketoimintayksiköissä osataan paremmin hallinnoida, kuka tarvitsee käyttöoikeuksia ja mihin. Kaikki liiketoimintayksiköiden data ei ole relevanttia koko yksikölle. Oikeuksia dataan pitäisi pystyä jakamaan liiketoimintayksikön sisällä eri tahoille eri määrä. Joillakin olisi vain oikeus päästä tarkastelemaan dataa ja toisilla on myös oikeudet muokata dataa.

Yritys haluaa, että tukifunktioiden dataa pääsisi katsomaan ja käsittelemään vain kyseisen funktion ylläpitäjät. Alkuperäisessä tilanteessa funktioita ei ole eriteltynä, joten eri funktioiden datan näki kaikki, joilla oli oikeus johonkin funktioon. Ideaali tilanne olisi esimerkiksi, että HR-dataa pääsee käsittelemään vain HR:ssä työskentelevät, joilla on oikeudet dataan. Esimerkiksi mikäli henkilöllä olisi tarve päästä käsittelemään tai tarkastella HR dataa, menisi hyväksymisprosessi HR-johtajan kautta.

Uusi käyttäjähallinta halutaan toteuttaa datalähtökohtaisesti eikä käyttäjälähtökohtaisesti. Datalähtökohtaisessa tarkastelutavassa yritys tarkastelee dataa ja selvitetään, kenelle oikeudet tarvitsee antaa. Kun taas käyttäjälähtökohtaisessa tarkastelussa yritys selvittäisi, mitä dataa käyttäjä tarvitsee.

Uusille käyttäjille oikeuksien lisääminen tulisi olla helppoa ja vaivatonta. Oikeusryhmät haluttaisiin rakentaa hierarkkisesti. Tällöin tietyt oikeudet periytyisivät pääryhmältä alaryhmille ja käyttäjälle, jotka on lisätty alaryhmään. Uudet ryhmät haluttaisiin rakentaa myös siten, että niitä voidaan käyttää myöntämään useammalle järjestelmälle oikeudet. Tällöin ei tarvitsisi olla niin montaa eri ryhmää ja käyttäjiä ei tarvitsisi lisätä niin moneen ryhmään. Esimerkkinä, jos käyttäjällä on oikeus päästä syöttämään liiketoimintayksikön dataa Manual UI:n kautta voisi hänelle antaa oikeudet päästä näkemään liiketoimintayksikön dataa kuutioista. Tällöin voitaisiin käyttäjä lisätä ryhmään mitä kautta hän saisi oikeudet kyseisen liiketoimintayksikön Manual UI:hin ja kuutioon.

Tutkimuksen tarkoituksena on siis tutkia yrityksen käyttäjähallintaa ja selvittää miten se on toteutettu eri järjestelmien välillä. Työn tavoitteena on kehittää konkreettisia kehitysehdotuksia paremman ja tietoturvallisen käyttäjähallinnan saavuttamiseksi. Tavoitteeseen pyritään pääsemään tutustumalla käyttäjähallinnan teoriaan ja yrityksen tilanteeseen, sekä haastattelemaan alan asiantuntijoita. Tutkimukselle määritettiin tutkimusongelman pohjalta pää- ja alatutkimuskysymykset, mihin tutkimuksella pyritään löytämään vastaus. Tutkimuksen päätutkimuskysymyksenä on:

- Miten toteuttaa tehokas ja käyttäjäystävällinen käyttäjähallinta konsernin tasoisessa organisaatiossa, jossa on useita järjestelmiä ja liiketoimintayksiköitä?

Tutkimuksen alatutkimuskysymykset ovat:

- Mitä on käyttäjähallinta?
- Miten käyttäjähallinta vaikuttaa tietoturvaan?
- Mitä ongelmia käyttäjähallinnassa esiintyy?

1.3 Tutkimuksen rajaukset

Työn aihetta pohdittaessa yritys kertoi ongelmansa olevan, että käyttäjällä on joko liikaa oikeuksia tai ei ollenkaan, käyttöoikeuksien antaminen on todella työlästä ja oikeuksien poistaminen on tuottanut ongelmia. Ensimmäiseen ongelmaan käyttöoikeuksien liiallisesta laajuudesta oli myös huomattu, että Power BI raportteja tehneet henkilöt eivät välttämättä tienneet tarkalleen mitä olivat tekemässä. Käyttäjät olivat saattaneet huomaamatta jakaa dataa vääriin paikkoihin.

Työn aiheen suunnitteluvaiheessa pohdittiinkin olisiko työ voinut sisältää käyttäjähallinnan uudistamisen lisäksi Power BI super user koulutusmateriaalin suunnittelun ja toteuttamisen. Nopeasti kuitenkin tultiin siihen lopputulokseen, että työ rajataan käsittelemään ainoastaan käyttäjähallinnan yhtenäistämistä. Power BI koulutusten suunnittelu ja toteutus olisi laajentanut työtä niin paljon, ettei työstä olisi enää saanut selkeää kokonaisuutta aikaiseksi.

Tutkimus rajattiin keskittymään yrityksellä jo käytössä olevien BI-alueen järjestelmien ja muutamaan käyttöön tulevan BI-järjestelmän käyttäjähallintaan. Yritys raportoi, säilöö ja analysoi dataa työssä käsiteltävien järjestelmien avulla.

1.4 Tutkimuksen rakenne

Työn rakenne koostuu seitsemästä osasta. Ensimmäinen luku on työn johdanto, missä käydään läpi tutkimusaiheen taustaa, tutkimuksen ongelmat, tavoitteet ja tutkimuskysymykset, tutkimuksen rajaukset ja tutkimuksen rakenne. Toisessa luvussa syvennytään tutkimuksessa käytettyihin menetelmiin tutkimusmetodologian, kirjallisuuskatsauksen aineistonkeruun, empiirisen tutkimuksen ja aineiston analysoimisen kautta.

Ennen itse tutkimusta perehdytään teorian avulla aiheeseen. Teoria on toteutettu kirjallisuuskatsauksena. Teoria on jaettu kahteen lukuun. Ensimmäisessä teoria luvussa käsitellään pilvipalveluita, identiteetin ja pääsynhallintaa, tietoturvallisuutta yleisesti ja käyttäjähallinnan roolia tietoturvallisuudessa. Toisessa teoria luvussa käydään käyttäjähallinnan työkaluja yleisesti läpi, minkä jälkeen tutustutaan Azure Active Directory palveluun ja sen ominaisuuksiin.

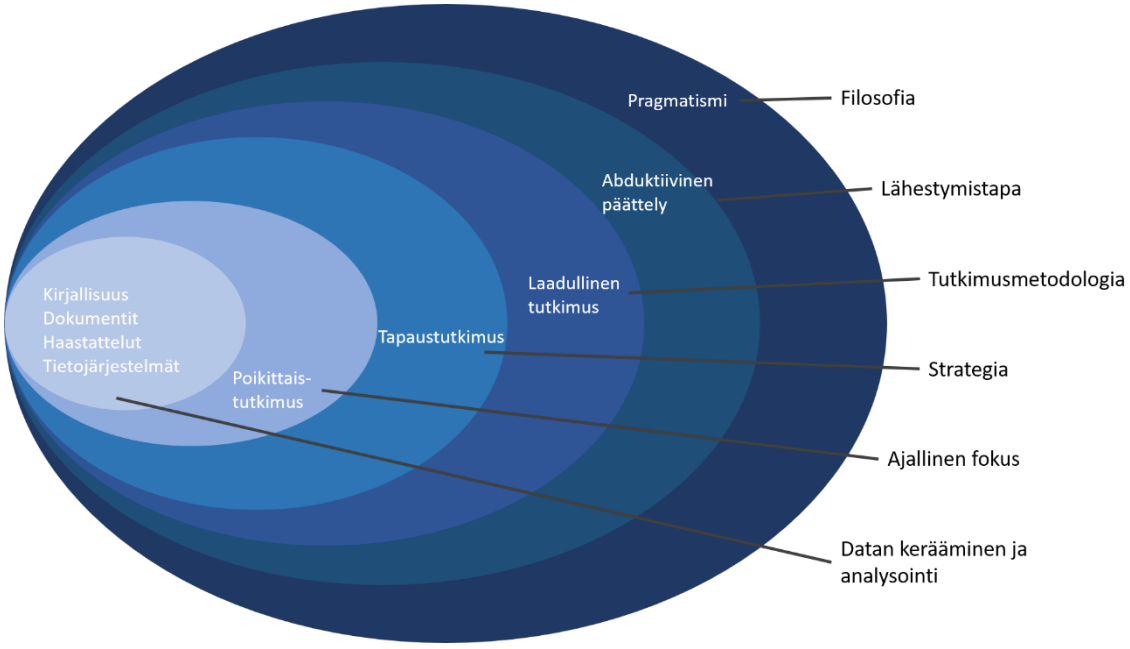
Viidennessä luvussa käydään yrityksen nykytilaa läpi. Tutustutaan, millainen organisaatio on työn kohteena, millaisia järjestelmiä yrityksellä on käytössä ja miten niiden käyttäjähallinta on toteutettu, sekä mitkä ovat tavoitteet järjestelmien käyttäjähallinnan suhteen. Luku kuusi on tutkimusluku, jossa käydään läpi mitä tuloksia haastatteluista on saatu. Viimeisessä luvussa käydään koko työn tulokset läpi ja vastataan tutkimuskysymyksiin.

2. TUTKIMUSMENETELMÄT

Tässä luvussa käydään tutkimuksen toteuttamiseen käytetyt menetelmät läpi. Ensimmäisenä esitellään tutkimuksen tutkimusmetodologiaa Sauders et al. (2016) sipulimallia hyödyntäen. Tämän jälkeen käydään läpi kirjallisuustutkimuksen aineiston hankinta- ja analysointimenetelmää. Kirjallisuustutkimuksen jälkeen tutustutaan haastattelututkimuksen toteuttamiseen ja viimeisenä aineiston analysoimiseen.

2.1 Tutkimusmetodologia

Saunders et al. (2016) on määritellyt sipulimallin, jonka ideana on koota tutkimuksen tekemiseen vaikuttavat tutkimusmenetelmät yhteen malliin. Tässä tutkimuksessa käytetty sipulimalli on kuvattuna kuvassa 1. Sipulin uloimmalta kerrokselta löytyy tieteenfilosofia. Seuraava kerros sisältää tutkimuksen lähestymistavan. Lähestymistavasta seuraavalla kerroksella on tutkimusmetodologia. Seuraavalla kerroksella on tutkimuksen strategia. Strategian jälkeiseltä kerrokselta löytyy tutkimukseen käytettävä ajallinen fokus. Kaikista sisäisimmältä kerrokselta löytyy datan kerääminen ja analysointi. Seuraavaksi käydään sipulimallin kerrokset tarkemmin läpi.



Kuva 1. Tutkimuksen metodologiset valinnat (mukaillen Saunders et al. 2016)

Tutkimusfilosofian perustana on arvioida tiedettä (Anttila 1998). Tähän työhön valikoitui tutkimusfilosofiaksi pragmatismi. Pragmatismi keskittyy ratkaisemaan ongelman ja kehittämään käytännön ratkaisuita. Pragmatismin mukaan käsitteet ovat merkityksellisiä tukiessaan toimintaa. Pragmatismissa tutkimussuunnitelman ja strategian kannalta tärkein tekijä on tutkimusongelma ja tutkimuskysymys. Kvalitatiivisia ja kvantitatiivisia tutkimusmenetelmiä käytetään usein sekaisin pragmatismissa. Pragmatismi pitää tavoiteltavaa tietoa sellaisena, jolla mahdollistetaan asioiden tekeminen oikein. (Saunders et al. 2016) Ongelmat tunnistettua nykyisessä käyttäjähallinnassa, voidaan kehittää uusia tapoja käyttäjähallinnalle, kun poiketaan olemassa olevista rutiineista.

Tieteellinen lähestymistapa määrittelee, miten teoriaa lähestytään tutkimuksessa. Lähestymistapoja on induktiivinen ja deduktiivinen sekä niiden sekoitus abduktiivinen. Deduktiivisessa ensin tehdään teoria, minkä perusteella tehdään havaintoja. Induktiivisessa tavassa asia on toisinpäin, ensin havainnot ja sitten teoria. Abduktiivisessa tavat yhdistetään niin, että ensin tehdään havaintoja, joiden pohjalta teoria ja teorian pohjalta uusia havaintoja. (Saunders et al. 2016)

Tutkimusmetodologian valinnassa on kolme vaihtoehtoa, kvantitatiivinen, laadullinen ja sekoitettu tutkimus. Kvantitatiivinen tutkimus tutkii muuttujien välisiä suhteita, joita mitataan numeerisesti ja analysoidaan käyttämällä erilaisia tilastollisia ja graafisia menetelmiä. Laadullinen tutkimus tutkii osallistujien merkityksiä ja niiden välisiä suhteita käyttämällä erilaisia tiedonkeruutekniikoita ja analyyttisiä menetelmiä. Sekoitetussa tutkimuksessa käytetään molempia, kvantitatiivista ja laadullista, sekaisin. (Saunders et al. 2016) Tässä tutkimuksessa käytetään laadullista tutkimusta. Tutkimus tehdään kirjallisuuskatsauksena ja tapaustutkimuksena. Näistä tiedoista saadaan ei-numeraalista aineistoa, joilla tutkimus voidaan toteuttaa.

Tutkimuksen tutkimusstrategian tavoitteena on määriteellä tapa, jolla saavutetaan tutkimuksen tavoitteet ja pystytään vastaamaan tutkimuksen tutkimuskysymyksiin (Saunders et al. 2016). Tässä tutkimuksessa tutkimusstrategiana toimii tapaustutkimus. Tapaustutkimuksessa "tapaus" voi viitata henkilöön, ryhmään, organisaatioon, yhdistykseen, muutosprosessiin, tapahtuma sekä moniin muihin tapauksiin. Tässä tutkimuksessa tapaus viittaa yritykseen. Tapaustutkimus pyrkii ymmärtämään tutkittavan aiheen dynamiikan sen ympäristössä. Aiheen dynamiikan ymmärtämisellä tarkoitetaan vuorovaikutusta tapauksen kohteen ja sen ympäristön välillä. Tapaustutkimusstrategialla on kyky luoda oivalluksia ilmiön tosielämän kontekstissa, mikä johtaa runsaisiin, empiirisiin kuvauksiin ja teorian kehittämiseen. (Saunders et al. 2016) Tässä tutkimuksessa tapaustutkimuksessa tutkitaan käyttäjähallintaa yrityksessä.

Tutkimuksen aikahorisontti määrittelee tutkimukseen käytetyn ajan käytön. Poikittaistutkimuksessa tutkimus on toteutettuna tietyllä ajanhetkellä ja aineisto on kerätty tutkimushetkellä. Pitkittäistutkimuksessa tutkimuksen tekoon kuluu pidempi aika, sillä tutkittavan asian muuttumista ja kehittymistä seurattaisiin ajan kuluessa. (Saunders et al. 2016) Tässä tutkimuksen aikahorisonttina on poikittaistutkimus, koska aineisto kerätään tiettynä ajanhetkenä ja tutkimukseen ei ole käytettävissä pitkää aikaväliä. Tässä tutkimuksessa käytetty käyttäjähallintaan liittyvä kirjallisuusaineisto on kerätty vuosilta 2010-2022.

Työssä kerätään dataa käyttäjähallinnan menetelmistä ja yrityksen käytöstä olevasta käyttäjähallinnasta. Koska tämä tutkimus on jaettu kahteen osaan, kirjallisuuskatsaukseen ja empiiriseen tutkimukseen, on datankeruu molemmissa hieman erilainen. Kirjallisuuskatsauksen datanhankinta menetelmät on käsitelty luvussa 2.2. Tutkimuksessa käytetään harkinnanvaraista otantaa, koska aineisto kerätään sen perusteella mikä vastaa tutkimusaihetta (Saunders et al. 2016). Yrityksen käyttäjähallinnasta ja tavoitteista data kerätään dokumenteista ja keskustelemalla yrityksen edustajien kanssa. Käyttäjähallinnan kehittämiseen liittyen järjestetään asiantuntijoiden kanssa haastattelut.

2.2 Kirjallisuustutkimus

Tässä luvussa käydään läpi kirjallisuuskatsauksen aineiston keruumenetelmä ja analysointimenetelmät. Kirjallisuuskatsauksen avulla tutustuttiin tutkimuksen aiheen teoreettiseen puoleen ja aiempiin tutkimuksiin aiheesta. Kirjallisuuskatsauksessa arvioidaan ja referoidaan aiempia tutkimuksia. Kirjallisuuskatsaus on systemaattinen ja toistettavissa oleva prosessi. Jotta kirjallisuuskatsauksesta saadaan tällainen, on sen tekemisessä käytetty Finkin mallia. Salminen (2011) mukaan Finkin (2005) mallissa ensimmäisenä asetetaan tutkimuskysymys. Toisena valitaan tietokannat, joita käytetään tiedostojen hakemiseen. Kolmantena kohtana valitaan hakutermit, joilla kirjallisuutta haetaan. Neljäntenä vaiheena on hakutulosten karsinta esimerkiksi kielen tai lähteen julkaisuvuoden perusteella. Sen jälkeen karsitaan tuloksia vielä tulosten laadun perusteella. Kuudentena vaiheena on tutkimuksen tekeminen. Viimeisenä tuloksista tehdään yhteenveto.

Alkuun tietoa haettiin lähtökohtaisesti suomeksi ja sen jälkeen vielä syvennyttiin englanninkielisiin materiaaleihin. Lähdemateriaalien lähdeluetteloista löytyi usein lisää tähän tutkimukseen sopivia lähteitä. Tutkimuksen lähdemateriaalien löytämiseen käytettiin Andor ja Google Scholar tiedonhakupalveluita. Google Scholarin laaja haku toiminto tuotti paljon osumia. Scholaria käyttäessä ongelmana kuitenkin oli usein, että aineisto oli maksumuurin takana tai aineistot eivät olleet tieteellistäkirjallisuutta. Andor on Tampereen

yliopiston hakupalvelu, josta usein löytyi samat aineistot kuin Google Scholarista. Andorista löytyneet aineistot sai ilmaiseksi käyttöön kirjauduttua sisään opiskelijatunnuksilla. Aineistoja tutkimuksen taustaksi etsittiin käyttäjähallintaan, ja tietoturvallisuuteen liittyviä aiheita ja teoksia. Kirjallisuuden löytämiseksi käytettiin muun muassa seuraavia hakusanoja:

- ”Käyttäjähallinta”
- ”User management” AND ”security problems”
- ”User Access Management” AND process
- “Identity Access Management”
- “Identity Access Management” AND security
- “Identity Access Management” AND cloud
- “Information security” AND “IAM”

Pääasiassa aikaisemmat tutkimukset ovat opinnäytetöitä ja tieteellisiä tutkimuksia mutta myös kirjoja. Tutkimuksessa on käytetty paljon lähteitä, joita on pyritty tutkimuksessa saamaan keskustelemaan keskenään. Hakutuloksia oli paljon, eikä kaikki tulokset vastanneet vaadittavan lähdemateriaalin kriteereitä. ”Identity access management” hakulausekkeella tuli 1 670 tulosta. Tuloksista haluttiin karsia väärät aiheet, ei-tieteelliset materiaalit ja liian vanhat materiaalit pois. Lähdeaineistona pyrittiin käyttämään 2010-luvun jälkeen toteutettuja tutkimuksia. Karsinta toteutettiin suodattimilla hakua tehdessä, jolloin hakutuloksista karsiutui ei halutut pois. Tarkennetun haun jälkeen luettiin teoksista aluksi otsikot, tiivistelmä ja sisällysluettelo, ja mikäli tutkimuksen sisältö vastasi tutkittavaa aihetta, jatkettiin aineiston tutkimista. Aineistot, jotka käsittelivät käyttäjähallintaa pilvipalveluissa ja käyttäjähallinnan turvallisuusongelmia pilvipalveluissa otettiin tarkasteluun. Aineistot, jotka käsittelivät vanhempia käyttäjähallinnan sovelluksia, kuten paikallisia käyttäjähallintasovelluksia, jätettiin tarkastelun ulkopuolelle. Tarkasteluun otetuista aineistoista silmäiltiin luvut läpi ja etsittiin tutkimuksen aiheelle relevantit kohdat ja luettiin ne.

2.3 Haastattelututkimus

Tässä työssä käytetiin haastattelututkimusta yhtenä aineiston keruumenetelmänä. Haastattelua varten suunniteltiin kysymysrunko, jonka pohjalta haastattelut toteutettiin. Haastattelukysymys runko oli pitkä. Kaikkia kysymysrungon kysymyksiä ei kysytty haastatteluissa, sillä aika ei riittänyt kuin murto-osan käyntiin. Osassa haastatteluissa ehdittiin

käymään useampia kysymyksiä, koska haastateltavat vastasivat lyhyemmin ja nopeammin kuin muut haastateltavat. Kysymysrungon lisäksi kysyttiin muita kysymyksiä haastateltavien vastausten pohjalta.

Haastattelutyylinä toimi siis puolistrukturoitu haastattelu. Puolistrukturoitu haastattelu toimi paremmin, kuin strukturoitu haastattelu, koska puolistrukturoitu haastattelu on joustavampi. Puolistrukturoidussa haastatteluissa on lista aiheista ja mahdollisesti keskeisistä kysymyksistä. Kysymysten käyttö voi vaihdella haastattelusta toiseen. Voidaan joko jättää tietyissä haastatteluissa joitakin kysymyksiä pois, vaihdella kysymysten järjestystä tai esittää lisäkysymyksiä. (Saunders et al. 2016)

Haastattelua suunnitellessa Saunders et al. (2016) suosittelevat, että haastattelijalla on tarpeeksi tietoa tutkimuksen aiheesta. Tällöin haastattelija pystyy osoittamaan haastateltaville uskottavuutta, arvioimaan vastausten oikeellisuutta ja rohkaisemaan haastateltavaa vastaamaan yksityiskohtaisemmin haastattelukysymyksiin. Teoria on kirjoitettu ennen haastatteluita, jotta haastatteluita pidettäessä haastattelijalla on tarpeeksi tietoa tutkimusaiheesta.

Uskottavuuteen voidaan myös vaikuttaa antamalla haastattelukysymykset haastateltavalle etukäteen. Tällöin haastateltava voi valmistautua haastatteluun esimerkiksi käymällä läpi projektin dokumentteja, mistä on kulunut aikaa. (Saunders et al. 2016) Kysymysten lähettäminen haastateltavalle ennen haastattelua voi tuoda muistoja paremmin mieleen. Haastateltavalla saattaa olla dokumentteja haastattelun teemaan liittyen, joita hän pystyisi tutkimaan ennen haastattelua. Tällöin haastateltavat pystyvät valmistautumaan kysymyksiin paremmin ja voidaan saada tarkempia vastauksia. Voi kuitenkin olla mahdollista, että haastateltava valmistautuu haastatteluun valmiilla kerronnalla tietäessään kysymykset. Tällaisessa tapauksessa haastattelutilanteen aitous ja vastavuoroinen kohtaaminen saattaa kärsiä. (Heimo et al. 2021) Selvittäessä haastateltavien tunteita tutkimus aiheeseen liittyen voi haastatteluaineiston etukäteen lähettäminen muuttaa muistikuvia kysymykseen liittyen, ja mahdollisuus keskustella asiasta jonkun kanssa saattaa muuttaa tuntemuksia kysymyksen aiheeseen liittyen.

Vaikka tämän haastattelun tavoitteena ei ole selvittää haastateltavien tunteita, olisi kysymykset voitu jakaa haastateltaville etukäteen. Lopulta päädyttiin jakamaan haastattelun teemat etukäteen, muttei valmiita kysymyksiä. Yksi haastateltava antoi palautetta haastattelun jälkeen, että olisi toivonut kysymykset etukäteen, jolloin hän olisi voinut valmistautua ja antaa parempia vastauksia.

Haastateltavien valitseminen on Saunders et al. (2016) mukaan, joko kiintiö, tarkoituksenmukainen, vapaaehtoinen tai satunnainen näytteenotto, jotka jakaantuvat vielä erilaisiin tekniikoihin. Kiintiö otannassa haastattelu otanta on täysin ei-satunnainen ja perustuu olettamukseen, että otos edustaa kohdepopulaatiota. Tarkoituksenmukaisella otannalla haastateltavat valitaan sen mukaan, joiden avulla saadaan varmasti kattavia vastauksia tutkimuskysymyksiin ja saavutetaan tavoitteet. Vapaaehtoisessa otannassa haastateltavat voivat ottaa yhteyttä haastattelijan jättämään haastatteluilmoituksen ansiosta. Satunnaisessa otannassa tapauksilla ei ole selvää organisointiperiaatteita tutkimuskysymykseen.

Tässä tutkimuksessa parhaana tapana kerätä haastateltavat on tarkoituksenmukaisen otannan perusteella. Haastatteluissa halutaan haastatella tutkimusaiheen asiantuntijoita, kehittäjiä ja yrityksen puolelta asiantuntijoita, jotka osaavat vastata kyseisiin järjestelmiin liittyviin kysymyksiin. Käyttäjähallinnan asiantuntijoita etsittiin haastateltavaksi palvelutuottajan omista työntekijöistä. Palveluntuottajan IAM-palvelutiimin esihenkilöön otettiin yhteyttä ja kysyttiin, osaisiko hän neuvoa ketä voisi haastatella. Kyseinen henkilö oli sairaslomalla pidemmän aikaa, joten sama viesti lähetettiin toiselle henkilölle tiimistä. Henkilön suostui haastatteluun ja vinkkasi vielä, ketä voisi vielä haastatella käyttäjähallinnan asiantuntijoista.

Jotta saatiin selville, ketkä olisivat sopivia haastateltavia yrityksen puolelta, otettiin yhteyttä yrityksen IT-johtajaan. IT-johtajan lisäksi yritykseltä haastatteluun sopivia olivat tietoturvajohtaja ja prosessikehityspäällikkö. Näiden lisäksi haastateltiin palveluntuottajan työntekijöitä, jotka olivat olleet kehitystehtävissä. Koska haastateltavissa ei ollut kovin montaa vaihtoehtoa ei mikään muu kuin tarkoituksenmukainen otanta olisi toiminut.

Haastateltavat on jaettu kolmeen ryhmään. Ryhmä 1 on IAM asiantuntijat. Ryhmä 2 on kehittäjät. Ja Ryhmä 3 on tutkimuksen kohdeyrityksen asiantuntijat. Haastateltavilta kysyttiin haastattelun alkuun esittelemään itsensä ja työkokemuksensa. Esittelyn jälkeen selvitettiin haastateltavien kokemukset käyttäjähallinnan projekteissa, mikäli se ei tullut työtehtävien esittelyssä selville. Haastateltavat ryhmineen ja tehtävänimikkeineen on koottu taulukkoon 1.

H1 työskenteli palvelutuottajalla IAM asiantuntijanroolissa. Haastateltavalla oli pitkä ura identiteetti ja käyttäjähallinta palveluiden parissa. Haastateltava oli toiminut 20 vuoden ajan käyttäjähallinnan alalla. Haastateltava oli ollut kehittämässä muun muassa kypsyys mallia IAMiin, jonka tarkoitus on ymmärtää asiakkaan kanssa missä he ovat IAMin suhteen. Aikaisemmin työtehtävät olivat olleet kirjautumisen ja tunnistautumisen ympärillä,

kun taas nykyisessä organisaatiossa työtehtävät ollut enemmän käyttäjähallintaan ja käyttöhallintaan liittyviä.

H2 oli työskennellyt laajasti eri IT-projektien parissa. Haastateltava oli aloittanut kehittäjän roolissa 10 vuotta sitten. Vuosien aikana oli kertynyt paljon kokemusta erilaisista IT-projekteista. Identiteetin ja pääsyhallinnan projekteja oli ollut aikaisemminkin. Nyt toimi nykyisellä työnantajalla IAM arkkitehtinä. Haastateltava oli ollut mukana muun muassa Suomen isompien firmojen IAM projekteissa. Kyseessä ollut sisäisiä ja ulkoisia käyttäjiä, robotteja, service accaunteja ja elinkaaren hallinnan prosesseja. Tutkimuksen kohdeyritysten IAM projektien koot olivat vaihdelleet 500 – 80 000 identiteettiä.

H3 työskenteli palveluntuottajalla IAM asiantuntijana ja IAM tiimin esihenkilönä. Haastateltava oli työskennellyt 20 vuotta IAM projektien parissa.

H4 työskenteli palvelutuottajalla kehittäjäroolissa. Kokemusta oli IT-alalla ehtinyt kertymään 10 vuodelta. Haastateltava oli tehnyt front end kehitys tehtäviä, mistä oli siirtynyt back end kehittäjäksi ja nyt toimi Fullstack kehittäjänä. Haastateltava oli ollut mukana kehittämässä identity palveluita, autentikaatio systeemeitä, asiakkaan asiakastietokannan hallintaa ja käyttöönottamassa Azure B2C.

H5 työskenteli myös palvelutuottajalla kehittäjäroolissa ja oli ollut alalla 15 vuotta ja toiminut myöskin monissa eri rooleissa. Haastateltava oli aloittanut 3D grafiikan piirissä ja kosketusnäyttöjen ohjelmistojen kanssa. Sen jälkeen tehnyt UI-suunnittelua ja UI-koodausta web sivustoille. Nykyisellä työnantajalla ollut pilviteknologioissa. Käyttäjähallintaan liittyen työtehtäviä oli ollut käyttöliittymän puolella. Haastateltava oli ollut toteuttamassa järjestelmäintegraatioita, joissa liikkui käyttäjätietoa.

Taulukko 1 Haastateltavien roolit ja tehtävänimikkeet

Hnro	Rooli	Tehtävänimike
H1	Ryhmä 1	IAM konsultti
H2	Ryhmä 1	IAM arkkitehti
H3	Ryhmä 1	IAM konsultti
H4	Ryhmä 2	Kehittäjä
H5	Ryhmä 2	Kehittäjä
H6	Ryhmä 3	IT-johtaja
H7	Ryhmä 3	Prosessikehityspäällikkö
H8	Ryhmä 3	Tietoturvavastaava

H6 työskenteli tutkimuksen kohdeyrityksellä IT-johtajanroolissa. Haastateltavalla oli IT-alueita vastuullaan eri funktioilta. Haastateltavalla oli ollut 11 vuotta töissä kyseisellä yrityksellä ja 1,5 vuotta ollut nykyisessä työtehtävässä. Sitä ennen oli toiminut master data puollella projektipäällikkönä vuoden. Tytäryhtiölle työskennellessä oli ollut käyttäjähallinnan prosesseissa mukana. Tällöin prosesseja yritettiin suoraviivaistaa tytäryhtiön osalta. Täydellistä prosessia ei saatu aikaiseksi, koska kyseessä konserni, joka yrittää pitää samat pelisäännöt kaikilla.

H7 työskenteli tutkimuksen kohdeyrityksellä prosessikehittäjäpäällikkönä. Haastateltava oli työskennellyt yrityksessä 30 vuotta ja nykyisessä työtehtävässä 10 vuotta. Aikaisempia työtehtäviä oli ollut muun muassa ERP tuessa tulkkaamassa käyttäjien tarpeita. Nykyään haastateltava on tehnyt Power BI raportteja.

H8 työskenteli tutkimuksen kohdeyrityksellä tietoturvavastaavana ja IT-infra-arkkitehtinä. Työkokemusta haastateltavalla oli 24 vuotta. Aikaisemmin oli toiminut muun muassa järjestelmäasiantuntijana. Työkokemusta käyttäjähallinnan työtehtävien parissa haastateltavalla oli muun muassa yritysten kokonaisvaltaisessa identiteetin hallinnassa, yksittäisten sovellusten ja web-sovellusten identiteetinhallinnasta.

Kontaktihenkilöiltä saaduille henkilöille laitettiin sähköpostia tai viestiä Teams-palvelussa, missä kerrottiin haastattelusta ja tutkimustyön aiheesta. Samassa viestissä ehdotettiin haastatteluaikaa. Kalenterikutsussa listattiin haastattelun teemat ja kerrottiin toiveesta nauhoittaa haastattelu. Haastateltavista kolme oli IAM palveluiden asiantuntijoita, kaksi palveluntarjoajan kehittäjiä ja kolme tutkimuksen kohdeyrityksen työntekijöitä. Haastattelut järjestettiin kahden viikon mittaisen ajanjakson aikana ja haastattelutilaisuuksille oli varattu tunti. Haastatteluissa meni 45 minuutista tuntiin.

Haastattelut järjestettiin yksilöhaastatteluina ja etänä. Etähaastattelut järjestettiin Teams yhteistyöalustan avulla. Haastateltavilta kysyttiin haastattelun alussa, sopiiko, että haastattelu nauhoitetaan. Jotta kaikki haastatteluista saatu data saatiin talteen, äänitettiin haastattelu tilanteet. Tällöin itse haastattelutilanne oli luontevampi, kun haastattelussa pystyttiin keskittymään vain keskusteluun eikä vastauksia tarvitse yrittää kirjoittaa ylös samassa hetkessä. Äänitteet käytiin lopuksi läpi ja kirjoitettiin auki.

Haastattelu eteni haastattelukysymysrungon mukaan (Liite A). Haastattelun kysymysrunko mukailee tutkimustyön teorialukujen järjestystä. Haastattelun teemat muodostettiin siten, että ne vastasivat mahdollisimman hyvin tutkimuskysymyksiin. Ensimmäisenä haastattelussa tutustutaan haastateltavaan ja keskustellaan haastateltavan kokemuk-

sista tutkimusaiheesta. Sen jälkeen siirrytään yleisesti käyttäjähallinnan ja käyttäjähallinnan prosessiin liittyviin kysymyksiin. Kun on käyty käyttäjähallinta yleisesti läpi, siirrytään käyttäjähallinnan rooliin tietoturvallisuudessa. Tietoturvallisuuden jälkeen kysymykset keskittyvät ensin erilaisten käyttäjähallinta tapojen selvittämiseen ja sen jälkeen Azure AD:seen ja Azure AD ryhmien hyödyntämiseen käyttäjähallinnan toteuttamisessa. Viimeisenä haastattelussa on kysymyksiä käyttäjien oikeuksien poistamiseen liittyen ja käyttäjähallinnan automatisoimisesta. Mikäli jokin vastaus jäi suppeaksi, saatettiin kysymysrungon lisäksi kysyä tarkentavia kysymyksiä.

2.4 Aineiston analysointi

Haastatteluissa kerättiin tietoa käyttäjähallinnan toteuttamisesta. Haastatteluista saatu aineisto analysoitiin temaattisella analyysillä. Braun ja Clarken (2006) mukaan temaattinen analyysi tunnistaa, analysoi ja raportoi säännönmukaisuuksia eli teemoja, joita löytyy datasta. Teema on oleellista tietoa suhteessa tutkimuskysymykseen (Braun ja Clarke 2006). Temaattinen analysointi sisältää kuusi vaihetta. Analyysin vaiheet ovat: 1) Tutustuminen aineistoon ja litterointi, 2) Aineiston koodaaminen ja koodiston luonti, 3) Teemojen luominen, koodatun aineiston kokoaminen, 4) Aineiston ja teemojen uudelleen arviointi, 5) Teemojen nimeäminen ja määritys, 6) Raportin tuottaminen (Braun & Clarke 2006; Vaismoradi et al. 2013; Nowell *et al.* 2017).

1. Aineistoon tutustuminen ja litterointi

Haastatteluiden aikana ei tehty muistiinpanoja, koska haluttiin keskittyä itse keskustelutilaisuuteen. Keskustelutilaisuuden aikana kirjattiin muistiinpanoihin kysymykset, jotka kysyttiin kysymysrungon lisäksi. Haastattelunauhoitteet kuunneltiin ja kirjoitettiin auki viikon sisällä haastattelu hetkestä.

Haastattelu tallenteita läpikäydessä ei haastatteluita litteroitu täysin sanatarkasti. Ainoastaan sellaiset vastaukset litteroitiin sanasta sanaan, jotka kiteyttivät vastauksen kysymykseen tiiviisti ja osuvasti. Haastatteluita pyrittiin saamaa mahdollisimman tiiviiseen muotoon, kuitenkin niin, että vastaus ei muuttunut. Näin aineiston läpikäyminen myöhemmin oli helpompaa, koska aineistoista oli karsittu täytelauseet ja toistot pois ja jäljelle jäi vain oleellinen asia.

2. Koodiston luonti kirjallisuudesta tunnistettujen teemojen pohjalta

Toiseen vaiheeseen siirryttiin, kun data oltiin käyty läpi. Toiseen vaiheeseen siirryttäessä oli käsitys mitä data sisälsi ja mitä kiinnostavaa sieltä löytyisi. Toiseen vaiheeseen kuuluu

koodien alustava luominen datasta. Koodauksen avulla voidaan yksinkertaistaa ja keskittyä datan tiettyihin ominaisuuksiin. Aineiston koodaamiselle on useita eri tekniikoita olemassa. Mitä tahansa tekniikkaa käytetäänkin, on tärkeää soveltaa sitä johdonmukaisesti kaikkeen tietoon. (Nowell *et al.* 2017)

Tutkimuksen kategoriat muodostettiin kirjallisuuden pohjalta. Kirjallisuuden pohjalta tunnistetut teemat olivat: käyttäjähallinta yleisesti, käyttäjähallinnan merkitys yrityksille, käyttäjähallinnan vaikutus tietoturvallisuuteen, Azuren rooli käyttäjähallinnassa, käyttäjähallinnan automatisointi, käyttäjähallinnan ongelmia ja uuden käyttäjähallintaprosessin suunnittelu. Teemat olivat pitkälti samat mitkä oli tunnistettu haastattelukysymysrunkoa tehdessä. Näiden teemojen lisäksi tehtiin löydös haastattelu aineistosta, jota ei oltu poimittu kirjallisuudesta. Haastattelun aineistosta löydetty teema oli: roolipohjainen käyttäjähallinta. Tässä työssä näkökulmana käytettiin abduktiivista lähestymistapaa, eli kirjallisuuskatsauksen teorian pohjalta muodostettiin kysymysrungolle teemat ja haastattelukysymykset. Haastattelussa tehtyjen havaintojen perusteella vielä täydennettiin tuloksissa teorian aiheita. Näin pystyttiin täydentämään teorian teemoja vielä haastatteluaineiston perusteella.

3.-5. Aineiston koodaus, uusien teemojen tunnistaminen, arviointi ja teemojen jalostus

Haastatteluaineisto käytiin ensin kerran kokonaisuudessa läpi. Aineisto käytiin uudelleen läpi vielä teemakohtaisesti. Haastatteluaineisto käytiin läpi kahteen kertaan. Osa haastateltavien vastauksista vastasi suoraan kysyttyyn kysymykseen. Tallaisissa tilanteissa vastauksen analysointi ja kyseisen teeman yhdistäminen oli yksinkertaista. Joissakin tapauksissa vastauksien seasta piti poimia eri teemaan olevia vastauksia. Raportti kirjoitettiin teema kerrallaan.

3. KÄYTTÄJÄHALLINTAA PILVIPALVELUISSA

Tässä luvussa tutustutaan tutkimusaiheeseen teorian avulla. Jotta voidaan ymmärtää, miten moderni käyttäjähallinta toimii nykypäivänä, on ymmärrettävä millaisia järjestelmiä ja ympäristöjä yritykset käyttävät. Ensimmäisenä siis tutustutaan pilvipalveluihin. Kun ollaan tutustuttu pilvipalveluihin, käydään läpi mitä identiteetin ja pääsynhallinta on. Identiteetin ja käyttäjähallinnan jälkeen selvitetään miten käyttäjähallinta vaikuttaa tietoturvallisuuteen. Ensin kuitenkin tutustutaan tietoturvallisuuteen ja kyberturvallisuuteen ja selvitetään mistä osa-alueista ne koostuvat. Sen jälkeen käydään käyttäjähallinnan roolia kyberturvallisuudessa. Viimeisenä esitellään käyttäjähallinnan automatisoinnin hyötyjä.

Kyberrikollisuuden lisäännyttyä tietomurrot voivat koitua erittäin kalliiksi organisaatiolle ja vahingoittaa organisaation imagoa. Käyttäjien pääsyn seuraaminen identiteetinhallinnan avulla on olennainen vaihe turvallisen tietoturvasuunnitelman kehittämisessä. Identiteetin hallinta on prosessi, jolla varmistetaan, että asianmukaisilla henkilöillä on pääsy asianmukaisiin resursseihin organisaation sisällä. Tämä edellyttää, että henkilöllä on tarvittavat oikeudet yrityksen tietoihin, mutta vain oikeudet, jotka ovat tarpeen työtehtävien suorittamiseen. Tarvitaan menettelyjä käyttäjän todentamiseksi, millä varmistetaan käyttäjän olevan sama identiteetti, mikä se väittää olevan. (Mohammed 2017)

Lin et al. (2010) tiivistivät pilvisovellusten käyttäjähallintajärjestelmän tavoitteet. Tavoitteita ovat yksinkertaisuus, luottamuksellisuus ja skaalautuvuus. Yksinkertaisuudella haluttiin, että käyttäjähallintajärjestelmää on helppo käyttää niin kehittäjien kuin käyttäjienkin. Identiteetin hallinta on yksinkertainen, edullinen ja nopea tapa lisätä turvallisuutta (Mohammed 2017).

Pilvipalvelut ovat korvaamassa paikalliset tietojenkäsittely mallit (On-premises), jotka toimivat yrityksen omilla tietokoneilla. Nämä paikalliset tietojenkäsittely mallit toimivat 1960-luvulta aina 1990-luvulle asti, kunnes pilvipalvelut yleistyivät. Pilvipalvelut tarjoavat yrityksille mahdollisuuden käyttää sovelluksia suoraan verkkoselaimella. (Hugos & Hulitzky 2010) Paikallinen malli koostuu ohjelmistoista, jotka on ladattu organisaation omistamalle fyysiselle laitteelle. Paikalliset resurssit tarjoavat rajallisen tallennus- ja käyttökapasiteetin, minkä takia organisaatioiden on harkittava tapaa, jolla resursseja halutaan käyttää ja kuinka kauan. Usein tästä seuraa ali- tai ylikulutusta ja rajoittaa samalla esimerkiksi sovellusten, tietokantojen ja tallennustilan käyttöä. Paikallisessa mallissa yritys hallinnoi ja ylläpitää kaiken infrastruktuurista sovelluksiin. (Torres-Corral 2021) Seuraavaksi tutustutaan mitä ovat pilvipalvelut.

3.1 Pilvipalvelut

Vuonna 1985 ARAPNET määrittelin silloisen pilven tarkoittamaan, tietokoneiden yhdistämistä (Miyachi 2018). Sana ”pilvi” pilvipalvelussa tarkoittaa laitteistoja ja ohjelmistoja, joita käyttäjä käyttää ilman, että tarvitsee tietää tarkalleen missä kyseinen laitteisto ja ohjelmisto fyysisesti sijaitsee (Hugos & Hulitzky 2010). Microsoft, Google ja Amazon ovat kehittäneet suosituimpia pilvialustoja. Asiakkaan tarvitsee vain tehdä tilaus ja hankkia oikeudet, minkä jälkeen pystyy käyttämään ja hallinnoimaan useita pilvialustan palveluita. (Fisher 2018)

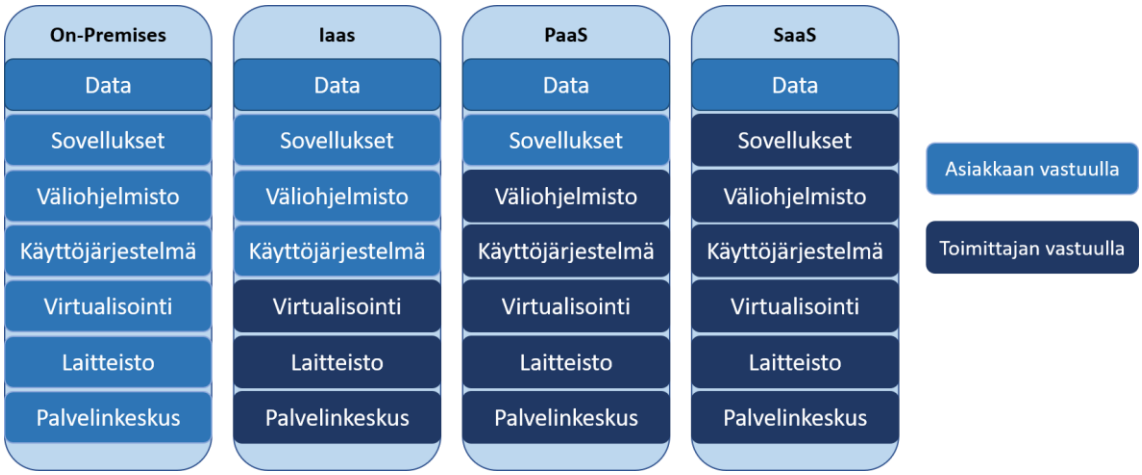
Jotta voidaan ymmärtää pilvipalvelu, on ensin ymmärrettävä mitä palvelu pitää sisällään. Palvelun ymmärtämiseksi Wright (2019) esitti hyvän esimerkin. Microsoftin Word-ohjelmiston on voinut ostaa ja ladata koneelle. Ohjelmiston avulla pystyy luomaan ja muokkaamaan asiakirjoja. Asiakirjat pystyttiin tallentamaan omalle koneelle. Jotta Wordista sai uusimman version käyttöön, oli ladattava versio omalle koneelle. Word on kuitenkin nykyään saatavilla palveluna, jota voi käyttää suoraan selaimessa. Palvelua käytettäessä asiakkaan ei tarvitse ladata mitään ohjelmistoa omalle koneelle. Asiakkaan data säilytetään pilvipalvelussa, eikä asiakkaan koneella. Asiakas maksaa vain käytön verran Wordista eikä joudu ostamaan tuotetta. Tällöin Word on palvelu eikä tuote.

Pilvipalveluissa on paljon hyötyjä, minkä takia monet yritykset ovatkin siirtyneet niiden käyttöön. Pilvipalveluiden etuna on skaalautuvuus. Asiakas voi käyttää juuri sen verran palvelua kuin tarvitsee ja maksaa ainoastaan käyttönsä verran palvelusta. Palvelusta ja sen kuluista on helppo päästä eroon, kun sitä ei enää tarvitse. Pilvipalvelut ovat joustavampia, koska niitä pystyy käyttämään missä vain, kunhan on internet yhteys. Palvelusta on aina käytettävissä uusin versio ilman, että sitä täytyisi ensin ladata tai asentaa omalle koneelle. Palveluntuottajat saattavat panostaa enemmän palveluihinsa tuotteiden sijaan, minkä takia palveluissa saattaa olla enemmän ominaisuuksia. (Wright 2019)

Pilvipalvelut eivät sisällä enää pelkästään ohjelmistotoimitusta. Pilvipalvelut on jaettu kolmeen eri tyyppiin sen mukaan, mitä ominaisuuksia palvelu sisältää. (Hugos & Hulitzky 2010) Kuvassa 2 on esitelty pilvipalvelu tyyppien ominaisuudet ja verrattu niitä keskenään ja perinteisen palvelun kanssa.

Infrastructure-as-a-service (IaaS) palvelussa pilvipalvelun toimittaja vuokraa ainoastaan infrastruktuurin asiakkaan käyttöön (Hugos & Hulitzky 2010). Infrastruktuuri sisältää muun muassa palvelimet ja tallennustilan, verkot, tietoturva ja datakeskuksen (Wright 2019). Yrityksen ei tarvitse omistaa tai ylläpitää konesaliympäristöä itse, koska palveluntarjoaja ylläpitää sen (Hugos & Hulitzky 2010). Koska palveluntarjoaja tarjoaa ainoastaan

pilvi-infrastruktuurin asiakkaalle, täytyy asiakkaan itse hallinnoida ja ylläpitää käyttöjärjestelmät ja käytössä olevat sovellukset. Asiakas pystyy päättämään käytettävät ohjelmistot, jotka voivat olla käyttöjärjestelmiä ja sovelluksia. (Miyachi 2018) Ulkoistamalla infrastruktuurin palveluntarjoajalle, yritykset pääsevät eroon omasta infrastruktuurista ja laitteiston aiheutuvasta vaivasta (Wright 2019). Microsoftin virtuaalikone on hyvä esimerkki IaaS-palvelusta (Microsoft 2022f). Asiakas saa infrastruktuurin, jossa voi esimerkiksi kehittää omia sovelluksia. IaaS on hyvä vaihtoehto, kun halutaan ainoastaan infrastruktuuri sovellusten tai järjestelmien kehittämistä varten (Rani & Ranja 2014).



Kuva 2 Pilvipalvelu tyypit (mukaillen Mokych ja Semeniak, 2020)

Platform-as-a-service (PaaS) palvelussa pilvipalvelun toimittaja tarjoaa kehitysympäristön, missä asiakas pystyy luomaan ja kehittämään sovelluksia palveluntarjoajan ympäristössä (Hugos & Hulitzky 2010, Wright 2019) ilman, että tarvitsee ylläpitää palvelintilaa, ohjelmointiohjelmistoja ja suojausprotokollia (Wright 2019). Asiakas pystyy luomaan sovelluksia käyttämällä palveluntarjoajan tukemia ohjelmointikieliä, kirjastoja, palveluita ja työkaluja. Asiakkaan ei tarvitse hallita tai ylläpitää taustalla olevaa pilvi-infrastruktuuria, mutta joutuu luomaan ja ylläpitämään käytössä olevia sovelluksia ja mahdollisesti sovellusisännöintiympäristön asetuksia. (Miyachi 2018) Esimerkiksi Microsoftin Power Platformin Power Apps on PaaS-palvelu, koska se antaa työkalut muttei valmista sovellusta (George 2021). Asiakas saa infrastruktuurin ja välijärjestelmän omien sovellusten rakentamiseen. PaaS on hyvä sellaisiin käyttö tapauksiin, joissa käyttäjä haluaa kehittää oman sovelluksen valmiilla työkaluilla eikä halua miettiä sen enempää sovellukseen käytettävästä tallennustilasta (Rani & Ranja 2014).

Software-as-a-service (SaaS) palvelussa pilvipalvelun tarjoaja toimittaa ja ylläpitää sovellusta asiakkaalle (Hugos & Hulitzky 2010). SaaS:ssa ohjelmisto toimitetaan internetin kautta asiakkaalle sen sijaan, että se ladattaisiin yksittäiselle laitteelle (Wright 2019).

Asiakas pääsee käyttämään valmiita sovelluksia, jotka toimivat palveluntarjoajan pilvi-infrastruktuurissa. Asiakkaan ei tarvitse hallita tai ylläpitää taustalla olevaa pilvi-infrastruktuuria. Verkko, palvelimet, käyttöjärjestelmät, tallennustila ja jopa yksittäisen sovelluksen ominaisuudet ovat palveluntarjoajan vastuulla hoitaa ja ylläpitää. (Miyachi 2018) Asiakkaan tarvitsee vain kirjautua sisään sovellukseen tai selaimeen ja käyttää ohjelmistoa. Ohjelmisto on käytettävissä mistä tahansa, millä tahansa laitteella, ja tiedot varmuuskopioidaan aina keskitettyyn paikkaan. Microsoftin Outlook on esimerkiksi SaaS-palvelu. (Wright 2019) Outlook on käyttöä vaille valmis sovellus, jota asiakas pystyy käyttämään ylläpitämättä mitään. SaaS on hyvä ratkaisu sellaisessa tapauksessa, kun tarvitaan valmis palvelu käytettäväksi. SaaS ei vaadi asennusta, ainoastaan selaimen ja sitä voidaan räätälöidä asiakkaan tarpeen mukaan siinä määrin kuin se on suunniteltu ennalta määritettyjen konfigurointivaihtoehtojen perusteella (Rani & Ranja 2014).

3.2 Identity and Access Management

Identiteetin ja pääsynhallinnalla (IAM) valvotaan, kenellä on pääsy kriittiseen tietoon. Jotta voidaan ylläpitää asianmukaisia kyberturvallisuuskäytäntöjä, on erittäin tärkeää valvoa, kenellä on pääsy suojattuun tietoon. (Mohammed, 2019b) Jotta tiedot voidaan salata, on ensin tunnistettava salattavat tiedot ja sen jälkeen ylläpitäjät voivat antaa tarvittavat käyttöoikeudet (Mohammed 2017). Käyttäjien käyttöoikeuksien hallinta on järjestelmien ja tietojen oikeuksien kontrollointia. Käyttäjien käyttöoikeuksien hallintaan liittyvät prosessit ja kontrollit ovat ensisijainen huolenaihe. Käyttäjien käyttöoikeusvalvonta on ensimmäinen puolustuslinja luvattomalta pääsyltä eri osiin. (Lee & Sawyer 2019) IAM prosessi sisältää muutakin kuin pelkän käyttöoikeuksien hallinnan. Identiteetin ja pääsynhallinta prosessiin kuuluu keskitetyt hakemistot, pääsynhallinta, identiteetinhallinta, roolipohjainen pääsynvalvonta, käyttöoikeuksien sertifikaatit, ylläpitäjäkäyttäjien ja käyttöoikeuksien hallinta, tehtävien erottaminen sekä identiteetin- ja käyttöoikeusraportointi (CSA 2012).

AbidHussain ja Praveen Kumar Sharma (2020) mukaan pääsynhallinnassa tulisi huolehtia kuudesta eri komponentista, jotta voidaan toteuttaa turvallinen työympäristö pilvipalveluissa. Ensimmäisenä on käyttäjän identiteetti, sen todennus ja valtuutuspalvelut. Nämä palvelut mahdollistavat ulkoistamisen käyttäjien todentamisesta useille eri identiteetintarjoajille. Toisena on monivaiheinen todennus, mikä vähentää riskiä joutua identiteettivarkauden kohteeksi. Kolmantena on hakemistopalvelut, jotka hallinnoivat käyttäjäprofiileja ja niihin liittyviä valtuustietoja, joita käytetään sovellusten käyttöön. Neljäntenä raportointi, mikä tarjoaa käyttäjäkeskeistä tietoa resurssien käytöstä tai resurssikeskeisen näkymän käyttäjien pääsystä. Viidentenä on tarkastus ja vaatimustenmukaisuus,

mitkä vahtivat säädöksien toteutumista ja raportoi poikkeamista. Säädökset voivat olla muun muassa turvallisuuspolitiikkaan, toimialan vaatimustenmukaisuuteen ja riskipolitiikkaan liittyviä vaatimuksia. Viimeisenä on käyttäjien käyttöoikeuksien hallinta, mikä mahdollistaa pilvipalvelujen tarjoajien hallita käyttäjien identiteettejä pilvipohjaisissa alustoissa, sovelluksissa ja palveluissa. (AbidHussain & Praveen Kumar Sharma 2020)

AbidHussain ja Praveen Kumar Sharman (2020) pääsynhallinnan komponentteja verrattuna CSA (2012) määrittelemiin huomataan, että pääsynhallinta ei ole pelkästään oikeuksien myöntämistä ja rajaamista. Yhteiset komponentit turvallisen pääsynhallinnan takaamiseksi olivat identiteetin hallinta ja siihen liittyvät toimet, keskitetty hakemisto, pääsynhallinta sekä identiteetin- ja käyttöoikeuksienraportointi. Näiden lisäksi muita tärkeitä komponentteja olivat roolipohjainen pääsynvalvonta, käyttöoikeuksien sertifikaatit, ylläpitäjäkäyttäjien ja käyttöoikeuksien hallinta, tehtävien erottaminen, monivaiheinen todennus sekä tarkastus ja vaatimustenmukaisuus.

IAM on käyttäjien roolien, käyttöoikeuksien ja tarpeiden hallintaa (Mohammed 2019). Se käsittelee digitaalisia identiteettejä ja käyttäjien pääsyä organisaation sisällä (Mohammed 2017). Identiteetti on kaiken turvallisuuden perusta (Soh *et al.* 2020). Digitaalinen identiteetti on käyttäjäattribuutti, mikä kuvaa kuka käyttäjä on ja kuinka käyttäjä voi todistaa henkilöllisyytensä ja resurssit mitä hän voi käyttää (Kabiru Hamza et al. 2018). Jokaiselle työntekijälle luodaan digitaalinen identiteetti. Käyttäjän identiteettiä on säilytettävä, päivitettävä ja valvottava koko käyttäjän olemassa olon ajan. (Mohammed 2019)

Identiteetin ja käyttäjähallinta antaa oikeat käyttöoikeudet oikeille käyttäjille oikeaan aikaan ja varmistaa, että käyttäjät ovat niitä, joita he sanovat olevansa autentikoinnin kautta (AbidHussain & Praveen Kumar Sharma 2020). Yrityksen käyttäessä pilvipalveluita, se ei useinkaan ole vastuussa autentikoinnin hallintaprosessista. Suurin osa autentikoinnista tapahtuu pilvessä. (Mohammed 2019) Käyttäjien hallinta pilvipalveluissa ei keskity pelkästään käyttäjien tietojen hallintaan vaan myös yritysorganisaation tietojen hallintaan (AbidHussain & Praveen Kumar Sharma 2020).

Identiteetinhallintajärjestelmä tallentaa tietoja, joiden avulla se tarjoaa valtuutuksen, todentamisen, käyttäjien rekisteröinnin, salasanojen hallinnan, auditoinnin, keskushallinnon ja delegoidun hallinnan. Identiteetti hallintajärjestelmä tallentaa tietoja resursseista, joita voivat olla muun muassa sovellukset, tietokannat, laitteet, tilat, ryhmät, käyttöjärjestelmät, ihmiset, politiikka ja roolit. Järjestelmä tunnistaa ja valtuuttaa sekä sisäiset että ulkoiset käyttäjät. Käyttäjän pyytäessä pääsyä resurssiin, identiteetinhallinta todentaa ensin käyttäjän pyytämällä tunnistetietoja. Tunnistetiedot voivat olla käyttäjänimi ja sala-

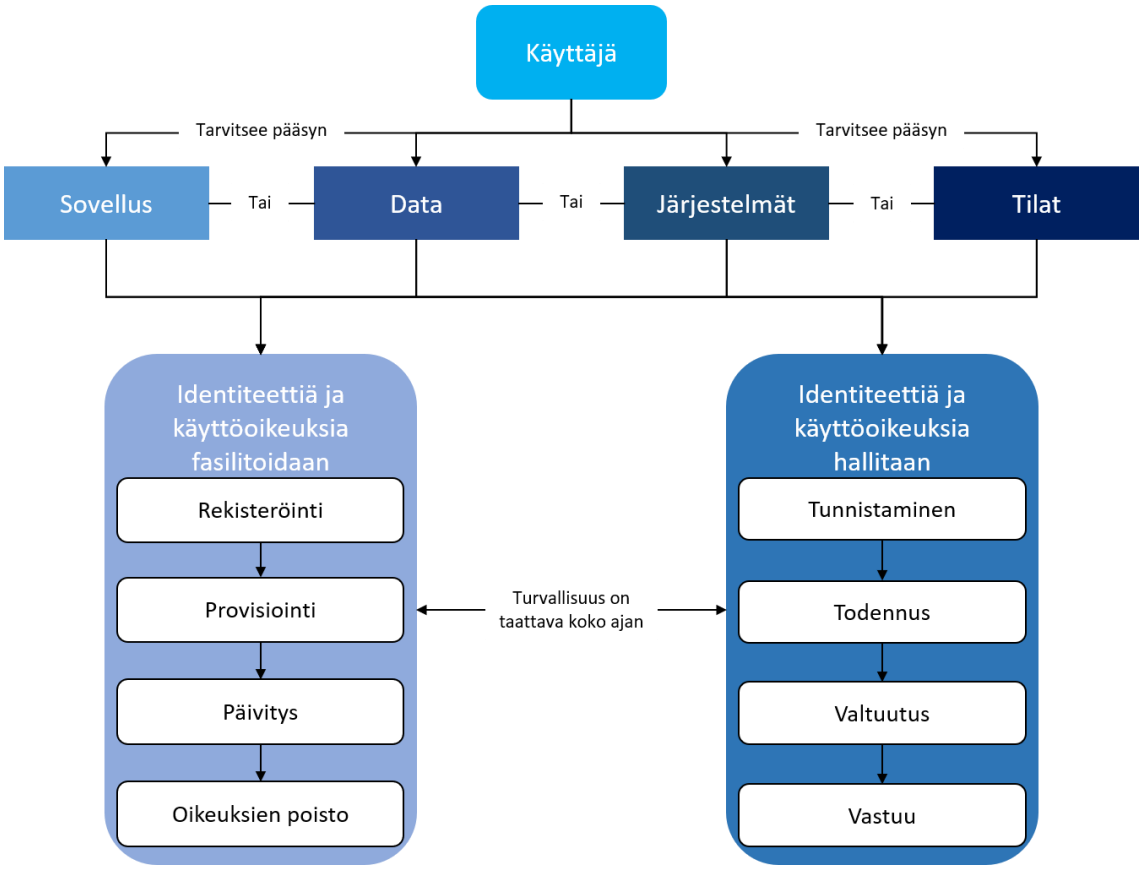
sana, digitaalinen varmenne, älykortti tai biometrisia tietoja. Sen jälkeen käyttäjälle valtuutetaan sopiva määrä käyttöoikeuksia käyttäjän identiteetin ja attribuuttien perusteella. (AbidHussain & Praveen Kumar Sharma 2020)

Ulkoisten käyttäjätilien rekisteröinti onnistuu myös identiteetinhallintajärjestelmään. Käyttäjän rekisteröidyttyä onnistuneesti identiteetinhallintajärjestelmään, hänelle voidaan myöntää pääsy resursseihin. (AbidHussain & Praveen Kumar Sharma 2020) Pilvipohjainen IAM on helpottanut ulkopuolisille käyttäjille käyttöoikeuksien lisäämistä sovelluksiin (Mohammed 2017). Sisäisillä käyttäjillä luodaan työsuhteen alussa jo identiteetti identiteetinhallintajärjestelmään, minkä takia sisäisen käyttäjän ei tarvitse jälkikäteen rekisteröityä. Identiteettihallintajärjestelmä helpottaa käyttäjätietojen tarkistamista. Ylläpitäjät voivat hallita keskitetysti identiteettejä hallintajärjestelmästä. (AbidHussain & Praveen Kumar Sharma 2020)

Säännösten, kuten GDPR, tiukentumisen ja monimutkaistumisen vuoksi yrityksille tehdään entistä enemmän säännösten tarkastuksia, vaatimustenmukaisuustarkastuksia ja vaaditaan raportointia (Mohammed 2017). Seuranta- ja raportointitoimenpiteiden avulla pystytään ennakoimaan ja ennustamaan altistumisia riskeille. Raportit tarjoavat auditoinnissa käytettäviä mittareita. Tarkastuslokit ovat tärkeä osa IAM-prosessia. Sovelluksen tulisi säilyttää toimintalokit, mukaan lukien kaikki todennus- ja pääsy-yritykset, sekä onnistuneet että epäonnistuneet. Prosessien ja tukijärjestelmien pitäisi pystyä tarjoamaan raportteja, jotka sisältävät yksityiskohtaisia käyttöoikeuksia ja tarkastuksia. Sekä datan, että prosessin raportointi on yhtä tärkeää. Tarkastusraportit sisältävät raportteja, joissa käsitellään esimerkiksi käyttäjätunnuksia ja niihin liittyviä käyttöoikeuksia, pääsyjä hyväksymistietoihin, hallinnollisia ja etuoikeutettuja tilejä ja niihin liittyviä omistajia, tietyn resurssin käyttäjämääriä ja niihin liittyviä tilastoja, pääsyhäiriöitä ja etuoikeuskäyttöhäiriöitä. (CSA 2012) Tiedonkeruu, raportointi ja käyttöoikeuksien tarkistus ovat kaikki automatisoitavissa IAM-hallintaratkaisujen avulla. Vaatimustenmukaisuuden auditoinnit tuovat esiin puutteet ja tarjoavat organisaatioille mahdollisuuden korjata haavoittuvuuksia ja ratkaista vaatimustenmukaisuusrikkomukset. (Mohammed 2017)

IAM prosessin kulku on esitettynä kuvassa 3 mukaille Mohammed (2017) alkuperäistä kuvaa. Prosessi alkaa, kun käyttäjällä on tarve päästä sovellukseen, dataan, järjestelmään tai tiloihin käsiksi. Identiteettiä ja pääsyä hallinnoidaan neljän vaiheen avulla. Ensimmäisenä on identiteetin hallinta, jossa luodaan ja poistetaan organisaation sisäisiä käyttäjätilejä. (Yang *et al.* 2014) Mikäli identiteetti on jo olemassa, voidaan suoraan siirtyä identiteetin tunnistamiseen. Kun identiteetti on tunnistettu seuraa identiteetin todennus. (Mohammed 2017) Todennuksessa varmistetaan, että käyttäjä on se, kuka hän väittää olevansa. Todennuksessa käyttäjä tunnistetaan erilaisten mekanismien, kuten

salasanan ja varmenteen avulla. (Yang *et al.* 2014) Todennuksen jälkeen seuraa identiteetin valtuutus (Mohammed 2017). Valtuutus on prosessi, jossa myönnetään käyttöoikeudet tiettyihin resursseihin tietyille identiteetille (Trnka et al. 2018). Varmistuksen jälkeen käyttäjälle myönnetään oikea käyttöoikeus taso (Yang *et al.* 2014). Identiteetin- ja pääsynhallinnoimisessa viimeisenä vaiheena on vastuullisuus. Käyttäjä joutuu toimimaan ennalta sovittujen sääntöjen mukaan käyttäessään järjestelmiä, dataa, sovelluksia tai tiloja. Säännöt koskevat, miten tietoja ja toimintoja järjestelmässä voi käyttää. (Yang *et al.* 2014)



Kuva 3 Identiteetti ja käyttöoikeushallinta prosessi (mukaillen Mohammed 2017)

Identiteettiä ja käyttöoikeuksia fasilitoidaan nelivaiheisella **prosessilla**. Ensimmäisenä on tunnuksen luominen eli rekisteröinti. Toisena vaiheena on provisiointi. (Mohammed 2017) Provisiointi on IT-infrastruktuurin perustamisprosessi, jota tarvitaan tietojen ja resurssien käytön hallitsemiseksi ja niiden saattamiseksi käyttäjien ja järjestelmien saataville (RedHat 2020). Provisiointia tarvitaan, kun uusi henkilö tulee organisaatioon, kun olemassa oleva työntekijä siirtyy toiselle osastolle tai kun olemassa oleva työntekijä lähtee yrityksestä. Kolmantena vaiheena on päivittää käyttäjän tietoja ja oikeuksia niiden muuttuessa. Viimeisenä vaiheena on poistaa käyttäjän oikeudet, kun niitä ei enää tarvita.

Identiteetin- ja käyttöoikeuksien fasilitointi ja hallinta prosesseja tulee toteuttaa samanaikaisesti ja yhdessä. Niitä ei pidä käyttää kahtena erillisenä prosessina vaan yhdessä, jolloin taataan parempi turvallisuus. (Mohammed 2017)

3.3 Käyttäjähallinnan rooli tietoturvassa

Nykypäivän digitaalisessa maailmassa identiteetin- ja pääsynhallinta on tärkeä rooli kaikissa yrityksen tietoturvasuunnitelmissa (Rathod 2019). Pilviverkkopalveluissa on huomattu esiintyvän suuria ongelmia, joita ovat muun muassa kelvollisten käyttäjien tunnistetietojen vahvistaminen, valtuustietojen suojaaminen, tietomurrot, tilin kaappaukset ja irralliset tilit (Kabiru Hamza et al. 2018). Yhä useammat yritykset säilyttävät arkaluontoiset tietonsa sähköisesti, joten tietojen turvallisuuden varmistaminen on erittäin tärkeää (Rathod 2019). On hyvä tarkastella identiteetin- ja pääsynhallinnan roolia tietoturvallisuuteen. Jotta voidaan ymmärtää pääsynhallinnan vaikutus yritysten tietoturvaan, on ymmärrettävä mistä muuttujista tietoturva ja kyberturva rakentuvat ja miten ne eroavat toisistaan.

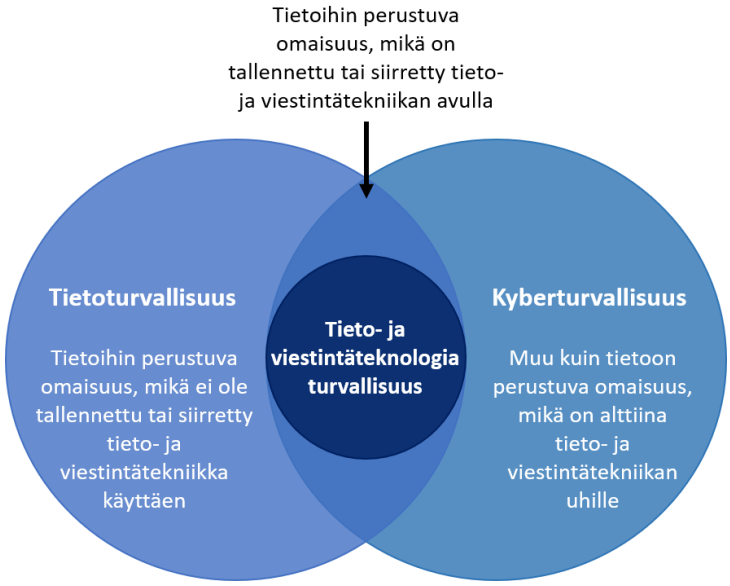
3.3.1 Tietoturvallisuus ja kyberturvallisuus

Tietoturvan tavoitteena on minimoida liiketoiminnan vahingot estämällä tietoturvahäiriöt ja näin varmistaa liiketoiminnan jatkuvuus (ISO/IEC 27002 2005, von Solms & van Niekerk 2013) sekä investointien tuoton ja liiketoimintamahdollisuuksien maksimoiminen (ISO/IEC 27002 2005). Kansainvälinen standardi ISO/IEC 27002 (2005) on määritellyt tietoturvan tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämisenä. Tietoturva ei ole tuote tai teknologia, vaan prosessi (Mitnick ja Simon 2002 lähteessä von Solms & van Niekerk 2013). Tietoturvaprosessissa voidaan käyttää tiettyjä tuotteita, mutta sitä ei voi ostaa pakettina (von Solms & van Niekerk 2013). Tietoturva koskee tietoa sen muodosta riippumatta. Tietoturva kattaa siis paperiasiakirjat, digitaalisen ja henkisen omaisuuden ihmisten mielissä sekä sanallisen tai visuaalisen viestinnän. (von Solms & von Solms 2018)

Kyberturvallisuus ja tietoturvallisuus termeinä usein saattavat sekoittua. Oli sitten kyseessä tietoturvallisuus tai kyberturvallisuus, niin tavoitteena on omaisuuden suojaaminen haavoittuvuuksien aiheuttamilta erilaisilta uhkilta (von Solms & van Niekerk 2013). Von Solms ja von Solms (2018) mukaan kyberturvallisuus on tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämistä kyberavaruudessa. Tämä tarkoittaisi, että kyberturvallisuuden ja tietoturvan ero on, että kyberturvallisuus rajoittuu kyberavaruudessa olevaan tietoon, kun taas tietoturva on tiedon suojaamista "kaikkialla". Kyberturvallisuus on digitaalisten resurssien suojaamista. Digitaalisiin resursseihin sisältyy kaikki verkoista

laitteistoihin ja tietoihin, joita käsitellään, tallennetaan tai siirretään verkkopohjaisissa tietojärjestelmissä. (von Solms & von Solms 2018) Kyberturvallisuus keskittyy siis digitaalisen tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaamiseen kaikilta uhilta (von Solms & von Solms 2018).

Tieto- ja viestintäteknologioiden turvallisuuden tapauksessa suojattava omaisuus on taustalla oleva tietotekniikan infrastruktuuri. Tietoturva puolestaan määrittää suojattavan omaisuuden kattamaan tietotekniikan infrastruktuurin lisäksi tiedon. (von Solms & van Niekerk 2013) Kyberturvallisuuden ja tietoturvallisuuden suhteesta ollaan useaa mieltä, eikä siitä ole yhtä oikeaa määritelmää tehtynä. Kyberturvallisuudessa suojattavaan omaisuuteen kuuluu kuka tahansa tai mikä tahansa, mikä voidaan tavoittaa kyberavaruuden kautta (von Solms & van Niekerk 2013). Von Solms ja von Solms (2018) ovat määrittäneet, että kyberturvallisuus on osa tietoturvaa ja näin ollen sijoittuisi kokonaan tietoturvallisuuden sisälle. Von Solms ja van Niekerk (2013) taas määrittävät, että tietoturvallisuus ja kyberturvallisuus ovat kaksi eri aluetta, joilla on yhteisiä ominaisuuksia. Von Solms ja van Niekerk (2013) määritelmä on esitettynä kuvassa 4.



Kuva 4 Tietoturvallisuuden ja kyberturvallisuuden suhde (mukaillen von Solms & van Niekerk 2013)

Kyberturvallisuus Alhija (2020) mukaan koostuu kyvystä palautua hyökkäyksistä, mobiililaitteista, identiteetin- ja käyttäjähallinnasta, tietoisuudesta, esineiden internetistä sekä pilven, sovellusten, verkon, infrastruktuurin ja tietokannan turvallisuudesta. Naik Bukht *et al.* (2020) olivat sitä miltä, että kyberturvallisuuden pää osa-alueet ovat sovellusten turvallisuus, tietoturvallisuus, sähköpostin turvallisuus, mobiilitaitteiden ja webin turvalli-

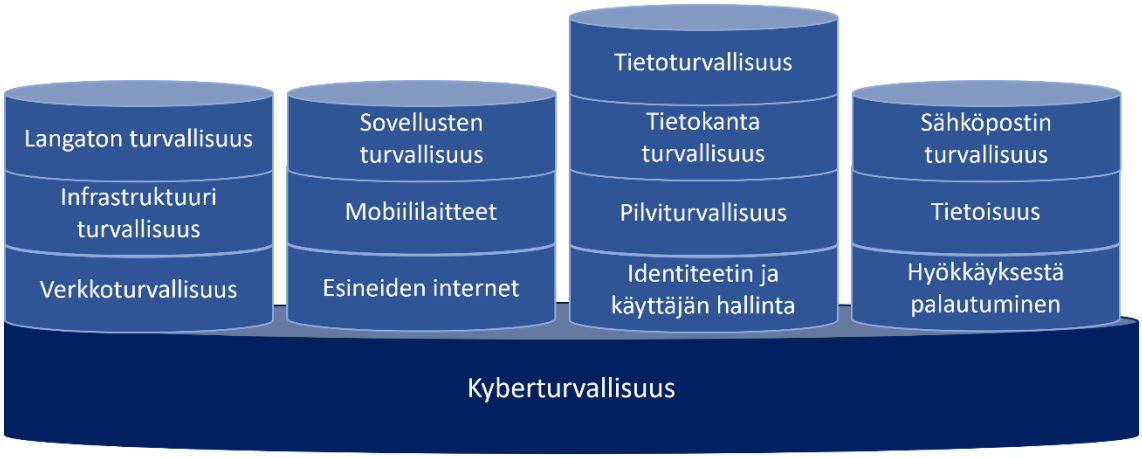
suus sekä verkkoturvallisuus. Alhija (2020) ja Naik Bukht *et al.* (2020) kyberturvallisuuden osa-alueet on esitetty kuvassa 5. Jotta voidaan ymmärtää käyttäjähallinnan vaikutus kyberturvallisuuteen, on ymmärrettävä mistä kyberturvallisuus koostuu. Seuraavaksi käydään tarkemmin kyberturvallisuuden osa-alueet läpi.

Verkkoturvallisuus suojaa pääsyä verkkosivustolle tai pilveen. Nykyään on syytä valikoida mitkä laitteet pääsevät käyttämään verkkoa. (Naik Bukht *et al.* 2020) Verkkoturvallisuudessa vartioidaan ulkopuolelta tulevaa luvatonta tunkeutumista sekä sisäpuolelta ilmenevää haitallista käytöstä. Verkkoturvallisuudessa suojataan verkkokomponentteja, verkkoihin liittyminen ja verkkoon liittyvä sisältö. Verkkoturvallisuus rakentuu kerroksista, jotka koostuvat useammasta kuin yhdestä verkkoon kuuluvasta komponentista, tietoturvaohjelmistoista ja -laitteistoista. Komponenttien toimiessa yhdessä voidaan parantaa verkon yleistä turvallisuutta ja suorituskykyä. Jotta voidaan varmistaa verkon turvallisuus, voidaan joutua tekemää kompromisseja. Esimerkiksi pääsynhallinnassa ylimääräiset kirjautumiset saattavat olla tarpeen, mutta se hidastaa tuottavuutta. (Alhija 2020) Tukiaseman kautta voi olla pääsy langattomaan verkkoon. Kiinteä verkko on turvallisempi kuin langaton verkko. Langattoman verkon tietoturva on yleistyvä ongelma. Tarvitaan tuotteita, jotka on suunniteltu erityisesti suojaamaan langatonta verkkoa. (Naik Bukht *et al.* 2020)

Tyypillisiä infrastruktuurisektoreita ovat terveys-, vesi-, liikenne-, viestintä-, hallinto-, energia-, elintarvike-, rahoitus- ja hätäpalvelut. Kaikki kriittisen infrastruktuurin sektorit ovat riippuvaisia fyysisestä infrastruktuurista, kuten rakennuksista, teistä, tehtaista ja putkista. Yhä useammin myös kriittiset sektorit luottavat kyberavaruuteen ja sen mahdollistaviin tieto- ja viestintätekniikoihin. Luottamuksen puute tieto- ja viestintätekniikoiden käyttöön voi haitata jokapäiväistä elämää, kauppaa ja kansallista turvallisuutta. Elektroninen turvallisuus on yhtä tärkeää kuin fyysinen turvallisuus kriittisten kyberresurssien toiminnan jatkuvuuden takaamiseksi. (Alhija 2020)

Tietokannan turvallisuuteen vaikuttaa muun muassa tietokannan luvattoman käytön rajoittaminen, mutta myös palvelimen ja varmuuskopiointilaitteiden fyysinen suojaus varkauden tai vahingoittumisen varalta. Joitakin hyviä käytäntöjä ovat vahva ja monivaiheinen tunnistautuminen, jolloin voidaan hallita paremmin, kenellä on pääsy tietoihin, sekä tunnettujen haavoittuvuuksien tarkistaminen ja kartoittaminen. Tietokanta kannattaa myös kuormitus- ja stressitestata, jotta voidaan olla varmoja, ettei se kaadu palvelunestohyökkäyksen (DDoS) tai käyttäjien ylikuormituksen takia. Organisaatioiden tulee aina pyrkiä jakamaan vähimmäismäärä oikeuksia, jotka tarvitaan heidän työnsä suorittamiseen. (Alhija 2020)

Naik Bukht *et al.* (2020) määritteli tietoturvan olevan joukko tekniikoita prosessien ja työkalujen hallintaan, joita tarvitaan ehkäisemään ja käsittelemään uhkia, jotka kohdistuvat digitaalisiin ja muihin asiakirjoihin. Tietoturva perustuu tietojärjestelmien eheyden, luottamuksellisuuden ja käytettävyyden sekä tiedon alkuperäisyyden säilyttämiseen. Luottamuksellisuudella tarkoitetaan, että luottamukselliset tiedot ovat luovutettava valtuutetuille tapahtumille. Eheys estää tietojen luvattoman muuttamisen. Käytettävyys varmistaa, että tietoihin pääsee käsiksi oikeat osapuolet.



Kuva 5 Kyberturvallisuuden pääalueet (mukaillen Alhija 2020 ja)

Sovellukset voivat sisältää aukkoja tai haavoittuvuuksia. Aukkojen ja haavoittuvuuksien avulla hyökkääjät voivat tunkeutua ohjelmistoihin. Sovellusturvallisuus tarkoittaa laitteiston, ohjelmiston ja menetelmien käytön turvaamista ulkoisilta hyökkääjiltä. (Naik Bukht *et al.* 2020) Sovellusten turvallisuus riippuu paljon, siitä miten turvallisesti se säilyttää ja käyttää tietoja. Siihen vaikuttaa paljon, kuinka hyvin ohjelmisto on suunniteltu, toteutettu, testattu, otettu käyttöön ja ylläpidetty. Jotkut sovellukset ovat alttiimpia uhille kuin toiset. Dokumentaatio on kriittisen tärkeä, jotta kaikki ymmärtävät nämä näkökohdat, ja eettisiä näkökohtia nousevat esiin koko ohjelmiston luomisen, käyttöönoton, käytön ja käytöstä poistamisen aikana. (Alhija 2020)

Kyberrikolliset keskittyvät yhä enemmän mobiililaitteisiin ja sovelluksiin. (Naik Bukht *et al.* 2020) Yli 60 % verkkopetoksista tapahtuu mobiilialustojen kautta, ja 80 % mobiilipetoksista tapahtuu mobiilisovellusten avulla mobiiliverkkoselaimien sijaan. Vähäisen tietoisuuden takia käyttäjät saattavat tietämättään ostaa viruksellisia laitteita, joutua mobiililaitteen kaappauksen uhriksi tai kadottaa laitteensa. (Alhija 2020)

Esineiden Internetin (IoT) turvallisuushaasteiden ja -uhkien tunnistamiseksi tulisi tunnistaa käytössä olevat laiteet ja IoT-laitteiden kohtaamien mahdolliset uhat, hyökkäykset ja

haavoittuvuudet ja dokumentoida ne hyvin. IoT-laitteiden turvallisuuden takaamiseksi tulisi tuotekehityksen varhaisessa vaiheessa panostaa kulunvalvontaan, autentikointiin, identiteetinhallintaan ja joustavaan luottamuksenhallintaan. (Alhija 2020)

Yrityksen siirtyminen pilveen luo uusia tietoturvahaasteita. Ulkoistaminen voi helpottaa turvallisuuden toteuttamista, mutta se keskittää pilvipalvelut erittäin kannattaviksi hyökkäyskohteiksi. Pilvipalveluiden pääongelma on, että se on kolmannen osapuolen toteuttama. Monilla on mielikuva, että heidän tietonsa eivät ole yhtä hyvin turvattu, kun tietoja isännöivän palvelimen fyysinen käyttöoikeus on menetetty. Pilvitietojen suojaus ei ole vain salausta, vaan myös pääsyoikeuksia. Pilvipalveluntarjoajat luovat jatkuvasti uusia tietoturvatyökaluja auttaakseen yrityskäyttäjiä suojaamaan tietonsa paremmin. (Alhija 2020)

Tietämättömyyden vuoksi työntekijät saattavat päästää vahingossa hyökkääjät suojauksen läpi. Tietoturvatietoisuus on tärkeää kyberhyökkäysten estämiseksi. Tietoisuus kyberturvallisuudesta edistää ymmärrystä kyberuhkista ja -riskeistä ja asianmukaisista reagointivaihtoehdoista. Tietoisuuden lisääminen parantaa työntekijöiden oikealaista reagoimista kohdatessaan riskejä. Työntekijöiden kouluttamisella voidaan tarkistaa ja testata, että työntekijät noudattavat heille annettuja ohjeita. (Alhija 2020) Hakkeroimalla sähköpostin hakkerit voivat helposti päästä käsiksi henkilön sähköpostiosoitteeseen ja sitten käyttää sitä negatiivisiin tarkoituksiin. Henkilökohtaisia tietoja käyttämällä hyökkääjät luovat kehittyneitä tietojenkalasteluprosesseja, jotka huijaavat vastaanottajia ja lähettävät heidät sivustoille, jotka määrittävät haittaohjelmia. Sähköpostin suojaussovellus voi estää saapuvat virukset, hyökkäykset ja viestejä valvomalla estää yksityisten tietojen varastamisen. (Naik Bukht *et al.* 2020)

Vaikka suunniteltaisiin ja toteutettaisiin kaikki toimenpiteet turvallisesti, voi hyökkäys silti onnistua ja päästä suojauksesta läpi. Hyökkäyksestä palautuminen ja organisaation toiminnan jatkuminen riippuu kyvystä replikoida IT-järjestelmiä ja dataa. Yrityksen kyky toipua katastrofista riippuu suoraan ennen katastrofia suoritetun liiketoiminnan jatkuvuuden suunnittelun tasosta. Jatkuvalla testauksella ja suunnitelmien parantamisella pystytään pitämään strateginen suunnittelu liiketoiminnan kehityksessä mukana. (Alhija 2020) On hyvä idea tutkia, mitkä korjaustiedostot sopivat yrityksen käyttöön. Korjaustiedosto on joukko muutoksia, jotka on suunniteltu korjaamaan tietoturva-aukkoja ja parantamaan käytettävyyttä ja suorituskykyä. Tiedostamalla sopivat korjaustiedostot voidaan välttää tietoturvariskejä, jotka johtuvat hyökkääjistä, jotka ovat valmiita käyttämään yrityksen haavoittuvuuksia. (DNSstuff 2019)

Alhija (2020) oli määritellyt käyttäjähallinnan omaksi kyberturvallisuuden pääalueeksi. Käyttäjähallinta ei ole yksi erillinen tehtävä, vaan se vaikuttaa kaikkeen turvallisuudessa, kuten edellä esiteltyjen kyberturvallisuuden pääalueiden esittelystä voi huomata. Turvallisesta tietokannasta, sovelluksista tai pilvipalveluista ei ole hyötyä, mikäli käyttäjähallinta on laiminlyöty. Koska identiteetin- ja pääsynhallinta on todella iso osa kyberturvallisuutta ja tämän työn aihe, on se käsitelty erillisenä alalukuna. Seuraavassa alaluvussa käydään läpi käyttäjähallinnan roolia kyberturvallisuudessa.

3.3.2 Käyttäjähallinta osana kyberturvallisuutta

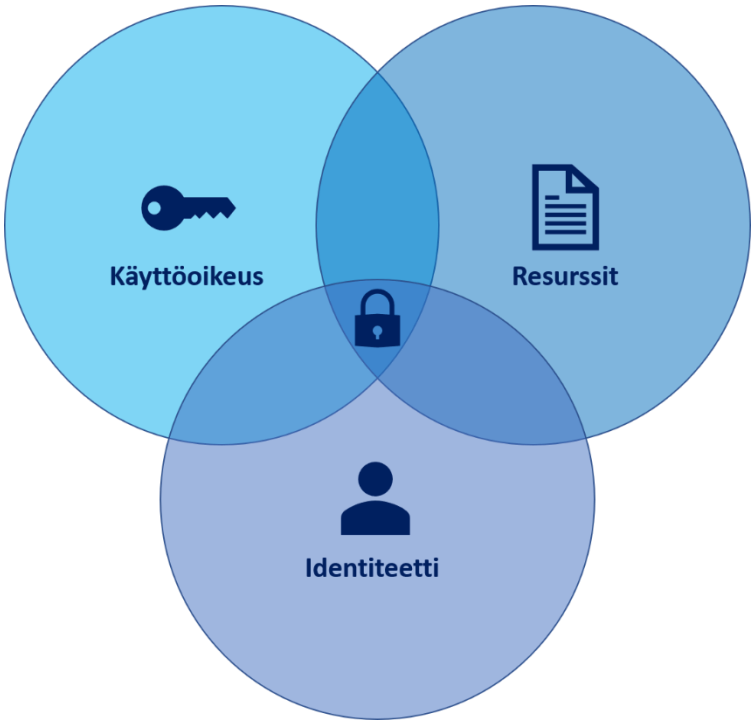
Pilvipalvelun myötä käyttöoikeuksien hallinnan tarve on kasvanut. Pilvipalveluiden takia käyttäjien ei tarvitse olla fyysisesti työpaikalla päästäkseen järjestelmiin. (Lee & Sawyer 2019) Identiteetti ja käyttöoikeuksien hallinta on vaikuttava tekijä pilven käytön (Yang *et al.* 2014) ja organisaation tietoturvajärjestelmää (Mohammed 2017). Identiteetin käyttöoikeuksien hallinta on yksi tärkeimmistä osista tietoturvan ylläpitämisessä pilvessä (Mohammed 2019).

IAM-projektien rahoittaminen organisaatioissa ei aina ole etusijalla, sillä ne eivät suoraan lisää kannattavuutta tai toimivuutta. Identiteetin- ja pääsynhallinta vastaa kuitenkin kriittiseen vaatimukseen varmistaa asianmukainen pääsy resursseihin. (Alhija 2020) Yritykset kohtaavat nykypäivänä erilaisia hallinnollisia vaikeuksia, tietosuojasäädöksiä, valvontaongelmia ja säännösten noudattamista. Identiteetinhallinnan avulla voidaan parantaa toimintaprosesseja, parantaa raportointikykyä ja varmistaa säännösten noudattaminen. (Mohammed 2017)

Haber ja Rolls (2019) mukaan kyberturvallisuuden pääpilarit muodostuvat, kun tunnetaan resurssit, käyttöoikeudet ja identiteetit. Kyberturvallisuuden pääpilarit ovat esitettynä kuvassa 6. Kyberturvallisuuden takaamiseksi tavoitteena on varmistaa, että ihmisillä on asianmukainen pääsy resursseihin, organisaatio tietää aina, kenellä on pääsy mihinkin, miten pääsyä voidaan käyttää ja onko pääsy käytäntöjen mukainen. Identiteetinhallinta on tekniikka ja prosessi, jolla voidaan varmistaa edellä mainitun tavoitteen toteutuminen (Haber & Rolls 2019). Se on käytäntöihin perustuvaa käyttäjien identiteetinhallinnan ja kulunvalvonnan organisointia (Shea 2014). Identiteetinhallinta on kriittinen osa yritysten tietotekniikan automatisointia, tietoturvaa ja vaatimustenmukaisuuksien hallintaa (Haber & Rolls 2019).

Käyttöoikeuksien hallinnassa ongelmia on aiheuttanut muun muassa käyttäjän luominen ja poistaminen, yhdellä tunnuksella pärjääminen, vaatimustenmukaisuuden näkyvyys, kolmannen osapuolen tai toimittajaverkoston suojaus ja salasanan uudelleenkäyttö.

Käyttäjän onboarding ja offboarding prosessin toteuttaminen turvallisesti ja oikea-aikaisesti on ollut haasteellista. (AbidHussain & Praveen Kumar Sharma 2020) Käyttäjien käyttöoikeuksien rajaamisen tavoitteena on vähentää järjestelmien luvatonta tai sopimatonta käyttöä. Säännöllisen käyttäjien tarkastelun avulla voidaan löytää työntekijöitä, jotka ovat lähteneet organisaatiosta tai siirtyneet toisiin tehtäviin, mutta joilla on edelleen pääsy resursseihin. Ongelmana on myös menettelyjen puute tai nykyisten menettelyjen tehottomuus, kun työntekijöiden asema organisaatiossa muuttuu. (Lee & Sawyer 2019)

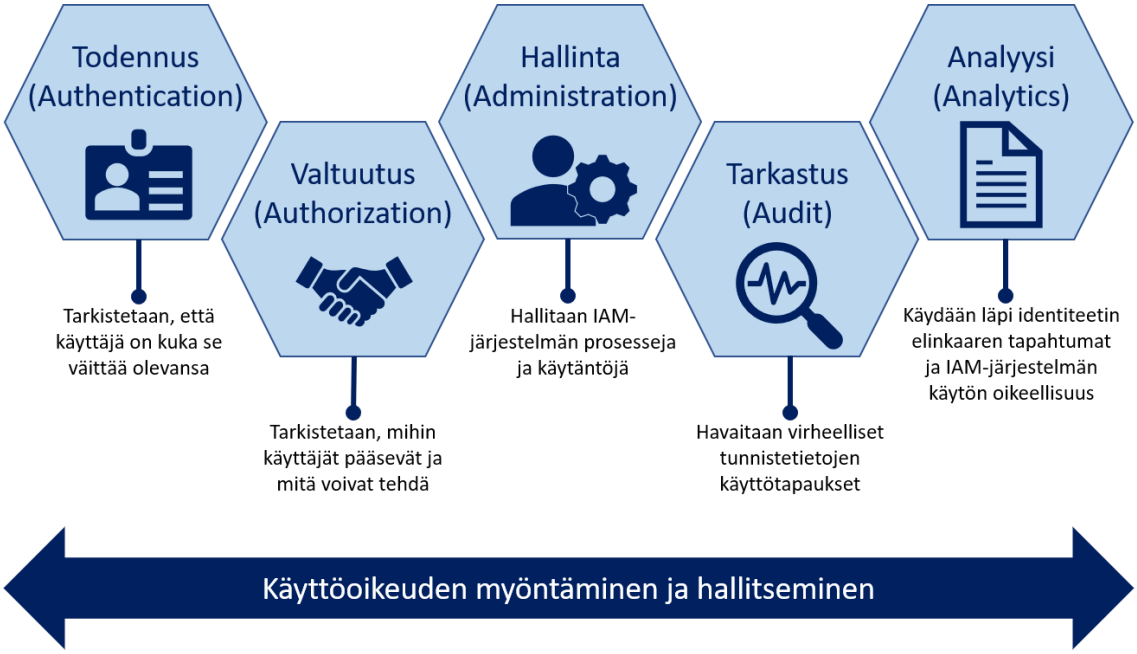


Kuva 6 Kyberturvallisuuden kolme pääpilaria (mukaillen Haber & Rolls 2019)

Organisaatioiden on vaikea seurata erilaisia kirjautumistunnuksia, joita työntekijät ylläpitävät työsuhteensa aikana. Käyttöoikeuksien hallinnassa ongelmia saattaa aiheuttaa vaikeus selvittää kenellä on pääsy mihinkin. Olisi tärkeää tietää, kenellä on pääsy sovelluksiin ja tietoihin, missä he käyttävät niitä ja mitä he tekevät niillä. (AbidHussain & Praveen Kumar Sharma 2020) On tärkeää käydä läpi säännöllisesti, keillä työntekijöillä on pääsy ja luvat mihin resursseihin. Etuoikeuden sääntö määrittää, että on tärkeää myöntää kaikille käyttäjätileille vähimmäistaso käyttöoikeuksia annettaessa, mikä tarvitaan määrättyjen tehtävien suorittamiseen. (DNSstuff 2019) Tietoturvan kannalta olennaista on säännellä, mitä tietty käyttäjä tarvitsee käyttöoikeuksien suhteen. Ihanteellisessa tilanteessa henkilö saa valtuutuksen ja näkee vain sen, mitä hänelle on myönnetty luparyhmien hallinnon kautta. (Mohammed 2017) Tarkoituksena on vähentää mahdollisia riski-

tekijöitä rajoittamalla ylimääräisiä oikeuksia (DNSstuff 2019). Hyvä keino on erotella tiimin tehtävät, jolloin pystytään helpommin myöntämään käyttäjille vain sen verran käyttöoikeuksia, mitä he tarvitsevat työnsä suorittamiseen (Microsoft 2022b).

Haber ja Rolls (2019) kehittivät tietoturvakehyksen identiteetinhallinnalle nimeltä ” The Five A’s of Enterprise IAM”. Viisi A:ta koostuu todennuksesta (Authentication), valtuutuksesta (Authorization), hallinnasta (Administration), tarkastuksesta (Audit) ja analytiikasta (Analytics). Kun viisi A:ta on hallinnassa, on identiteetinhallinnan toteuttaminen helpompaa ja turvallisempaa. Kuvassa 7 on esitelty nämä viisi osaa.



Kuva 7 Viisi A:ta identiteetinhallinnassa (mukaillen Haber & Rolls 2019)

Todennus ja valtuutus sekoitetaan usein keskenään. Ne kuitenkin ovat eri tekniikoita. Todennuksella vahvistetaan, onko käyttäjä se, kuka sanoo olevansa. Henkilöllisyys usein todennetaan käyttäjätunnuksella ja salasanalla, mutta voidaan käyttää myös esimerkiksi pin-koodia, avaimia, kaksivaiheista todennusta. Todennus ei anna käyttöoikeuksia tai etuoikeuksia, se vain vahvistaa, että käyttäjä on se, joka väittää olevansa. (Haber & Rolls 2019)

Valtuutus on seuraava vaihe todennuksen jälkeen. Käyttäjälle ei voida valtuuttaa minkään näköisiä oikeuksia ilman todennusta. Valtuutus antaa oikeudet suorittaa toiminto, mikä perustuu todentamiseen. Käyttäjä saa henkilöllisyytensä perusteella tietyt oikeudet tiettyjen toimintojen suorittamiseen. Käyttäjältä voidaan myös evätä oikeuksia henkilöllisyytensä perusteella. (Haber & Rolls 2019)

IAM prosessin yhteydessä halutaan hallita todentamisen, valtuutuksien ja auditointien muutoksia. Identiteetinhallinnan tehtävä on keskittää hallintaominaisuuksien tarjoaminen

kaikille pääsyjärjestelmille. IAM:n hallinta on suuri osa identiteetinhallinnan tehtäviä. Kun hyödynnetään identiteetinhallinnan prosesseja, hallinta voi tarjota näkyvyyttä, ohjausta, automaatiota ja täyden elinkaarihallinnan kaikille käyttäjille ja heidän käyttöoikeuksilleen. (Haber & Rolls 2019)

Tarkastus-prosessi on identiteetinhallinta prosessin vastuulla. Tarkastus on tärkeä osa identiteetinhallintajärjestelmää. Tarkastus prosessi voi olla käyttäjien pääsyn varmentamisohjelma, määritellä ja toteuttaa ennaltaehkäisevää ja etsivää politiikkaa tai todistaa hallintoprosessien ja -käytäntöjen määritelmät, käytössä olo ja niiden noudattaminen. (Haber & Rolls 2019)

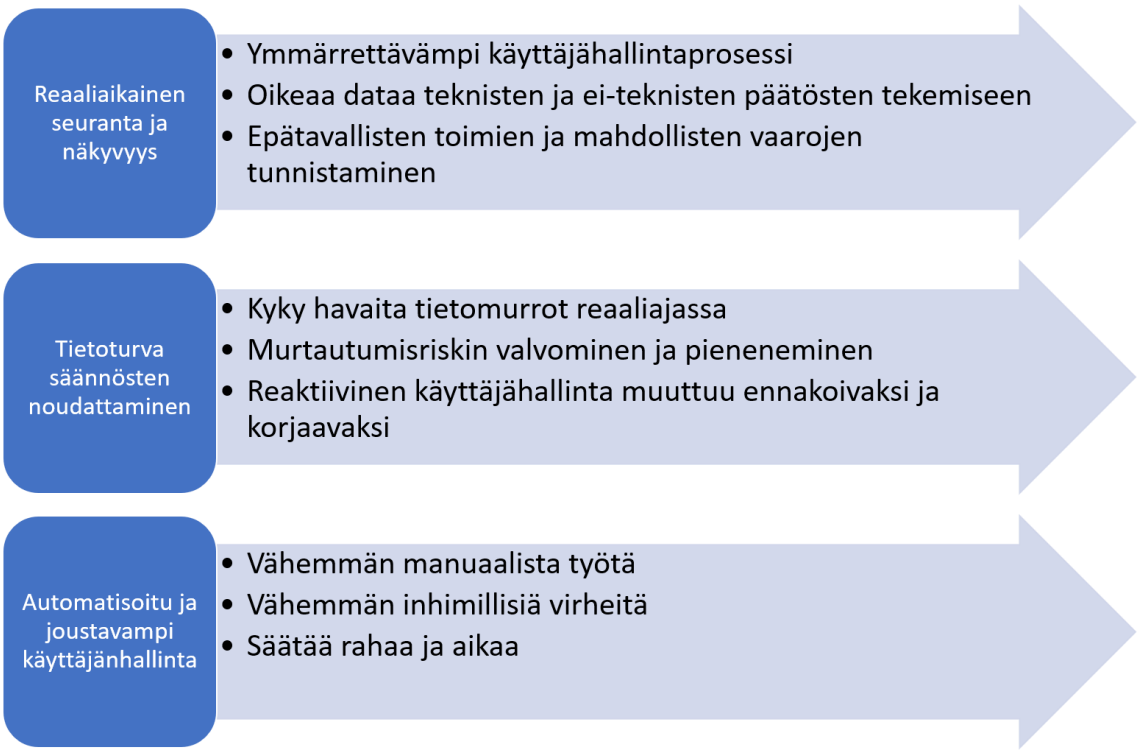
Kattava analyysi IAM-järjestelmän toiminnasta antaa tietoa toiminnallisuus ja turvallisuus ominaisuuksista. Koneoppimisen ja tekoälyn avulla saadaan ennakoivaa ja tietoisempaa analyysia, mikä voi auttaa identiteetin tarkastuksessa esimerkiksi havaitsemalla epäilyttäviä, sopimattomia tai epätavallisia käyttöoikeuksia. Analyysi voi kehottaa järjestelmänvalvojia tarkistamaan käyttöoikeudet. Analyysi voi tarjota automaattisesti luotuja näkemyksiä ja suosituksia, joiden avulla voidaan tehdä tietoisempia päätöksiä käyttöoikeuksiin liittyen. Näin voidaan parantaa turvallisuutta ja varmistaa vaatimustenmukaisuus. (Haber & Rolls 2019)

3.4 Automatisoitu käyttäjähallinta

Mohammed näki jo vuonna 2015 tekoälyteknologioiden käytössä potentiaalia käyttäjähallintaprosessin onnistuneessa toteuttamisessa (Mohammed 2015). Älykäs käyttäjähallinta vähentää monimutkaista valvontaa ja ylläpitoa yhdistämällä tietoja eri järjestelmistä ja lähteistä (Mohammed 2021). Tekoälyteknologioiden avulla pystyttäisiin siirtymään liian teknisestä pääsynhallinnasta ymmärrettävään pääsynhallintaan yrityksen kaikilla tasoilla. (Mohammed 2015) Tekoäly- ja koneoppimisteknologiat mahdollistavat prosessien automatisoinnin ja voivat vaikuttaa merkittävästi käyttäjähallinnan onnistumiseen (Mohammed 2021).

Nykyaikaisten tekniikoiden avulla voidaan saada uusia näkemyksiä ja menetelmiä prosessien automatisoimiseksi, joiden avulla voidaan nopeuttaa nykyistä käyttäjähallintavaatimustenmukaisuuksien valvontaa. Näin voidaan tunnistaa poikkeavuudet ja mahdolliset vaarat ilman, että täytyy palkata suurta määrää turvallisuudesta vastaavia työntekijöitä. (Mohammed 2015) Tekoäly on ratkaisu yritysten kamppailuun jatkuvasti lisääntyvien haitallisten sisältä ja ulkopuolelta tulevien pääsy-yritysten suhteen (Mohammed 2021). Tekoälyä hyödyntäessä pääsynhallinta muuttuisi reaktiivisesta pääsynhallinnasta

ennakoivaan tai jopa korjaavaan pääsynhallintaan. Työntekijöillä olisi tiedot, joita tarvitaan oikeiden teknisten ja ei-teknisten päätösten tekemiseen. Tällöin yritykset olisivat aina ajan tasalla ja aina turvattuja. (Mohammed 2015)



Kuva 8 Käyttäjähallinnan automatisoimisen hyötyjä

Tekoäly mahdollistaa käyttäjähallinnan paremman seurannan ja näkyvyyden. (Mohammed 2015) Käyttöoikeuksien hallinnassa oikeuksien myöntäminen tulisi perustua oikeaan tietoon siitä, kuka henkilö on ja miksi hän oikeuksia tarvitsee. Ongelmana usein on, että nykyiset oikeuksienvalvontamenetelmät perustuvat oletuksiin eikä täysin dataan. (Mohammed 2021) Tekoäly pystyy tunnistamaan toimia, joita ihminen ei välttämättä pysty tunnistamaan. Tekoälyn kehittyneillä todennusjärjestelmillä on tärkeä rooli, mikäli tietoa halutaan kerätä ja analysoida paljon nopeammin, mihin ihmiset pystyisivät. Tekoälyn avulla voidaan havaita omituisia, epäloogisia tai muuttuneita käytöksiä, jotka voivat johtua muun muassa siitä, että käyttäjät vierailevat järjestelmän osassa, jota he eivät yleensä tee tai hakevat enemmän tiedostoja kuin tavallisesti. IT-organisaatio pystyy tekemään älykkäitä hallinnollisia päätöksiä ja tietoisempia valintoja käyttäjien suhteen saadessaan ajantasaista tietoa jatkuvasti. (Mohammed 2015)

Tekoäly mahdollistaa käyttäjähallinnan automatisoinnin ja joustavuuden. Tekoälyn analysoidessa käyttäjien toimintojen monimutkaisuutta voidaan alhaisen riskin käyttöskenaarioiden todennus automatisoida. Tekoälyn avulla voidaan tutkia kaikkia käyttöoikeuspyyntöihin liittyviä ehtoja, joita voi olla muun muassa käyttöoikeuspyynnön kellonaika, käytettävän laitteen tyyppi, laitteiden sijainti ja pyyntöä koskeva omaisuus. Pääsyä

myönnettäessä tekoäly ottaa asetetut ehdot huomioon. Tekoälyjärjestelmät käyttävät niille annettuja käyttäjähallintaohjeita jokaiseen sille tulleeseen käyttöoikeuspyyntöön. Automatisoitu käyttäjähallinta säästää IT-osastolta aikaa ja vaivaa. (Mohammed 2015)

Tekoälyn ansiosta voidaan saavuttaa parempi tehokkuus käyttäjähallinnan säännösten noudattamisen varmistamisessa. Tietoturva- ja yksityisyyslakien noudattaminen ei riitä yksin pitämään kyberrikollisia loitolla. (Mohammed 2015) Identiteetin hakuprosessin automatisointi tekoälyä hyödyntämällä antaa IT-asiantuntijoille kyvyn havaita tietomurrot reaaliajassa. Tällöin voidaan varmistaa, että käyttäjät ovat alttiina juuri sille sisällölle ja palveluille, jota he tarvitsevat. (Mohammed 2021) Tekoäly ja koneoppiminen seuraavat jatkuvasti liikennettä, oppivat käyttäjien käyttäytymistä ja soveltavat yksityiskohtaisia pääsyrajoituksia, minkä takia yrityksillä on vähemmän ongelmia turvatoimien täytäntöönpanossa, ja hakkereiden on vaikeampi käyttää vaarantuneita tunnistetietoja. Tekoäly ja koneoppiminen yhdistettynä sopiviin valvonta- ja raportointiteknologioihin auttavat valvomaan ja vähentämään murtautumisriskiä käyttäjähallintasääntöjen avulla. (Mohammed 2015)

Parempien käyttäjähallintamenetelmien ja alentuneiden tietoturvariskien, parantuneen tuottavuuden, Privileged Access Management (PAM) ja merkittävästi pienentyneen taloudellisen tappion välillä on huomattu selkeä yhteys (Mohammed 2021). Vaikka tekoäly ja koneoppiminen mahdollistavat prosessien automatisointia, se ei kuitenkaan tarkoita sitä, että tekoälylle ja koneoppimiselle voitaisiin siirtää kaikki työ ja automatisoida koko käyttäjähallintaprosessi. On todettu, että näistä teknologioista on enemmän hyötyä, kun ne toteuttavat yhden tehtävän suorittamisen useiden sijasta. Vaikka vielä täysi automaatio ei ole vielä kannattavaa tai edes mahdollista, tekoäly ja koneoppiminen voivat auttaa ja parantaa identiteetin- ja pääsynhallintaa. (S'Heeren 2020)

Hyvä esimerkki käyttäjähallinnan automatisoinnista on Shyam R (2019) opinnäytetyö. Projektin tarkoituksena oli vähentää IT:n tekemää manuaalista työtä. Manuaalinen työ vie aikaa ja jopa toistuva manuaalinen työ voi joskus mennä pieleen monista syistä. Yrityksen kustannukset pienenevät suuremmassa määrin, kun manuaalista työtä automatisoidaan. Shyam R (2019) oli opinnäytetyössään käyttänyt Azure Bot Serviceä, Microsoftin Language Understanding (LUIS) ja Microsoft Automatea uuden käyttäjän ja oikeuksien jakamisen automatisoimisessa. (R 2019) Azure Bot Service on kattava kehitysympäristö tekoälyn suunnitteluun ja rakentamiseen (Microsoft 2022b). Luis on koneoppimiseen perustuva palvelu, jonka avulla pystyy rakentamaan luonnollisen kielen sovelluksiin, boteihin ja IoT-laitteisiin (Microsoft 2022c). Microsoft Automate on palvelu, jolla pystyy automatisoimaan työnkulkuja sovellusten ja palveluiden välillä (Microsoft 2022f).

Prosessi alkoi, kun käyttäjä teki pyynnön bottikanavalle. Työssä käytettiin keskustelukanavana Skypeä. Skype-kanava välitti käyttäjän tekemän pyynnön Azure bot -palvelulle, minkä jälkeen botti muodosti yhteyden Luisiin. Luisiin oli luotu sovellus, jonka avulla pystyttiin löytämään mitä käyttäjä pyysi. Luis etsi sopivat tavoitteet käyttäjän pyyntöön ja palautti sen takaisin. Sen jälkeen botti lähetti tiedon Microsoft Automatelle, mikä suoritti käyttäjän pyytämän tietyn automaatiotehtävän. (R 2019)

4. KÄYTTÄJÄHALLINTA TYÖKALUJA

Tässä luvussa käsitellään Azure Active Directoryn ominaisuuksia ja palveluita. Alkuun on kuitenkin hyvä ymmärtää, mikä Active Directory on ennen kuin siirrytään Azure AD:n ominaisuuksien pariin. Ymmärrettyä, mikä AD on ja mihin sitä käytetään, käydään läpi Azure AD yleisesti ja sen palveluita. Sen jälkeen käsitellään Azure AD ryhmien käyttötarkoituksia.

Active Directoryä voidaan ajatella puhelinluettelon kaltaisena tietovarastona. AD säilyttää tietoa organisaatioista, sivustoista, järjestelmistä, käyttäjistä, osakkeista ja paljon muuta ja yhdistää käyttäjätilit objekteihin ja resursseihin. Yksi merkittävä ero AD:n ja puhelinluettelon välillä on, että AD tallentaa objektit hierarkkisessa järjestyksessä ja kaikki objektit ovat ainutlaatuisia. (Amaya 2017)

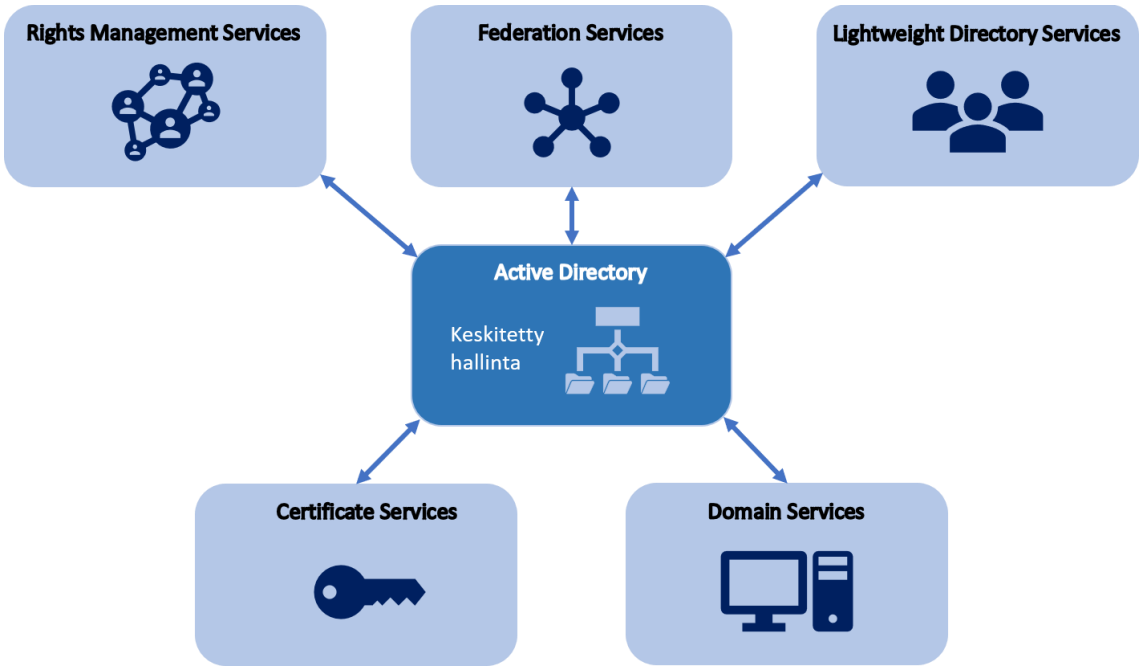
Objektien tiedot voidaan tallentaa AD:hen, minkä avulla järjestelmänvalvojien ja käyttäjien on helppo löytää ja käyttää näitä tietoja (Microsoft 2022). Objekti voi olla yksittäinen käyttäjä, ryhmä tai laitekomponentti, kuten tietokone tai tulostin. Jokaisella toimialueella on tietokanta, joka sisältää objektin tunnistetiedot. (Rubenstein 2012) Tiedot on järjestetty objekteiksi, joihin jokaiseen objektiin liittyy tietty joukko attribuutteja. AD:ssä on mahdollista tallentaa objektit hierarkiaan. AD:sta voi etsiä kohteita, joita halutaan käyttää. (Clines & Loughry 2008)

Active Directoryn avulla voidaan hallita siis koko yrityksen tietoja tehokkaasti keskitetystä arkistosta (Desmond *et al.* 2013). AD on siis eräänlainen tietovarasto (Clines & Loughry 2008). AD käyttää strukturoitua tietovarastoa tietojen hierarkkiselle järjestämiselle (Microsoft 2022a). Domain Services (AD DS) tarjoaa ominaisuudet hakemistotietojen tallentamiseen ja hallintaan (Arley 2021). AD DS esimerkiksi tallentaa tietoja käyttäjätileistä, kuten nimiä, salasanoja, puhelinnumeroita ja niin edelleen, ja sallii muiden valtuutettujen käyttäjien pääsyn näihin tietoihin samassa verkossa (Microsoft 2022a).

Domain Controlleria (DC) pidetään Active Directoryn avaimena (Bhardwaj 2020). Domain Controllerin ensisijainen tehtävä on todentaa ja valtuuttaa käyttäjiä ja heidän resurssejaan. (Arley 2021) Active Directoryn ja Domain Controllerin ero on, että AD käsittelee käyttäjän henkilöllisyyttä ja Domain Controller todentaa käyttäjän valtuudet. DC on vastuussa käyttäjätunnuksen, salasanojen ja muiden tunnistetietojen tarkistamisesta. DC:llä on oikeus sallia tai estää pääsyä yrittävä käyttäjä. (Bhardwaj 2020) Kuvassa 9 kuvattu Domain Controllerin todennusprosessi.

Kuva 9 Domain Controllerin todennusprosessi (mukaillen Arley 2021)

Kun tiedot käyttäjistä ja ryhmistä, tietokoneista, tulostimista, sovelluksista ja palveluista on lisätty AD:he, ne voidaan asettaa käytettäväksi koko yrityksessä, niin monelle käyttäjälle tai niin harvalle kuin halutaan. Tietoihin pääsyt voidaan delegoida organisaatioyksiköiden mukaiseksi. (Desmond *et al.* 2013) Active Directory Rights Management Services (AD RMS) hallinnoi käyttäjien pääsyjä tietoihin. AD RMS tarjoaa menetelmiä digitaalisen sisällön, kuten asiakirjojen, sähköpostien, toimistodokumenttien ja verkkosivujen suojaamiseen määrittelemällä, kuka voi avata, muokata, tulostaa, lähettää edelleen tai tehdä muita toimia. (Arley 2021)



Kuva 10 Active Directoryn palvelut (mukaillen Amaya 2017; Arley 2021)

Active Directory Federation Services (AD FS) on identiteetinhallintapalvelu, joka mahdollistaa kertakirjautumisen ulkoisille Web-sivustoille ja sovelluksille Single-Sign-On (SSO) -sisäänkirjautumisen avulla (Arley 2021). AD FS todentaa sovelluksia tai palveluita verkon ulkopuolella (Amaya 2017). Käyttäjän tarvitsee muistaa vain yksi tunnus, kirjautuakseen useisiin paikkoihin (Arley 2021).

Active Directory Lightweight Directory Services (AD LDS) palvelu tarjoaa hakemistopalveluita (Arley 2021). AD LDS on Active Directoryn itsenäinen tila ilman infrastruktuurin

ominaisuuksia ja joka tarjoaa hakemistopalveluita sovelluksille (Microsoft 2018). AD LDS voi toimia millä tahansa erillisellä palvelimella ja tarjoaa oman tietovaraston (Arley 2021).

Active Directory -Certificate Servicellä (AD CS) voi luoda ja hallita julkisia avaimia, tarjota digitaalisia varmenteita ja allekirjoituksia organisaation käyttöön (Arley 2021) ja hallita sertifikaatteja ja muita salauskomponentteja (Amaya 2017). Kuvaan 10 on koottu AD:n palveluita, selventämään AD:n kokonaisuutta.

4.1 Azure Active Directory

Azure Active Directory (Azure AD) on pilvipohjainen identiteetin- ja pääsynhallinta palvelu (Microsoft 2022b, Microsoft, 2022c). Azure AD on monivuokralainen, pilvipohjainen hakemisto- ja identiteetinhallintapalvelu. Azure AD yhdistää ydinhakemistopalvelut, sovellusten käyttöoikeuksien hallinnan ja identiteetin suojauksen yhdeksi kokonaisuudeksi. (Microsoft 2022b) Microsoft Azure AD on erittäin turvallinen Active Directoryn pilvilaajennus (Soh *et al.* 2020). Azure AD:n avulla voidaan keskittää turvatarkastukset, havainnot käyttäjistä- ja palveluidentiteeteistä sekä hallinta identiteettejä yhdestä paikasta (Microsoft 2022b). Azure Active Directory tarjoaa paljon ominaisuuksia ja palveluita identiteetin ja pääsynhallintaan (Microsoft 2022c), joista muutamia esiteltynä seuraavana.

Azure AD:lle voi delegoida käyttäjätunnusten hallinnan, kuten kirjautumisen, käyttäjätunnukset, salasanat, monivaiheisen tunnistautumisen, älykkään lukituksen ja monia muita tehtäviä (Sahay 2020, Microsoft 2022c). Azure AD hyödyntää ehdollista pääsyä ja monivaiheista tunnistautumista useilla eri vaihtoehdoilla, mukaan lukien älykortit, sertifikaatit, biometriset tiedot, kuten sormenjälki ja kasvojentunnistus Windows Hellolla (Soh *et al.* 2020).

Azure AD:n itsepalvelun avulla käyttäjät voivat nollata salasanansa. Itsepalvelu tunnistaa salasanat, mitkä ovat kiellettyjen salasanojen luettelossa ja näin estää ottamasta liian heikkoa salasanaa käyttöön. (Microsoft 2022c) Ottamalla salasanan hash-synkronointi käyttöön, voidaan auttaa suojaamaan aiempien hyökkäyksien vuotaneiden tunnistetietojen toistamiselta. Salasanahajautussynkronointi on ominaisuus, jota käytetään käyttäjien salasanahajautusten synkronoimiseen paikallisesta Active Directory -esiintymästä pilvipohjaiseen Azure AD -esiintymään. (Microsoft 2022b)

Microsoft (2022b) mukaan mikäli yrityksellä on käytössä hybridi-identiteettiskenaario, olisi suositeltavaa, että yritys integroisi paikalliset- ja pilvihakemistot. Integroinnin avulla IT-tiimi pystyy hallitsemaan tilejä yhdestä paikasta riippumatta siitä, missä tili on luotu. Integraation avulla käyttäjät pystyvät olemaan tuottavampi, kun identiteetti toimisi sekä pilvi- että paikallisten resurssien käytössä. Johdonmukaisuus ja yksi virallinen AD lähde

lisää selkeyttä ja vähentää inhimillisistä virheistä sekä konfiguroinnin monimutkaisuudesta johtuvia turvallisuusriskejä. Organisaatiolla voi olla enemmän ylimääräistä tilien hallintaa, mikäli sillä ei ole integroitu paikallista identiteettiä pilvi-identiteettiin. Integroiminen vähentää virheiden ja tietoturvaloukkausten todennäköisyyttä. (Microsoft 2022b)

Uusien sovellusten kehittämiseen kannattaa käyttää Azure AD:tä todentamiseen. Todennukseen on erilaisia ominaisuuksia olemassa, riippuen käyttäjän roolista organisaatiossa. Organisaation työntekijöille on Azure AD, vieraskäyttäjille ja ulkoisille kumppaneille Azure AD B2B ja asiakkaiden hallinnointia varten on Azure AD B2C. (Microsoft 2022b) Vieraskäyttäjien ja ulkoisten kumppanien hallitseminen helpottuu, kun niitä voidaan hallita samalla tavalla kuin yrityksen omien yhteystietojen hallintaan (Microsoft 2022c).

Azure AD tarjoaa raportteja ja seurantaa, joiden avulla voidaan hankkia näkemyksiä ympäristön turvallisuudesta ja käyttötavoista. Raporttien avulla voidaan tunnistaa mahdolliset haavoittuvuudet, jotka vaikuttavat organisaation identiteettiin. Tunnistamalla haavoittuvuudet voidaan määrittää käytännöt, millä reagoidaan epäilyttäviin toimiin ja mikä helpottaa ryhtymistä asianmukaisiin toimiin haavoittuvuuksien ratkaisemiseksi. (Microsoft 2022c)

Azure AD auttaa yrityksen työntekijöitä käyttämän sisäisiä resursseja ja ulkoisia resursseja, kuten Microsoft 365:tä, Azure-portaalia ja useita muita SaaS-sovelluksia. Sisäisiä resursseja ovat resurssit, joita voivat olla yrityksen verkossa ja intranetissä olevat sovellukset sekä organisaation kehittämät pilvisovellukset. Azure AD:ta käyttävät IT-järjestelmänvalvojat, sovelluskehittäjät ja Microsoft 365-, Office 365-, Azure- tai Dynamics CRM Online -tilaajat. IT-järjestelmänvalvoja voi hallita sovelluksien ja sovellusresurssien käyttöoikeuksia Azure AD:n avulla liiketoimintavaatimusten perusteella. Azure AD:n avulla voi ottaa sisäänkirjautumisen yhteydessä monivaiheinen tunnistautumisen käyttöön, mikä lisää turvallisuutta. Sovelluskehittäjät voivat käyttää Azure AD:ta kertakirjautumisen (SSO) lisäämiseen sovellukseen, jolloin sovellus toimii käyttäjän olemassa olevilla tunnistetiedoilla. Jokainen Microsoft 365-, Office 365-, Azure- ja Dynamics CRM Online -käyttäjä on automaattisesti Azure AD -käyttäjä. (Microsoft 2022c)

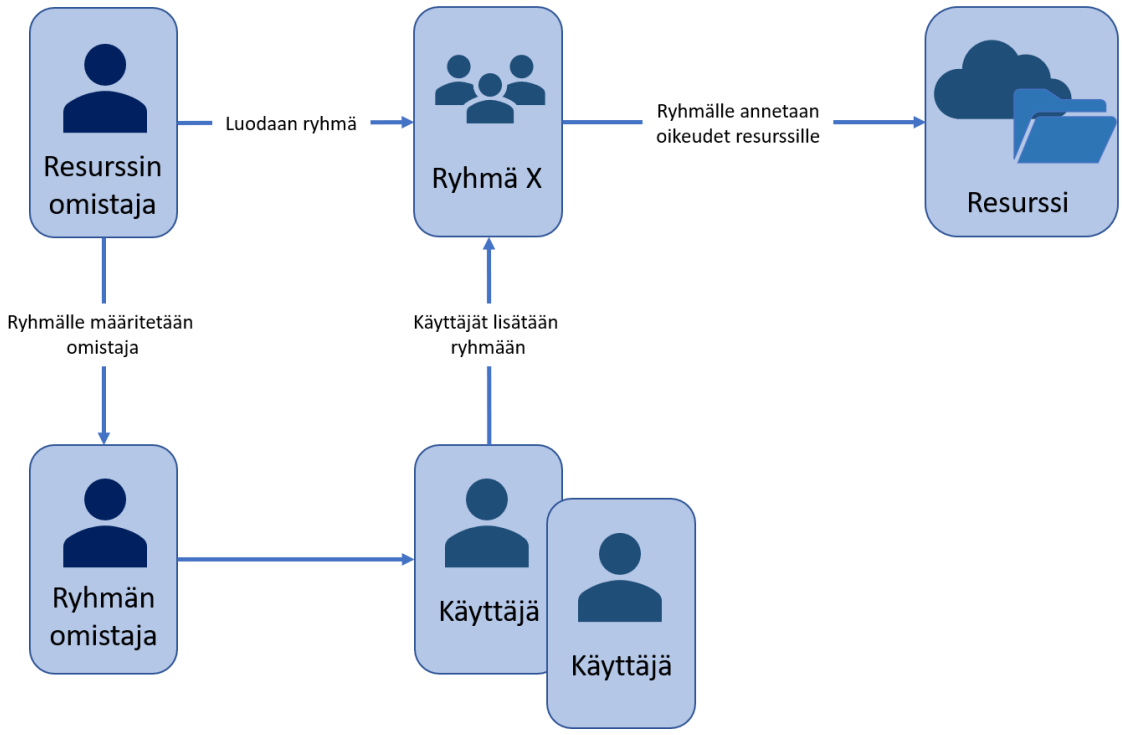
4.2 Azure Active Directory ryhmät

Ryhmä on joukko käyttäjiä tai resursseja, joilla on samat ominaisuudet ja vastuut (Francis 2021). Organisaatiossa yksittäisiä identiteettejä lisätään ja poistetaan, mutta roolit ja vastuut eivät juurikaan muutu. Siksi hyvä tapa hallita oikeuksia organisaatioissa perustuu

rooleihin ja vastuisiin yksilöiden sijaan. (Francis 2021) AD-ryhmiä käytetään hallitsemaan käyttäjätilejä, tietokonetilejä ja muita ryhmiä. Ryhmissä voi olla jäseniä, jotka voivat olla käyttäjätilejä, yhteystietoja, tietokoneita ja muita ryhmiä. Ryhmien kanssa toimiminen yksittäisten käyttäjien sijaan yksinkertaistaa oikeusverkon ylläpitoa ja hallintoa (Microsoft 2021).

Active Directory -ryhmien avulla voidaan jaotella identiteetit käyttöoikeusvaatimusten perusteella. Active Directory -ympäristössä on kaksi ryhmäluokkaa, suojausryhmät ja jakeluryhmät. (Francis 2021, Microsoft 2021) Tarvittaessa jakeluryhmä voidaan muuttaa suojausryhmäksi ja päinvastoin (Berkouwer 2019).

Jakeluryhmiä tulee käyttää sähköpostijärjestelmän, kuten Microsoft Exchangen, kanssa (Francis 2021). Jakeluryhmiä käytetään vain sähköpostin jakeluluetteloiden luomiseen (Microsoft 2021). Tämän tyyppistä ryhmää käytetään saapuvien sähköpostien jakamiseen ryhmän jäsenille. Nämä ryhmät eivät ole suojattuja, joten et voi käyttää niitä käyttöoikeuksien määrittämiseen. (Francis 2021, Microsoft 2021)



Kuva 11 Active Directory suojausryhmän käyttö (mukaillen Arley 2021b)

Suojausryhmiä käytetään jaettujen resurssien käyttöoikeuksien määrittämiseen (Francis 2021, Microsoft 2021). Käyttäjäoikeudet määrittävät, mitä kyseisen AD-ryhmän jäsenet voivat tehdä toimialueen puitteissa. Suojaryhmien avulla voidaan määrittää käyttäjäoikeudet tiettyjen tehtävien delegoimiseksi. Kun järjestelmänvalvoja on määrittänyt käyttö-

oikeudet resursseille, määrittää järjestyksenvalvoja ne suojausryhmälle yksittäisten käyttäjien sijaan. Jokainen ryhmään lisätty käyttäjä saa kyseiselle AD-ryhmälle määritetyt oikeudet. (Microsoft 2021) Kuvassa 11 on esitetty suojausryhmän käyttöprosessi.

Jäsenten lisääminen ryhmiin tapahtuu usein organisaatiossa manuaalisesti jonkin IT-henkilön toimesta (Centero Oy 2012). Manuaalisen prosessin takia on mahdollista, että vääriä oikeuksia jaetaan vahingossa (Francis 2021). Ryhmien jäsenten hallinta on haasteellista manuaalisen lisääminen takia. Isoissa organisaatiossa usein käyttöoikeuksia hallinnoiva henkilö ei edes välttämättä tiedä mitä dataa resurssi sisältää. Sen takia on vaikeaa tehdä päätöksiä, voidaanko käyttäjälle myöntää oikeudet kyseiseen resurssiin. (Centero Oy 2012) IT-osaston ei kannata olla vastuussa ryhmänhallinnasta. Eri osastojen johtajat ja ryhmien omistajat, voidaan valtuuttaa hallitsemaan, kenellä on pääsy ryhmään. (DNSstuff 2019)

Azure AD suojausryhmiä voi myös lisätä sisäkkäin. Jäsenryhmä (subgroup) perii pääryhmän attribuutit ja ominaisuudet. (Microsoft 2021b) Kun ryhmä on toisen ryhmän jäsen, kutsutaan tätä sisäkkäisiksi ryhmiksi (Berkouwer 2019). Ryhmien ryhmitteleminen sisäkkäin helpottaa oikeuksien hallintaa (Windows Active Directory 2021). Toteuttamalla sisäkkäiset ryhmät oikein ja huolellisesti suunniteltuna voidaan varmistaa, että tiedot pysyvät turvassa ja samalla parantaa käyttäjähallinnan tehokkuutta (DNSstuff 2019).

Suunnitellessa sisäkkäisiä ryhmiä on huolehdittava lupien periytymisistä. On muistettava, että pääryhmän sisälle lisätty jäsenryhmä saa pääryhmän oikeudet. On tiedostettava, kenelle saa jakaa oikeuksia ja minne, kun lisätään ryhmiä sisäkkäin. Ryhmiä laitettaessa sisäkkäin on kannattavaa miettiä myös ryhmien nimeämistä. Ryhmien nimeäminen selkeästi auttaa hahmottamaan mihin kyseinen ryhmä antaa oikeudet. Hyvä nimeämiskäytäntö on esimerkiksi nimetä ryhmä käyttäjäryhmän mukaan, mikä voi olla esimerkiksi osaston nimi (myynti, markkinointi, HR jne.) ja mihin ryhmä antaa oikeudet. Kun ryhmiä on paljon sisäkkäin epäselvästi nimettyjen ryhmien käyttäminen voi olla monimutkaista ja aiheuttaa tietoturvariskejä. (DNSstuff 2019)

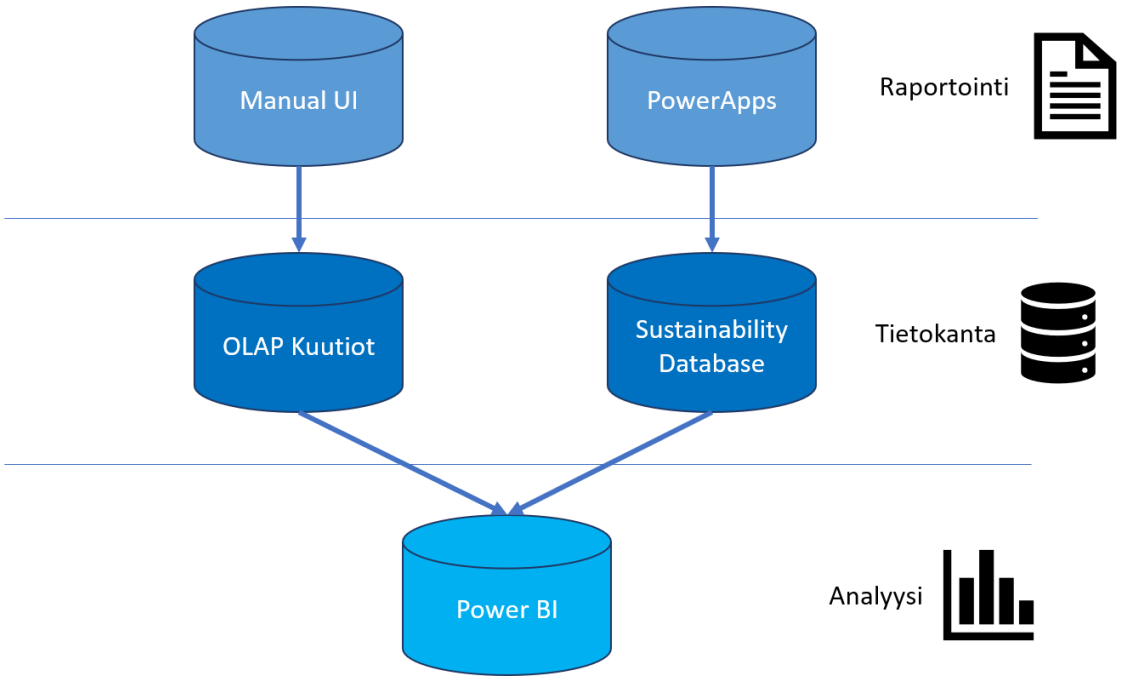
5. YRITYKSEN NYKYINEN KÄYTTÄJÄHALLINTA

Tässä luvussa tutustutaan tarkemmin työn yritykseen ja sen nykytilaan. Yrityksen puolelta asetettiin tavoitteet uudelle käyttöoikeuksienhallinnalle, mitkä käydään läpi viimeisessä alaluvussa.

5.1 Organisaatio

Kyseinen yritys on kansainvälinen konserni, jolla on tytäryrityksiä useissa maissa. Konserni toimii 17 maassa ja työllistää kaiken kaikkiaan lähes 10 000 henkilöä. Konsernilla on tytäryrityksiä Euroopassa, Pohjois-Afrikassa, Etelä-Amerikassa ja Kauko-Idässä. Konsernin tytäryhtiöillä saattaa olla useita toimipisteitä ja tehtaita kyseisissä maissa. Esimerkiksi yrityksen Suomen tytäryhtiöllä on 12 tehdasta ja 1 toimipiste suunnittelulle.

Yritys käyttää Power BI:tä datansa analysointiin. Yritys käyttää myös Exceliä datan analysoimiseen. Data Power BI ja Excel raportteihin saadaan OLAP kuutioista. Kuutioihin data tulee käytössä olevan Manual UI:n kautta, jota käytetään raportoitavan tiedon keräämiseen. Liiketoimintayksiköillä on omat OLAP kuutiot, jotka toimivat datavarastoina ja Power BI raportit, joihin muut liiketoimintayksiköt eivät pääse.



Kuva 12 Yksinkertaistettu kuva työn aiheena olevista yrityksen järjestelmistä

Kuvassa 12 on kuvattu jo käytössä olevat ja uusien järjestelmien suhde toisiinsa. Uutena käyttöön on tulossa PowerAppsillä kehitetty sovellus, jolla voi syöttää tietoja. Tiedot kulkeutuvat PowerAppsistä Sustainability Database -tietokantaan. Sustainability databasessa on ryhmitelty eri tukifunktioiden datat erikseen. Power BI saa Sustainability Databasesta dataa raportteja varten.

Liiketoimintayksiköiden käyttäjien käyttöoikeuksia hallinnoidaan keskitetysti konserni tasolla. Liiketoimintayksiköiden lisäksi konsernilla on erilaisia tukifunktioita, kuten myynti, HR ja talous. Konsernin eri tukifunktioiden dataa pääsee käsittelemään ne, joille on myönnetty oikeudet funktioon yleisesti.

Käytössä olevista järjestelmistä Manual UI:n, OLAP kuutioden ja Power BI:n käyttöoikeuksien jakaminen tapahtuu tällä hetkellä eri tavalla. Aikaisemmin yrityksellä oli pitkään vain OLAP kuutiot käytössä, jolloin käyttäjähallinnassa ei ollut ongelmia. Käyttöoikeuksien hallinnointi tapahtui yhdestä paikkaa, kun piti myöntää oikeuksia vain kuutioihin. Viime vuosina yritykselle on tullut käyttöön useampi järjestelmä. Järjestelmille on luomisvaiheessa rakennettu oma käyttäjähallinta. Se onkin pääsyy, miksi käyttöoikeuksien myöntäminen on hajautettu. Yrityksessä on herätty käyttäjähallinnan ongelmiin. Käyttäjähallinta muuttui nopeasti haasteelliseksi.

5.2 Käytössä olevat järjestelmät

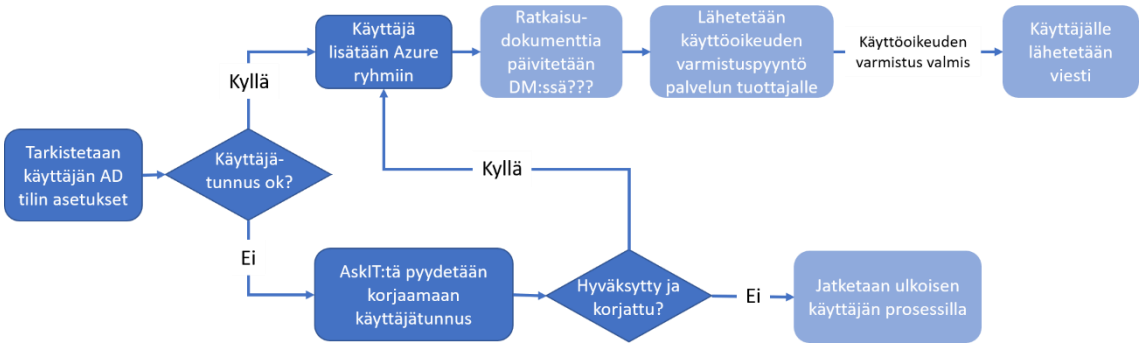
5.2.1 Manual UI

Manual UI on palveluntuottajan toteuttama palvelu, jolla yrityksen käyttäjät pystyvät raportoimaan tehtaiden tilanteista syöttämällä dataa lomakkeiden kautta. Manual UI:ssä on perus output-input tietoa, eli paljonko on valmistettu, paljonko meni tunteja, mikä oli tuottavuus ja niin edelleen.

Käyttöoikeuksien saaminen järjestelmään tapahtuu palvelutuottajan kautta. Käyttöoikeuksia on vain muutamalla tehdasta kohden, yleensä raportoinnista vastaavalla tehtaanjohtajalla. Palveluntuottajalla käyttöoikeuksien lisäämisestä vastaa järjestelmän ylläpidosta vastaava työntekijä. Kuvassa 13 on esitetty sisäisen Azure käyttäjän lisääminen Manual UI:hin.

Ensimmäisenä tarkistetaan, että käyttäjän tilillä on tarpeeksi määrittelyitä. Käyttäjän AD-tunnus pitää olla muun muassa osa jotain organisaatiota, maayhtiötä ja sille pitää olla asetettuna esihenkilö, jotta sen kohdalla voidaan prosessia jatkaa. Mikäli käyttäjätunnuksen asetukset ovat kunnossa, käyttäjä lisätään Azure-ryhmiin. Lisäyksen jälkeen päivi-

tetään dokumenttia, jossa pidetään käyttäjälistaa Excelissä. Sen jälkeen lähetetään käyttöoikeuksista pyyntö palveluntarjoajalle. Kun palveluntarjoaja on saanut varmistettua käyttöoikeuden ja lisättyä käyttäjän, lähtee käyttäjälle viesti.



Kuva 13 Sisäisen Azure käyttäjän lisääminen

Mikäli käyttäjätunnuksen asetukset eivät olleet kunnossa, pyydetään AskIT:tä korjaamaan käyttäjätunnus asianmukaiseksi. Mikäli tunnus on tämän jälkeen korjattu ja hyväksytty lisätään se aikaisemmin mainittuihin Azure-ryhmiin ja jatketaan normaaliin tapaan prosessia. Mikäli tunnusta ei saatu korjattua ja sitä ei hyväksytty, jatketaan prosessia ulkoisen käyttäjän lisäämisen mukaan.

Manual UI:ssa on tällä hetkellä käyttöoikeuksia lähinnä vain käyttäjillä, jotka raportoivat tehtaiden tuloksia. Nämä käyttäjät ovat yleensä tehtaan johtajia tai raportoinnista vastaavia työntekijöitä. Yritys antaa käyttäjälle oikeudet yleisesti Manual UI:hin AD-ryhmällä ja palveluntuottaja antaa Manual UI:n sisällä eri raportointi oikeuksia. Palveluntarjoaja lisää henkilön Manual UI:n kantaan, jossa voidaan määrittää, kenellä on oikeuksia ja mihin. Manual UI:hin sisäänkirjaudutaan Azure AD-tunnuksilla. Manual UI sisäänkirjautumisen yhteydessä tarkistaa kannasta onko tunnuksella oikeuksia. Manual UI:ssa voi olla kenttäkohtaisia oikeuksia, esimerkiksi menneen kuukauden kenttään ei voi syöttää enää tietoja. Tehtaanjohtajat pystyvät syöttämään vain sellaisia tietoja mihin heillä on oikeudet. Manual UI:n tietokantaan on vain muutamalla palveluntarjoajan edustajalla oikeudet. Tiedot viedään Manual UI:sta myös kuutioon, josta tutkimuksen kohdeyritys pystyy raportoimaan tietoja muun muassa Power BI:n avulla.

5.2.2 OLAP kuutiot

OLAP kuutioiden ominaisuuksiin pystyisi mennä paljon syvemmälle, mitä tässä työssä mennään. Tässä työssä kuitenkin riittää perusymmärrys siitä, mikä on OLAP kuutio. OLAP viittaa tekniikkaan, jolla suoritetaan monimutkainen analyysi tietovarastoon tallen-

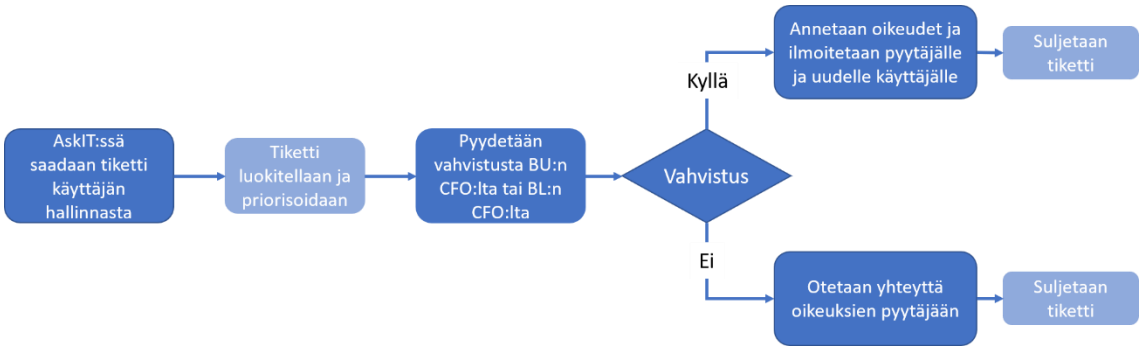
netuille tiedoille (Datta ja Thomas 1999). OLAP tulee sanoista Online Analytical Processing. OLAP-tietokannat on jaettu yhteen tai useampaan kuutioon. Kuutiot on suunniteltu siten, että raporttien luominen ja katselu on helppoa. (Taylor 2020) OLAP-kuutio on tietorakenne, joka mahdollistaa tietojen nopean analysoinnin useiden liiketoimintaongelman määrittelevien ulottuvuuksien mukaan (OLAP.com).

Yrityksellä on käytössä OLAP kuutioita, joissa se säilöö muun muassa Manual UI:stä tulevaa dataa. Kuutiot ovat olleet pitkään käytössä ja ne ovat vanhempaa teknologiaa. Yrityksen kaikilla liiketoimintayksiköillä ei ole kuutioita käytössä, vain vanhemmilla liiketoimintayksiköillä. Yrityksellä on kahden tyyppisiä kuutioita. Kuutioita, jotka ovat liiketoimintayksikkö kohtaisia ja kuutioita, joissa on kaikkien liiketoimintayksiköiden dataa koottuna. Kuutiot on rakennettu ERP:n päälle ja näin ollen sisältävät operatiivista dataa. Kuutioissa on pitkälti samaa dataa mitä raportoidaan Manual UI:sta. Lisäksi kuutioissa on esimerkiksi myyntidataa, dataa tilauskannasta ja tarjouskannasta, projektien statuksista ja perus talousdataa. Pääosin data on matalariskistä. Datasta muun muassa tuotantomäärät ja liikevaihdot ovat käytännössä julkista dataa. Tilausten hinnoitteluun liittyvä data on liikesalaisuudeksi luokiteltavaa tietoa, joten sen pitäisi olla hyvin suojattua.

Yrityksen käytössä olevasta ERP-järjestelmistä tulee dataa suoraan kuutioihin. Yrityksellä on keruuajo ja prosessointiajo, joilla kerätään dataa kuutioihin. Keruuajo kerää datan ERP-järjestelmistä tiettyihin tauluihin joka yö. Prosessointiajo on ajastettu keruuajon perään, millä päivitetään kuutioiden tiedot. OLAP kuutiot toimivat nykyisessä käyttötarkoituksessa kohtuullisen hyvin. Jatkossa kuitenkin isoimmat kehitys hankkeet tullaan todennäköisesti tekemään hieman eri teknologioilla. OLAP kuutiot toimivat hyvin, kun dataa haetaan suoraan yrityksen nykyisestä ERP järjestelmästä. Kuutiot tulevat todennäköisesti olemaan käytössä niin kauan kuin kyseinen ERP on käytössä.

Yritys jakaa OLAP kuutioihin käyttöoikeudet yhdessä tasossa olevien Active Directory ryhmien kautta. Ryhmiä on reilu 70, joilla jaetaan käyttäjille oikeuksia yrityksen käytössä oleviin järjestelmiin. Suurin osa AD-ryhmistä on jäämässä turhiksi, vanhan järjestelmän poistuttua käytöstä. Käyttäjän lisääminen ryhmiin tapahtuu siten, että käyttäjälle pyydetään oikeuksia ja Service Deskistä käydään lisäämässä käyttäjän oikeisiin AD-ryhmiin.

AD-ryhmien sisällä ei ole mitään rooleja erikseen. Osa AD-ryhmistä on jaettu rooleihin. ”Dev”-ryhmien jäsenillä on pääsy testipalvelimelle luomaan raportteja. ”Members”-ryhmien jäsenillä on oikeudet Exceleiden kautta kuutioiden dataan ja pystyvät luomaan raportteja. ”Visitors”-ryhmien jäsenillä on vain katseluoikeudet. AD-ryhmien nimet muodostuvat lähdejärjestelmästä, yrityksen tytäryhtiöstä ja roolista: U_YRITYS_lähdejärjestelmä_liiketoimintayksikkö_rooli.



Kuva 14 Yrityksen kuutioiden käyttöoikeusprosessi

Kuutioiden käyttöoikeuksien saaminen tapahtuu kuvassa 14 kuvatun prosessin mukaan. Ensimmäisenä IT-tuessa saadaan tukipyyntö uusista oikeuksista. Pyyntö luokitellaan ja priorisoidaan. Sen jälkeen käyttöoikeuksien oikeellisuus vahvistetaan liiketoimintayksikön tai BL:n CFO:lta. Mikäli vahvistuksesta tuli myöntävä vastaus, annetaan käyttäjälle oikeudet ja ilmoitetaan siitä oikeuksien pyytäjälle ja uudelle käyttäjälle. Lopuksi suljetaan tiketti. Mikäli vahvistuksessa ei annettu myöntävää vastausta käyttäjän oikeuksille, otetaan oikeuksien pyytäjään yhteyttä ja suljetaan tiketti.

5.2.3 Power BI

Power BI on eräänlainen kattotermi ja se voi viitata joko Windows-työpöytäsovellukseen Power BI Desktop, Power BI:n online SaaS-palveluun tai Power BI -mobiilisovellukseen (Wright 2019). Power BI on Microsoftin ohjelmistopalvelu, jonka avulla voidaan muuntaa datalähteistä oleva data johdonmukaiseksi, visuaaliseksi ja vuorovaikutteiseksi raporteiksi (Microsoft 2022c). Power BI:n avulla käyttäjät voivat luoda ja jakaa selkeitä ja hyödyllisiä tilannekuvia yrityksensä tapahtumista. Power BI työkalujen avulla organisaatio pystyy kokoamaan, hallitsemaan ja analysoimaan tietoja useista eri lähteistä käyttäjäystävällisen käyttöliittymän kautta. (Wright 2019)

Yritys analysoi Power BI:ssä dataa, mikä saadaan kuutioista ja tulevaisuudessa Sustainability Databasesta. Power BI työtiloihin käyttäjä saa oikeudet työtilan järjestelmänvalvojalta. Käyttöoikeudet myönnetään Power BI:hin työtilakohtaisesti, lisäämällä käyttäjä työtilan käyttäjiin. Power BI:ssä raportteja tekevät eri käyttäjät, jotka raportoivat Manual UI:n kautta tehtaan lukuja. Käyttäjä on saanut oikeudet työtilaan työtilan ylläpitäjältä. Power BI työtilojen tulisi olla yhteydessä tiimiin, jotta vältyttäisiin irtonaisilta työtiloilta.

5.2.4 Power Apps

Power Apps on Microsoftin sovelluskehitysympäristö, mikä tarjoaa nopean ja helpon tavan rakentaa mukautettuja sovelluksia liiketoiminta tarkoituksiin (Microsoft 2022d). Po-

wer Appsistä on mobiilisovellus ja verkkoversio, joilla sovelluksia voi hallinnoida ja rakentaa (Karnes 2017). Sovelluksia voi kehittää mobiili- ja verkkoympäristöille (Guimonet 2019).

Yritys on rakentanut Power Appsin raportointi käyttöä varten. Power Apps on periaatteessa rinnakkainen järjestelmä Manual UI:lle. Power Apps tulee käyttöön yrityksen Sustainability raportointia varten. Power Apps ja Manual UI tulevat olemaan käytössä rinnakkain. Järjestelmiin syötetään hiukan eri dataa. Kun Manual UI:ssa raportoidaan tehtaiden dataa, niin Power Apps sovelluksella raportoitaisiin tukifunktioiden dataa.

Power Appsissa käyttäjällä olisi oikeudet syöttää tietoja omalle tukifunktiolle, mikäli rooli oikeuttaa raportointi oikeuteen. Raportointioikeus on vain raportoinnista vastaaville käyttäjille. Käyttäjällä on oikeudet syöttää vain tietoja tietylle tukifunktiolle. Esimerkiksi myynnin työntekijä ei voisi syöttää HR-dataa. Power Appsista pystyy myös tarkastelemaan tukifunktion historiadataa. Käyttäjällä on oikeudet tarkastella myös muiden syöttämiä tietoja, mikäli ne ovat tukifunktion tietoja, jossa käyttäjä työskentelee. Power Appsilla pystyttäisiin viemään dataa kuutioihinkin, mutta sitä ei todennäköisesti tulla tulevaisuudessa käyttämään siihen käyttötarkoitukseen.

5.2.5 Sustainability Database

Yritys on kehittämässä Sustainability databasea säilömään Power Appsistä tulevaa dataa. Sustainability databasen tietoja pystyisi tarkastella taulukko tasolla. Sustainability Database sisältäisi enimmäkseen tukifunktioihin liittyvää dataa. Vaikka tukifunktioiden data pääsääntöisesti, raportoidaan Power Appsista Sustainability Databaseen, niin myös OLAP kuutioissa on jonkin verran tukifunktioihin liittyvää dataa. Muun muassa myyntii liittyvää dataa löytyy myös kuutioista.

Tukifunktioiden datassa voi olla GDPR-dataa tietyssä taulukossa. Tällöin taulukko on luokiteltu GDPR-dataksi ja arkaluontoiseksi. Vain käyttäjä, jolla on oikeudet käsitellä GDPR-dataa, pääsee näkemään ja käsittelemään kyseisien taulukkojen tietoja. Yritys käy aina taulukot luonti vaiheessa läpi ja luokittelee ne sen mukaan, onko taulukossa kriittistä dataa ja pitääkö taulukko rajata pienemmälle ryhmälle. Yrityksellä on riskiluokitukset taulukkokohtaisesti.

5.3 Tavoitteet

Työn tavoitteena on kehittää yrityksen käyttäjähallinnan ongelmiin ratkaisut. Pääongelmina oli, että käyttäjillä on ollut oikeuksia joko liikaa tai ei ollenkaan ja käyttäjähallinnan monimutkaisuus. Lisäksi ongelmana on käyttöoikeuksien poistaminen, kun käyttäjä ei enää tarvitse kyseiseen resurssiin oikeutta. Tavoitteena on yhtenäistää käyttäjähallinta

yhteen paikkaan ja tehdä ryhmistä tarkempia. Tällöin käyttäjät saisivat oikeuksia oikean määrän oikeaan paikkaan keskitetystä paikasta.

Nykyisessä tilanteessa käyttäjät ovat saattaneet saada liikaa oikeuksia, mikä on voinut aiheuttaa tietoturvariskejä. Kun henkilö lisätään esimerkiksi Suomen liiketoimintayksikön ryhmään, pääsee henkilö kaikkeen liiketoimintayksikön dataan käsiksi. Ryhmistä haluttaisiin tehdä tarkempia, jolloin oikeuksia dataan tulisi rajattua paremmin. Ryhmiä pitäisi pystyä olla tietyillä yhdistelmä säännöillä, esimerkiksi talous + Suomi, jolloin Suomen liiketoimintayksikön talous henkilö pääsisi käsiksi kyseisen liiketoimintayksikön taloustietoihin. Tällöin pystyttäisiin rajaamaan oikeuksia siten, että kaikki Suomen työntekijät eivät pääsisi tarkastelemaan arkaluontoista dataa.

Tukifunktioiden data haluttaisiin rajata omiksi kokonaisuuksiksi. Sen lisäksi tukifunktioiden ja liiketoimintayksiköiden taulukot, mitkä sisältävät GDPR-dataa rajattaisiin käyttäjille, jotka saavat käsitellä ja nähdä GDPR-dataa. GDPR-taulukoiden käyttäjäoikeuksien hallinnointi pitäisi tapahtua paikallisesti. Väärän tahon päästessä yrityksen dataan käsiksi, mahdollisia ongelmia olisi hinnanmuodostuksen aukeneminen kilpailijoille ja GDPR säännösten rikkominen.

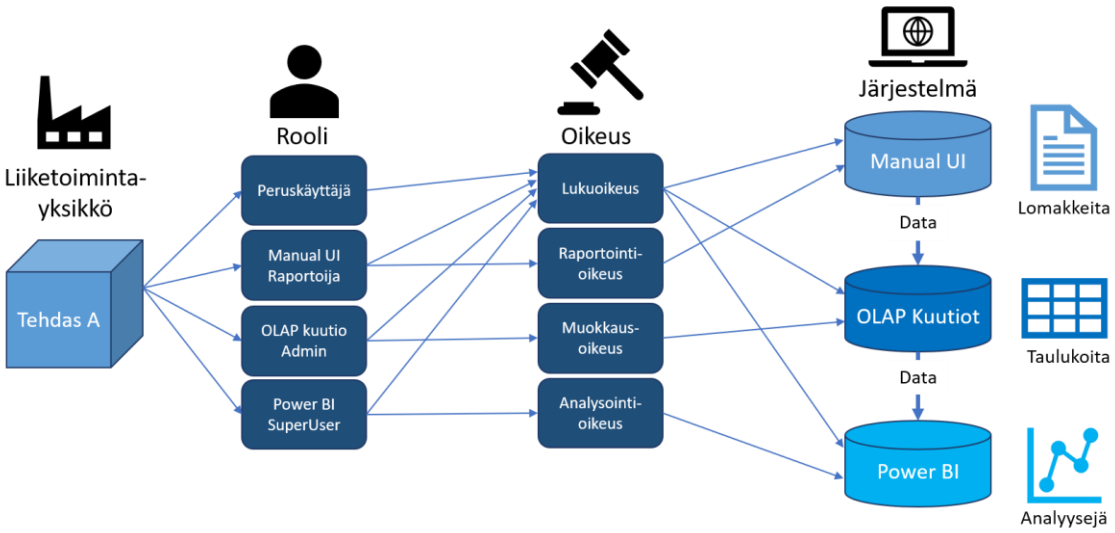
Liiketoimintayksiköiden välillä saattaa olla eroavaisuuksia, miten haluavat omaa lokaaliraportointiaan pyörittää. Käyttäjähallintaprojektin laajuus rajautuu konsernin Group IT:n tarjoamiin palveluihin. Tilanteissa, joissa liiketoimintayksikkö toteuttaa käyttäjähallintansa itse, konsernin toimesta tietoturvajohtaja käy kuitenkin datan läpi ja tekee riskiluokittelun. Tällöin voidaan varmistaa, että esimerkiksi GDPR tietoa käsitellään asianmukaisesti.

Uutena käyttöön tulevilla järjestelmille ei ole vielä toteutettu käyttäjähallintaa. Tarkoituksena on, että uusien järjestelmien käyttäjähallinta toteutetaan samasta paikkaa, mistä jo käytössä olevien järjestelmien käyttäjähallinta tullaan jatkossa toteuttamaan. Käyttöoikeudet haluttaisiin myöntää Azure AD-ryhmien kautta. Kun tiedetään, että henkilö aloittaa yrityksessä, henkilön esihenkilö pyytää IT-operaattori luomaan uuden käyttäjätilin. Käyttäjätilille annetaan tiedot, missä työntekijä tulee työskentelemään ja millä roolilla. Mikäli käyttäjän profiililta puuttuu jotain tietoja täyttämättä niin esihenkilö täydentää. IT-puolella on yksi operaattori, joka ylläpitää käyttäjätunnuksia. Työskentely sijainnin ja roolin perusteella työntekijä lisätään oikeisiin ryhmiin automaattisesti. Mikäli käyttöoikeuksiin tulee myöhemmässä vaiheessa muutos tarpeita henkilö itse pyytää IT- operaattorilta oikeuksia, henkilön esihenkilö hyväksyy oikeudet ja IT-operaattori tekee päivityksen.

Sama data kulkee usean järjestelmän läpi, minkä takia ei ole väliä mistä järjestelmästä käyttäjä sitä tarkastelee. Enemmän on väliä, mitä dataa käyttäjä pääsee tarkastelemaan.

Minkä takia yritys asetti tavoitteeksi, että jatkossa käyttöoikeudet olisivat suunniteltu sen mukaan mihin dataan käyttäjällä saa olla oikeudet, eikä mihin järjestelmään käyttäjällä pitäisi olla oikeudet.

Toiveena olisi, että jatkossa oikeuksien poistaminen olisi automaattista. Mikäli käyttäjä poistuu organisaatiosta, poistuu tili edelleen käytöstä työsuhteen loputtua. Mutta mikäli käyttäjä vaihtaa organisaation sisällä esimerkiksi toiseen liiketoimintayksikköön, muuttuisi käyttöoikeudet AD-roolin muuttuessa. Tavoitteena olisi, että käyttäjän tili olisi osa jotain organisaatiorakennetta ja oikeudet tulisivat ja poistuisivat, sitä mukaan, kun käyttäjän sijaintia organisaatiossa muutetaan.



Kuva 15 Yrityksen tavoitteet rooleille, oikeuksille ja järjestelmille

Yritys määritteli järjestelmäkohtaisesti käyttöoikeuksia koskevat tavoitteet. Toiveena olisi, että kaikki käyttöoikeuksien myöntäminen onnistuisi samojen AD-ryhmien kautta. AD-ryhmät pitäisi olla jatkossa suunniteltu siten, että niitä olisi jokaiselle liiketoimintayksikön alueelle ja tukifunktioille omat. Tavoitteena olisi luoda ryhmät siten, että niitä voisi olla sisäkkäin ja niiden avulla voitaisiin jakaa samaan dataan oikeudet yhdestä pääryhmästä. Oikeuksien tason mukaan pääryhmän sisällä olisi eri rooleille eri oikeuksia antavia ryhmiä. AD-ryhmien rakenne noudattelisi yrityksen liiketoiminnan organisaatio rakennetta. Manual UI:n käyttöoikeudet haluttaisiin jatkossa hallinnoida AD-ryhmien kautta. Tavoitetila on hahmoteltu kuvassa 15.

Manual UI:n ja PowerAppsin käyttörooleja tarvitaan kahta eri tyyppiä. Ryhmien perusteella pitäisi pystyä määrittämään henkilölle pelkkä lukuoikeus tai raportointioikeus. Kun palkataan uusi henkilö, tulisi hänelle pääsy automaattisesti oman tehtaan tai tukifunktion tietoihin ja roolin mukaan, joko katselu- tai raportointioikeudella.

OLAP kuutioihin ja Sustainability Databaseen tarvitsi olla myös kahden tyyppisiä rooleja, Admin tai tavallinen käyttäjä. Admin saisi oikeudet muokata kuutiossa olevaa dataa ja tavallinen käyttäjä saisi pelkästään katseluoikeuden. Henkilön käyttäjätilin luomistilanteessa tulisi hänelle samalla lailla automaattisesti oikeudet oman tehtaan tai tukifunktion tietoihin ja roolin mukaan, joko katselu- tai muokkausoikeudella. Jotta uudet taKuutiot tarvitsevat ryhmittelyä.

Power BI:ssä olisi käytössä roolit SuperUser tai tavallinen käyttäjä. Roolit antaisivat, joko katseluoikeuden tai oikeuden tehdä Power BI:ssä raportteja. Katseluoikeudella käyttäjä pääsee tarkastelemaan raportteja omalta tehtaalta tai tukifunktiolta. SuperUserilla on oikeus tehdä raportteja ja käsitellä dataa. Toisin kuin muut oikeudet SuperUser oikeutta ei myönnetä suoraan käyttäjän luomistilanteessa. Oikeus tehdä raportteja myönnetään jälkikäteen käyttäjille, joille myönnetään SuperUser rooli. SuperUser roolin voi saada vain suorittamalla roolille suunniteltu koulutus. Koulutuksen päätteeksi käyttäjän pitää vielä läpäistä testi, jolla varmistetaan, että käyttäjä on sisäistänyt koulutuksen opit. Kun käyttäjä on suorittanut SuperUser koulutuksen, menee käyttäjä IT-johtajalle hyväksyttäväksi. Mikäli IT-johtaja hyväksyy, että käyttäjälle myönnetään SuperUserin oikeudet, pyydetään IT-operaattoria lisäämään käyttäjä SuperUser AD-ryhmään. Kaikki muut hyväksynnät menevät esihenkilön kautta paitsi SuperUser.

6. EMPIIRISET TULOKSET

Tässä luvussa käydään läpi empiirisen tutkimuksen tuloksia. Tässä työssä empiirinen tutkimus toteutettiin haastatteluiden avulla. Luvussa käydään haastatteluista saadut tulokset läpi teemoittain. Ensimmäisenä aiheena on käyttäjähallinta yleisesti. Sen jälkeen pohditaan, mikä käyttäjähallinnan merkitys on yrityksille. Seuraavana tutustutaan haastateltavien kokemuksiin käyttäjähallinnan vaikutuksista tietoturvaan. Jonka jälkeen selvitetään, miten Azure AD vaikuttaa käyttäjähallinnan onnistumiseen. Azuren jälkeen pohditaan käyttäjähallinnan automatisoimista. Jonka jälkeen käydään läpi haastateltavien kokemuksia käyttäjähallinnan ongelmista. Viimeisenä tutustutaan mitä pitää huomioida, kun suunnitellaan onnistunutta käyttäjähallinnan prosessia.

6.1 Käyttäjähallinta yleisesti

IAM on jaettu identity ja access puoleen. IAMissa access puoli on enemmän pääsynhallintaa, mikä ei vaadi samanlaista räätälöintiä kuin identiteetinhallinta puoli. Identiteetinhallinta on kokonaisuutena pidemmälle vietyä, jolloin hallitaan muutakin kuin käyttövaltuutuksia. Identiteetinhallinnassa ollaan tarkemmalla tasolla ja tehdään henkilökohtaisempia määrityksiä. (H3)

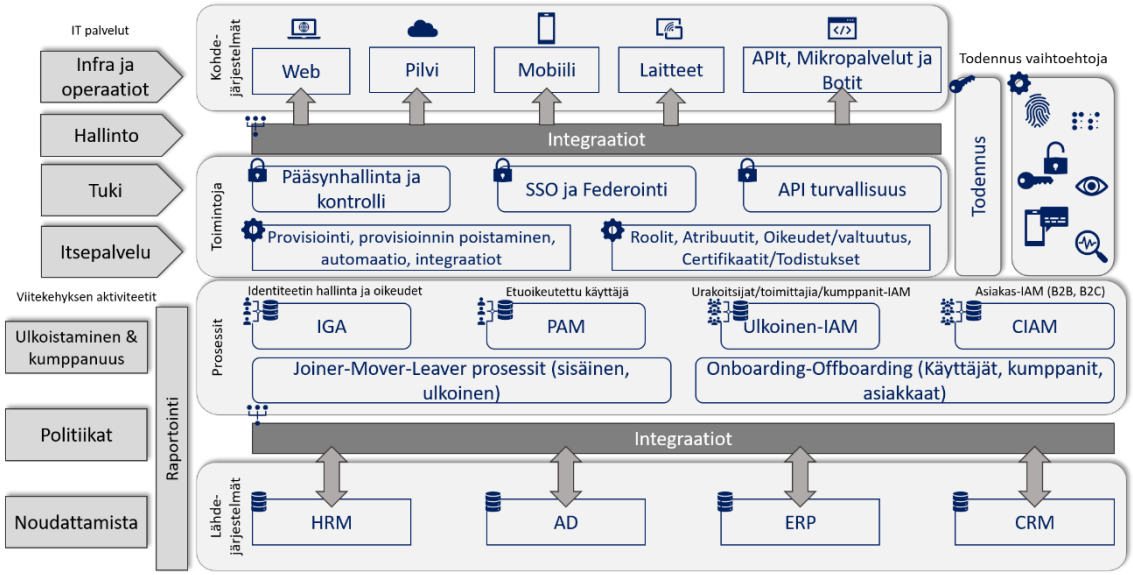
Käyttäjähallinnan prosessi riippuu pitkälti siitä, minkälaisia käyttäjiä ollaan luomassa, mutta yleensä siihen liittyy jonkinnäköiset käyttöoikeudet ja roolit. Nykymaailmassa myöskin on otettava huomioon GDPR. Kun puhutaan käyttäjistä niin yleensä puhutaan nimenomaan juuri ihmiskäyttäjistä. (H5) Pitää olla jokin paikka missä voidaan hallita käyttäjien tietoja. Pitää olla myös tapa tehdä autentikointi ja tarjota erilaisia kirjautumispalveluita. On olemassa mobiilisovellusta, websovellusta ja service-autentikaatiota autentikointiin. Käyttäjärekisterin päällä täytyy siis olla jonkin näköinen autentikointi palvelu. On yrityskohtaista, miten itse käyttäjähallintaprosessi toimii. Voi olla yrityksiä, missä täyttämällä lomakkeen self-servise portaalissa pääsee käyttäjäksi. On myös monivaiheisempia prosesseja, joissa pitää hyväksyä ja vahvistaa asiakkaan ominaisuuksia. (H4)

Käyttäjähallinnan perus prosessin runko ei yritysten kesken eroa toisistaan paljoa. Luodaan käyttäjätunnus henkilölle ennen työsuhteen alkamista. Näin mahdollistetaan, että voidaan hakea oikeuksia etukäteen tunnukselle. Aloitus päivänä aktivoidaan tunnukset ja työntekijällä olisi näin tunnukset ja oikeudet jo ensimmäisenä työpäivänä. Joitakin variaatioita on olemassa. Prosessissa saattaa olla muitakin polkuja mutta runko on lähinnä sama kaikissa tapauksissa. (H2)

Haastateltava H1 esitteli haastattelun yhteydessä PowerPoint-esityksestä muutamia dioja, joista yksi käsitteli IAMin kokonaisuutta. Kuva 16 on jäljitelty mukaillen kyseistä kuvaa. IAM on jaettu tarkoituksella eri osiin. Tällöin nousee kysymyksiä, miten kyseinen osa-alue on yrityksellä toteutettu ja miten sitä voidaan kehittää, kun mietitään elinkaarikehitystä asiakas organisaatiolla. (H1)

Sisäiset käyttäjät liittyvät HR järjestelmään, ulkoiset käyttäjät ERPiin ja asiakaskäyttäjiä säilytetään CRM järjestelmässä. HR järjestelmä on useissa tapauksissa master järjestelmä. Integraatioiden avulla voidaan viedä käyttäjätietoja HR järjestelmän, ERPin ja CRM järjestelmän välillä. Alkuperäisessä kuvassa lähdejärjestelmissä ei ollut AD:ta, mutta haastateltava oli sitä mieltä, että AD sopisi parhaiten lähdejärjestelmien kanssa samalle tasolle. (H1)

Joiner-Mover-Leaver prosessit ja Onboarding-Offboarding prosessit ovat IAM ydin prosesseja. Mover-prosessissa henkilö voi vaihtaa roolia yrityksen sisällä, mikä vaikuttaa oikeuksiin. AD-tiliä voidaan myös siirtää paikasta toiseen. Uudelleen palkkaus lasketaan myös mover-prosessiksi, jolloin henkilölle voidaan antaa jo suljetut käyttäjä tunnukset takaisin. (H2) Vaikka joiner on osa onboardingia ja leaver osa offboardingia, on ne eritelty omiksi prosesseiksi. Onboarding ja offboardin koskee myös organisaatioita. Kun tulee kokonaan uusi käyttäjä tai organisaatio, on se osa onboardingia. Kun käyttäjä tai organisaatio poistuu, on se silloin offboarding prosessi. Kyseessä on onboarding tai offboarding, koska ne ovat omia tapahtumaketjuja. Joiner-Mover-Leaver ajatellaan koskevan enemmän käyttäjiä ja muutoksia käyttäjäkunnassa. (H1)



Kuva 16 IAM kokonaisuus (mukaillen H1 näyttämää kuvaa)

Onboarding prosessi lähtee siitä, kun tulee uusi ihminen rooliin ja hänen esihenkilönsä huolehtii, että identiteetti tulee AD:hen perustettua oikein. Sen jälkeen kaikki muutokset

tulisi mennä esihenkilön kautta. Offboarding on onboardingia isompi ongelma. Kun rooli muuttuu niin usein mitään ei tapahdu. Vanhat oikeudet ja pääsyt jäävät voimaan. (H6)

IAMin ydin on käyttäjäidentiteettien, attribuuttien ja roolien käsittelyssä. Tätä osaa IA-Mista kutsutaan identiteetinhallinnaksi. Ytimessä on organisaation omat käyttäjät, mutta mukana myös ulkoiset käyttäjät, alihankkijat, toimittajat, jotka näkyvät infrassa. Laatikot IGA, PAM, Ulkoinen-IAM, CIAM eivät tarkoita, että ne ovat erillisiä järjestelmiä, vaan pikemminkin erilaisia käyttötapauksia. PAM käyttötapauksissa on riskejä tai enemmän oikeuksia, jolloin identiteettejä ja oikeuksia täytyy käsitellä erityisemmin ja tarkemmin. PAMille käytetään usein ihan omaa ratkaisua, mutta samakin tuotteella pystyy toteuttamaan IGA ja PAM. CIAM toimii asiakasmaailmassa. (H1)

Provisioinnit ovat oleellinen osa identiteettihallintaa. Provisiointi voi olla molempiin suuntiin, lähdejärjestelmiin tai kohdejärjestelmiin. Jatkuvia sisäisiä prosesseja ovat muun muassa roolien, attribuuttien, käyttöoikeuksien, sertifiointien ja valvonnan ylläpito. Tarkastus prosessien avulla tarkastetaan, että käyttäjät ovat heitä keiden heidän pitää olla ja käyttöoikeudet ovat kohdillaan. Tarkastusta tapahtuu erityisen paljon PAMin puolella, mutta myös muilla alueilla. Muita keskeisiä ovat pääsyhallinta, SSO, federointi ja yhä enemmän API hallinta sekä API käyttötapaukset. Nykyään kun rakennetaan sovelluksia, niin hyödynnetään APIa. Tunnistaminen on osa pääsynhallintaa. Tunnistamiselle on useita eri mekanismeja. (H1)

IAMin logitieto tuottaa tärkeää dataa käyttäjistä, valtuuksista ja pääsyistä. Tätä dataa hyödynnetään muun muassa raportoinnissa, tietoturvassa ja liiketoiminnan kehittämisessä. Datalla myös pystytään vastaamaan ulkoisiin raportoinnin vaatimuksiin ja mitä politiikkoja noudatetaan. (H1)

IAM on osa IT-hallintoa, joka voidaan hoitaa sisäisesti ja ulkoisesti. Sisältää IT-strategioita, tukiprosesseja, hallintoja ja itsepalveluita. Itsepalvelut ovat usein läsnä IAM puolella, koska jos kyseessä on tuhansia tai jopa miljoonia käyttäjiä, ei IT-hallinto pysty manuaalisesti tekemään kaikkea. (H1)

Käyttäjähallinta lähtee aina siitä, että tulee uusi työntekijä tai työntekijä vaihtaa uuteen rooliin. Yrityksellä tulisi olla onboarding prosessi, jolla käyttäjän pitäisi saada pääsyt roolin kannalta relevantteihin paikkoihin. Käyttäjän roolin ja vastuiden muuttuessa pitäisi pystyä ylläpitämään oikeuksia. Uusia IT-projekteja ja palveluita tullessa pitäisi hyödyntää käyttäjähallinnan sabluunoita ja hyödyntää samoja ryhmiä. Pääsyt tulisi jakaa ryhmien kautta eikä niin, että lisättäisiin yksitellen käyttäjälle oikeuksia. Tällöin käyttäjähallinta olisi jotenkuten suoraviivaista ja yksinkertaista. (H6)

6.2 Käyttäjähallinnan merkitys yrityksille

Riippuu paljon yrityksestä, miten käyttäjähallinta vaikuttaa sen toimintaan. Voi olla kyseessä yritys missä on paljon regulaatiota ja tilintarkastaja vaatii paljon eri asioita, eli toiminta on tarkasti säänneltyä. Tallaisessa tapauksessa on paljon hyötyä, että muutokset saadaan kiinni helposti. Pystytään säännöllisesti katselmoimaan käyttöoikeuksia ja voidaan olla varmoja siitä, että kellä on ollut oikeus tehdä mitä milläkin ajan hetkellä. Säätelyä on enemmän muun muassa pankeilla, terveydenhuollolla ja vakuutusyhtiöillä. (H2)

Yrityksissä, joissa ei ole niin paljon säätelyä, niin käyttäjähallinnalla voidaan helpottaa toimintaa paljon. Oikeuksien saaminen on helpompaa. Käyttäjähallinta hankkeella voidaan saavuttaa jonkin asteen kustannus säästöjä. Yleensä vaaditaan, että pidettäisiin huolta siitä, että kenellä on mitäkin käyttöoikeuksia ja mihinkin järjestelmään. (H2) Käyttäjähallinnassa tärkeää on, että pystytään hallinnoida, kenellä on pääsy dataa. On tärkeää, että pystytään tehokkaasti rajoittamaan pääsyjä. (H6)

Hyvä politiikka on, että käyttäjille annetaan vain, mitä käyttäjä tarvitsee. Käyttäjä pääsee vain, minne tarvitsee päästä. Sekä käyttäjä pystyy tekemään vain asioita, joita heidän kuuluu tehdä, jotta suoriutuvat omista töistään. Jos laiminlyödään käyttäjähallintaa tai sitä ei ole, niin edellä mainitut tekijät vaarantuvat. (H8) Pitää pystyä kuvaamaan miten dataa käsitellään ja kenellä on pääsy siihen. Ja käytettävyyden näkökulmasta saadaan oikeat työkalut oikeille ihmisille jaettua helposti. Ettei käyttäjähallinta olisi tapauskohtaista oikeuksien jakamista. (H6)

Kun henkilö tulee yritykseen työntekijäksi, pitäisi tilin tulla voimaa vasta työsuhteen ensimmäisenä päivänä, eikä yhtään aikaisemmin (H5). Mikäli ei ole minkään laista käyttäjähallintaa, ei myöskään saada ollenkaan käyttäjiä. Yrityksellä täytyy olla kontrolli mitä palveluita käyttäjät pystyvät käyttämään. Pienissä muutaman hengen yrityksissä voi toimia systeemi, jossa kaikki palvelut ovat kaikkien käyttäjien saatavilla. On myös mahdollista tehdä lokaalit tunnukset palveluille. Yrityksen koon kasvaessa tämä ei kuitenkaan toimi. Järjestelmiä ja käyttäjiä on enemmän yrityksen koon kasvaessa, jolloin tarvitaan keskitetty paikka hallita tunnuksia ja käyttäjiä. Tällöin voidaan luoda ja hallita mihin käyttäjä pääsee. (H4)

Henkilön lähtiessä yrityksestä, pitää tili deaktivoida. Monesti on huomattu, että poistaminen ole mahdollista. Tiliä ei voida niin vain poistaa, mutta on tärkeää, että se deaktivoidaan oikein. Yhdellä tilillä saattaa päästä asiakkaidenkin tietoihin käsiksi, mikäli tiliä on käytetty asiakkaan ympäristöissä. Tämä luo pahan tietoturvaongelman, koska jos menetetään yhden tilin hallinta, niin saattaa useamman yrityksen tiedot päätyä vääriin käsiin.

(H5) Kun työsuhde loppuu, kaikki käyttäjätunnukselle linkitetyt oikeudet päättyy, kun tili disabloidaan. Ongelmana on, jos käyttäjä on luonut omia tunnuksia, työsuhteen päättyessä oikeuksia ei välttämättä osata poistaa oikeista paikoista. Palvelun ylläpitäjän pitäisi käydä käyttäjät aina läpi ja varmistaa saako heillä olla oikeudet edelleen palveluun. Mitä enemmän on väkeä ja palveluita sitä mahdottomampaa asiaa on hallita. (H4)

Jos käyttäjähallinta on huonosti toteutettu eikä skaalaudu konsernilta liiketoimintayksiköille, vaikuttaa se sovellusten käytettävyyteen. Jolloin erilaisten ratkaisuiden implementointi ja ulosrullaaminen muille liiketoimintayksiköille konserni tasolla on hankalaa. (H6)

Käytäntö on kirjavaa, miten päästetään ulkoisia käyttäjiä ympäristöihin. Osa luo vierailija tunnukset ja osa jakaa oikeudet jo olemassa olevalle sähköpostitilille. On otettava huomioon, että nykyään on olemassa MFA-standardi, mikä tulisi olla käytössä. MFA:ssa on eri tasoja. Heikoimpia on, kun koodi lähetetään sähköpostin kautta. Ongelmana on se, että jos sähköposti on jo murrettu niin silloin väärä henkilö saa koodin haettua sähköpostista. Toinen on tekstiviesti, jossa koodi tulee tekstiviestillä puhelimeen. Kuitenkin tämän pystyy murtamaan soittamalla asiakaspalveluun ja pyytämällä viestien siirtoa toiseen numeroon. Mikäli henkilö on tarpeeksi uskottava ja asiakaspalvelija uskoo tätä, joutuvat koodit silloinkin vääriin käsiin. MFAssa turvallisin tapa on käyttää siihen luotuja sovelluksia. Sovelluksessa on koodi, mikä vaihtuu kolmenkymmenen sekunnin välein. (H5)

6.3 Käyttäjähallinnan vaikutus tietoturvallisuuteen

Isoin riski tietoturvalle on käyttäjä eli mitä huonompi käyttäjien hallinta niin sen enemmän on riskejä. Haastateltava 8 koki oman kokemuksen perusteella, että tämä on verrannollinen eli mitä parempi käyttäjien hallinta niin sitä vähemmän tulee "ohi osumia". (H8) Tapa käyttää, hyväksyä ja katselmoida käyttöoikeuksia vaikuttaa tietoturvallisuuteen. Työkalu itsessään ei paranna tietoturvallisuutta. Tietoturvallisuuteen vaikuttaa paljon käytössä olevat prosessit. Käyttäjä on aina heikoin lenkki. (H2)

Lokaaleita tunnuksia käytettäessä, henkilöllä saattaa olla pääsy joihinkin palveluihin työsuhteen päätyttyä. Mikäli vanhalla työntekijällä on tarvetta saada jotain tuhoa aikaiseksi, on se mahdollista, mikäli käyttäjätunnukset toimivat työsuhteen päättymisenkin jälkeen. Työnantajaa vaihdettaessa voidaan saavuttaa kilpailuetua, mikäli on edelleen pääsy vanhan työnantajan asiakasrekisteriin. Tietokannoissa voi olla lokeja, joiden perusteella voidaan selvittää ketkä ovat käyneet tietoja tarkastelemassa. Esimerkiksi potilastietokantaan voi olla tiettyjä lakeja tietojen tarkastelun suhteen. Jos tehdään erilaisia virityksiä uusien ja vanhojen järjestelmien välille, ei voida aina olla ihan varmoja tieturvallisuuden onnistumisesta. Turhat pääsyt vaikuttavat tietoturvallisuuteen. (H4)

Haastateltava 1 pohti alkuun käyttäjähallinnan hyötyjä tietoturvallisuuteen riskien sijaan. Digitalisointi toimii paremmin ja elämä on helpompaa tai tehokkaampaa käyttäjille. Ihan sama onko käyttäjä oma, kumppanin tai asiakkaan, käyttäjillä tulee olla pääsy sinne, minne tarvitsee ja eikä paikkoihin mihin ei tarvitse. Käyttäjähallinta tarjoaa hyvän pohjan kumppanuuksien rakentamiselle, kun on turva ja luottamus siihen ratkaisuun, jolla voidaan tehdä digitalisoituja prosesseja kumppaneiden kanssa. Hyvin toteutettu asiat auttavat keskitetyn tiedon hyödyntämistä, kun ei tarvitse taistella samojen murheiden kanssa eri järjestelmissä. (H1)

Käyttäjähallinnan hälytyskelloja voivat olla seuraavat. Uusi palvelu otetaan käyttöön ja huomataan ettei sen käyttö suju. Uusien palveluiden tuominen käyttöön voi olla hankalaa, koska ei saada kaikkia ominaisuuksia toimimaan oikein. Käyttäjät joutuvat odottamaan liian kauan, että saavat oikeuksia. Käyttöoikeus prosessit voivat olla liian hitaita tai toimimattomia. Ulkoisten käyttäjien rekisteröinti ei toimi, mikäli IAM prosessit eivät ole kohdallaan. Uusien käyttövaltuutuksien saaminen voi olla hidasta, kun tulee uusi projekti, jolle oikeuksia pitäisi jakaa. Palvelu omistajan tai tiimin vetäjän täytyy tarkistaa ovatko käyttöluvat kohdallaan. Ongelmana on, että prosessit ovat hitaita. Muutokset eivät onnistu koska tieto ei ole kohdallaan. IAM ei toimi, jos arkkitehtuuri on hajallaan tai vaikka vanhalla teknologialla tehty. Single sign-on puute aiheuttaa ongelmia, jolloin käyttäjät joutuvat kirjautumaan kaikkialle erikseen. Erillisissä järjestelmissä ei välttämättä ole tieto ajan tasalla. (H1)

On kriittistä, kuka pääsee ja mihin käsiksi. Kun noudatetaan kaikkia säädöksiä, ei esimerkiksi ylimääräiset käyttäjät pääse GDPR tietoon käsiksi tai käyttäjät näe sellaisia tietoja mitä heidän ei pitäisi nähdä, mikä on äärimmäisen tärkeä asia. Käyttäjiä ei saa päästää sellaisiin paikkoihin missä käyttäjät pystyisivät tekemään vahingossa tai tarkoituksella paljon tuhoa. On riskienhallintaa, olla jakamatta pääsyjä kuin karkkeja. Pääsyjä tulisi jakaa vaan ja ainoastaan todelliseen tarpeeseen. Tietoturvallisuuden kannalta tärkeää on, että tiedetään, miten tieto liikkuu ja kenellä on pääsy, sekä auditoidaan tätä. Auditointia auttaa, kun on hyvin raportoidut käyttäjähallinnan prosessit ja, kun järjestelmät toimivat niin kuin pitää. Tietoturvaan riskejä luo käyttäjät, minkä takia ei päästetä käyttäjiä turhaan sinne, minne niiden ei pitäisi päästä. (H6)

6.4 Azuren rooli käyttäjähallinnassa

Isoissa yrityksissä ulkoisten järjestelmien määrä on valtava, jolloin esimerkiksi 1990-luvulla käyttöönotetut järjestelmät eivät välttämättä tue uudempia autentikointi palveluita. Uudempia teknologioita voidaan käyttää kuitenkin siltoina vanhojen ja uusien palveluiden välillä. (H4)

Azure ei itsessään tarkoita, että IAM tai käyttäjähallinta olisi hallussa. Täytyy tietää, miten Azurea hyödynnetään ja millä työkaluilla. Vaikka ottaisi kolmannen osapuolen IAM ratkaisun käyttöön, on Azure keskeinen niissä aina. Azure AD ja AD ovat keskeisiä lähdejärjestelmiä. Ennen Azurea oli AD, joka oli vastaavassa asemassa. Ei ole yhtä tapaa ratkaista käyttäjähallintaa Azurella. Microsoft on hyvä IAM ratkaisu mutta se ei ole ainoa. Se on hyvä mutta se on valinta kysymys mitä alustaa ja millä arkkitehtuurilla lähdetään ratkaisemaan. (H1)

Azure AD:hen usein peilataan käyttäjät perinteisestä AD:sta. Azure AD:lta löytyy premium ominaisuuksi. Azure AD on vakaa ja hyvin toimiva työkalu. (H5) Azure AD on hyvä yrityksille, joiden strategiassa kaikki tapahtuu Azuren ympärillä. Azuren hyväpuoli on, että kolmannen osapuolen sovellukset ja palvelut pystyvät hyödyntämään Azurea. (H1)

Yrityksen tapauksessa oli vaikeaa kommentoida mikä on työkalun osuus. Enemmän syynä on puutteelliset prosessit sekä liiketoimintayksikön että IT puolella. Ongelmat eivät ole itse työkalusta kiinni. (H6)

Azure AD koettiin olevan toimiva työkalu. V1 kohdalla ongelma oli, ettei menty protokollan mukaan muttei standardienkaan mukaan, säädettiin sinne jotain omaa. V2 palvelun kohdalla tehtiin ryhtiliike, minkä jälkeen on näyttänyt siltä miltä standardien mukaan pitäisikin näyttää. Kun tuntee protokollat ja ottaa käyttöön Azure AD:n huomaa termien vaihtuvuuden. Azuren synkronointi palvelut on-premises ja pilven välillä ovat hyödyllisiä. (H4)

6.5 Käyttäjähallinnan automatisointi

Käyttäjähallinnan automatisointi on vain integraatio esimerkiksi käyttäjän luontia varten ja tietojen siirtoon. Integraation keinoin on automatisoitu asioita, mitä olisi muuten viety käsin. (H2) Automaation avulla yleinen hallintaprosessi muuttuu helpommaksi. Myös prosessit muuttuvat niin, että IT henkilöiden työtehtävät muuttuvat selkeämmiksi. Jos roolit ovat kunnossa, niin oikeuksien antaminen voidaan muuttaa automaattiseksi. (H7)

Kun työntekijä tulee taloon, hänelle luodaan käyttäjätili ensimmäisenä esimerkiksi HR-järjestelmään (H2). Tyypillisimmin automatisoidaan käyttäjätilin aktivointi. Kun tiedetään, että tulee uusi työntekijä, saatetaan tili luoda etukäteen mutta aktivointi suoritetaan vasta, kun on ensimmäinen työpäivä. (H5) Esimerkiksi HR-järjestelmästä voidaan tehdä ilmoitus, kun luodaan uusi käyttäjä. Voidaan kuunnella jonoja, kun käyttäjä siirtyy jono palveluun. Järjestelmästä voidaan luoda näin reaaliaikainen. (H4) Deaktivointi voi olla samalla tavalla järjestetty kuin aktivointi. Kun tiedetään viimeinen työpäivä, niin tilin deaktivointi

kirjataan järjestelmään ylös ja integraatio hoitaa deaktivoinnin viimeisenä työpäivänä. (H5)

Jokaisella yrityksellä tulisi olla perustyökalupakki, mikä sisältää ohjelmat ja datan. Näin käyttäjienhallinnan automatisointia mietittäessä kaikki ohjelmien provisiointi, pääsy dataan ja datan oikeuksien provisiointi, voidaan laittaa kaikki samaan pakettiin. Tämä yksinkertaistaa käyttöönottoa, sekä onboarding ja offboarding prosessia huomattavasti. (H8) Jotta automatisointi voi onnistua, on oleellista määritellä järjestelmien välillä vaihdettavat tiedot. Hyvä idea on tehdä esimerkiksi taulukko, jossa käydään läpi mitä parametrejä välitetään. Valmiilla liittimillä voidaan helposti muodostaa integraatioita järjestelmien välille. Täytyy ymmärtää, mitä tietoja pyritään vaihtamaan, jotta käyttäjähallintaa voidaan automatisoida. Kaikkia kohdejärjestelmiä ei välttämättä kannata automatisoida, mikäli on esimerkiksi pieni määrä käyttäjiä kohdejärjestelmässä. (H3)

Tietojen synkronointi eri järjestelmiin voidaan automatisoida. Kaikki järjestelmät ei välttämättä pysty käyttämään Azure AD:ta. Tällöin muutoksien täytyy liikkua järjestelmien välillä integraatioiden avulla. (H5) On tärkeitä lähdejärjestelmiä, joihin tulee uusi työntekijä tai kumppani. Muutoksen aiheuttamana aiheutuu triggeröinti, minkä tarkoituksena on synkronoida tiedot kaikkiin järjestelmiin, jotta tiedot ovat ajan tasalla. Myös toiseen suuntaan eli kohdejärjestelmiin on provisiointia. Monet palvelut tarvitsevat identiteetti tiedon. Osa palveluista pystyy hyödyntämään sen lennosta, jolloin tieto tulee pääsynhallinasta tokenin mukana. Jolloin hyödynnetään sitä tietoa. On myös olemassa palveluita, jotka tarvitsevat etukäteen tapahtuneen provisioinnin. Tällöin käyttäjän tiedot täytyvät olla etukäteen vietynä, jotta pystytään kirjautumaan. (H1) Automatisoinnin kohteena voi olla provisiointi tiketti, jonka robotti hoitaa. Automatisoinnille on paljon vaihtoehtoja. Ei ole mitään tyypillistä tapaa automatisoida käyttäjähallintaa. (H2)

Integraatio voi viedä käyttäjän tiedot Azure AD:hen, jossa työntekijälle luodaan käyttäjätili. Myönnettyä rooli käyttäjälle voidaan identiteetti viedä tiettyyn ryhmään, josta se saa oikeudet. Perinteisiä integraatio menetelmiä käyttäen voidaan tehdä prosessista erittäinkin yksinkertainen. (H4) Lisenssien ja pääsyjen automatisointi on kriittinen, mikä onkin kohdeyrityksellä jo jollain tolalla. AD-tietojen perusteella pitäisi pystyä allokoimaan käyttäjiä ryhmiin. (H6)

Voidaan myös automatisoida federointi kolmannen osapuolen pilvipalveluihin. Tällaisia yrityksillä käytössä olevia voi olla esimerkiksi raportointityökalut. Federoinnit ja pääsynhallinta pilven sisällä voidaan automatisoida. On suositeltavaa automatisoida prosessia niin pitkälle kuin on vain mahdollista. (H8) Riippuu ihan yrityksestä ja että mitä sattuu

olemaan käytössä ja mitä halutaan automatisoida. Riippuu tuotteesta mitä ollaan ottamassa käyttöön ja organisaatiorakenteesta. Joissakin tapauksissa saattaa olla esimerkiksi niin, että halutaan kaikkien käytössä olevien järjestelmien välille integraatiot. Jolloin voidaan joutua toteuttamaan esimerkiksi 500 integraatiota. Jos organisaation rakenne on sellainen, että integraatioita voidaan kopioida, on integraatiot helppo toteuttaa. (H2)

Yrityksellä on IAM kautta automatisoitu paljon federointeja työpaikan sosiaalisiin medioihin, jotka ovat pilvessä, sekä muita pilvi työkaluja. Automatisointia on tehty myös omiin webbisovelluksiin ja jossain maissa jopa omaan ERP-järjestelmiin. Yrityksellä on tarkoituksena lisätä automatisointiin mobiililaitteiden sovellukset ja työasemakohtaiset sovellukset. Kaikki muu oleellinen tullaan myös automatisoimaan, kuten käyttäjien pääsy omiin tietoihin sekä käyttäjän tieto mihin kaikkialle hän pääsee. (H8)

Käyttäjähallinnan automatisoinnista on yrityksille hyötyä. Aina kun tulee tai lähtee työntekijä, niin automatisointi huolehtii, että työntekijällä on perus pääsy ja perus työkalut päivittäiseen työntekoon tai kun käyttäjä poistuu talosta niin tarvittavat käyttöoikeudet poistetaan. Varsinkin pilvi puolella auttaa, kun ei ole haamutunnuksia ja lisenssejä häiritsemässä prosesseja sekä nostamassa käyttäjämääriä. (H8) Hallintanäkökulmasta jää jälki kaikesta mitä ollaan tekemässä. Milloin on haettu oikeus, onko sen joku hyväksynyt ja parhaimmassa tapauksessa se vielä auditoidaan, kun käyttöoikeuksien katselmointi on toteutettu esimerkiksi kerran vuodessa. (H2)

Kustannussäästöjä koituu, kun teknistä tukea ei tarvita yhtä paljon käyttäjän itse hakiessa oikeudet. Tietoturva paranee, kun tiedetään kenellä ja mitä oikeuksia on kohdejärjestelmiin. (H2) Automatisointi myös auttaa siihen, ettei unohda. Käyttäjätietojen synkronointi isolle käyttäjämäärälle olisi todella raskasta. Joten on tärkeää, että se menee automaattisesti joka puolelle. (H5) Yrityksessä koettiin, että eniten hyötyä esiintyi, kun työtaakkaa oli vähemmän ja prosessi on selkeämpi. Aina on hyvä asia, kun manuaalinen työ vähenee. (H8) Mikäli prosesseja automatisoidaan, voidaan käyttäjähallintaprosessia hoitaa pienemmällä porukalla (H7).

Automatisointikaan ei ratkaise kaikkia ongelmia ja tuo jopa omia ongelmia mukanaan. Automatisoidessa järjestelmät eivät välttämättä aina toimi odotetusti. Voi tulla jokin virheellinen syöte HR tiedoista, jolloin tiedoista palautuu esimerkiksi vain puolet tiedoista. (H2) Synkronoinneissa voi tulla ongelmia, jos on ristiriitaisia tietoja eri järjestelmissä (H5). Jos tietoja on syötetty väärin lähdejärjestelmiin, siirtyy väärää tietoa myös kohdejärjestelmiin. (H3)

Isoin riski on, että automatisoinnin yhteydessä annetaan vääriä oikeuksia (H8). Automaatiossa voi käydä jonkin näköisiä suunnittelu virheitä tai jonkin prosessin kohdalla

määritellään käyttäjille liikaa oikeuksia (H6). Jos automaatiolla tehdään muutoksia, se vaikuttaa kaikkiin sen käyttäjiin, ketkä ovat automatisaation piirissä. Kun tehdään isoja virheitä, niin haitta vaikutuskin on iso automaatiossa. Automaatiossa pitääkin olla hyvin tarkka testauksessa ja määrittelyssä. (H8)

Pahimmassa tilanteessa saattaisi poistua jotain mitä ei pitäisi (H2). Jokin tehtävä saattaa jäädä tekemättä, mikäli esimerkiksi yölle ajastettu ajo ei pystykään suoriutumaan. Sama riski voi kuitenkin esiintyä myös käsin tehtynä. Automatisoinnissa paras tapa on monitoroida ja käyttää hälytysjärjestelmää, jolloin saadaan ilmoitus siitä, että jokin menee pieleen. (H5) Jos tunnistetaan, että on kriittistä dataa, kannattaa tehdä erikoisryhmiä, jotka hoidetaan tarkemman prosessin mukaan ja tarkemman hyväksymisketjun kautta, jolloin ei lipsahda vahingossa liikaa oikeuksia. (H6)

Yrityksen tuotanto puolella ei ole esiintynyt riskejä, sillä riskit ovat huomattu jo testauspuolella. Kaikki mitä on tehty, on hyvin testattu. Iso riski on, kun automatisoidaan, ettei ihmisillä ole tarpeeksi tietotaitoa sekä ymmärrystä aiheesta, miten automaatio tehdään. Yrityksellä esiintyi testausvaiheessa ongelmia esimerkiksi, kun käyttäjällä annettiin toisessa automaatiossa oikeudet ja toisessa ne otettiin pois. Tämä aiheutti, että testiympäristössä ruvettiin antamaan oikeuksia manuaalisesti, mikä kuormitti resursseja. Testipuolella huomattiin myös, kun automaatiossa ei ollut tarpeeksi tarkat säännöt, niin testikäyttäjä sai myös väärään datapaikkaan oikeuksia. Laveat säännöt toivat erilaisia riskejä. (H8) Automatisoinnissa riskinä on myös, että käyttäjät saattaisivat nähdä laajemmalta alueelta tietoja. Jos säännöt on tehty väärin, on mahdollisuus, että käyttäjä pääsee esimerkiksi toisen tytäryrityksen tietoihin. Kyseessä on kuitenkin sama konserni, minkä takia ongelman ei pitäisi olla niin vakava. (H7)

6.6 Käyttäjähallinnan ongelmia

Monesti organisaatiot ovat havahtuneet siihen, että käyttäjähallinta on liian hankalaa tai siihen menee liikaa aikaa. Omat ja ulkoiset käyttäjät saattavat hermostua siihen, että oikeuksia ei ole eikä näin ollen päästä tarvittaviin järjestelmiin. Pahimmassa tapauksessa dataa pääsee sellaisten henkilöiden käsiin, kenellä ei pitäisi olla oikeuksia. Kun tulee uusia palveluita, jotka ovat osa digitalisointi polkua, saatetaan havahtua olemassa oleviin ongelmiin. IAM on iso osa digitalisointia. IAMn täytyy olla kunnossa, jotta voidaan muilla segmenteillä edetä. Harvemmin nykyään enää on tilanteita, että ei ole mitään käytössä. (H1)

IAM projekteissa on haasteita paljon. IAM on mielenkiintoinen projekti, jos vertaa muihin IT-projekteihin. Integraatioita tarvitaan melkein joka järjestelmään mitä asiakkaalta löytyy. Täytyy huomioida liiketoiminta prosesseja ja mitä vaiheita henkilöillä on yrityksessä, esimerkiksi vanhempain vapaat ja sairasloma. Mitä tunnuksille käy poissaolojen aikana. Miten siinä tilanteessa toimitaan, kun henkilö lähtee yrityksestä mutta tuleekin hetken päästä takaisin. (H2) Toistuva haaste yrityksien sisäisissä järjestelmissä on, ettei ole RBAC-malli tai ei ole DRBAC-mallia, mitä voitaisiin käyttää käyttäjän provisiointiin ja deprovisiointiin eri järjestelmien välillä. (H8)

Aika usein asiakas olettaa, että ollaan valmiita ottamaa käyttäjähallinta käyttöön ja, että kyseessä on vain tuote, mikä otetaan käyttöön ja sillä ratkaistaan kaikki ongelmat. Yleensä se ei ole niin. Riippuen siitä, kuinka kypsiä ollaan uuden prosessin vastaanottamiseen, onko asiakkaalla aikaisemmin ollut vastaavaa järjestelmää. Jos asiakkaalla on aikaisemmin ollut vastaava järjestelmä ja on kyseessä kypsä organisaatio, vastaavia ongelmia ei esiinny. Esimerkki tilanteessa yritettiin tehdä käyttöönottoa asiakkaalle, kunnes saatiin asiakas ymmärtämään, ettei kyseistä projektia voida tehdä. Projektissa ei olisi ollut asiakkaallekaan mitään järkeä. Asiakas tajusi asian ja päätti ottaa kahden vuoden aikalisän, minkä jälkeen yritti uudelleen. IAM projekteissa täytyisi olla ajatusmalli, jossa ymmärretään, että kyseessä ei ole pelkän teknologian käyttöönotto vaan paljon muutakin. Pitää olla prosessit kunnossa. Kun prosessit ovat jollain tasolla hallussa, niin seuraava ongelma on organisaation data. Integraation tekeminen järjestelmien välille on helppoa. Jokaisella organisaatiolla on oma käyttötapa datalle. (H2)

Tekniset integraatiot loppupelissä on aika simppeleitä. Integraatiota varten käytössä on rajapinta, jonka kautta jutellaan järjestelmälle ja aika usein saattaa löytyä valmis yhteys, jota voidaan hyödyttää. Integraatioissa tekniikka osuus on kaikista helpoin. Haastavinta IAM projektissa kuitenkin on se kaikki muu tekniikan ympärillä. Kyseessä on iso muutos organisaatiossa, jos ei ole aikaisemmin toteutettu vastaavaa. Täytyy olla selvillä, miten jatkossa asiat hoidetaan ja mitä halutaan automatisoida. Organisaation koosta riippuen täytyy tiedottaa, kouluttaa ja toteuttaa muutoshallintaa, joista syntyy organisaatiolle iso työurakka. IAM projektia ei tulisi nähdä pelkkänä teknisenä projektina. Haastateltava 2 arvioi, että 30 prosenttia olisi teknistä tekemistä ja 70 prosenttia kaikkea muuta. (H2)

Suurin osa ongelmista nousee datan laadusta. Dataa hyödyntäessä suurimmat ongelmat yleensä johtuvat datan puutteellisuudesta tai päällekkäisyydestä. Se tekee automaatio puolesta hankalampaa toteuttaa. Usein esimerkiksi käyttäjämäärä on niin suuri, että se hallinnointi käsin olisi mahdotonta. Kaikki tietysti aina riippuu järjestelmässä ja mitä sillä voi tehdä. AD on hyvä hallintatyökalu. Tekniset vaikeudet tulee siitä eteenpäin. Ongelmana on muutokset eri järjestelmiin, jotka ei pysty toimimaan AD:n kanssa. (H5)

Käyttäjien vaihtaessa työtehtävää yrityksessä ja vanhojen oikeuksien jäädessä käyttäjälle roikkumaan on tyypillisin oire, josta huomataan, että prosessit eivät ole kohdallaan. Tässä esiintyy riski, jos käyttäjä on siirtynyt toisen yrityksen palvelukseen, ja pääsee edelleen vanhan yrityksen tietoihin käsiksi. (H1) Käyttäjien oikeuksien poistamiselle pitäisi olla prosessi. Jos poistuu asiakkaan töistä, niin siitä pitäisi olla ilmoitus asiakkaalle. Kun taas on kyse sisäisestä muutoksesta, pitäisi muutoksella olla olemassa sisäisesti käytössä oleva prosessi. Oikeuksien sitominen rooliin, auttaisi vaihtamaan vanhat oikeudet uuden roolin oikeuksien mukaisiksi. (H5) Kun pystyy mahdollisimman hyvin pitämään käyttäjähallinnan roolipohjaisena, niin ongelman pystyisi ratkaisemaan (H6). Hyvä vaihtoehto on dynaaminen roolipohjainen käyttäjähallinta. Se perustuu esimerkiksi yrityksen osastoon, lokaatioon (maa, toimipiste, paikka toimipisteen sisällä). Jos jokin näistä muuttuu, niin automaatio hoitaa oikeudet ja työkalut taustalla kuntoon, eli vanhat oikeudet poistetaan ja uudet otetaan käyttöön. (H8)

Kyseisellä yrityksellä on paljon järjestelmiä, joihin kirjaudutaan erillisillä tunnuksilla eikä ole single sing-on käytössä tai muuta aktiivista integraatiota AD:hen, minkä takia tunnuksia jää voimaan ja roikkumaan työsuhteen päätyttyä. Ongelma on ratkaistu siten, että vain firman sisäverkosta pääsee sovelluksiin. Kun ei ole enää CNS tunnuksia voimassa, niin vanha työntekijä ei pääsisi kirjautumaan sisälle. Muitakin reittejä on kuitenkin olemassa. (H6)

Kohdeyrityksellä isoin ongelma on ollut, että on puuttunut iso kuva käyttäjähallinnasta. Ei ole mietitty miten käyttäjähallinta yleisesti toteutettaisiin. Käyttäjähallinta on ollut aina vain projekti kohtaista, jolloin on mietitty vain, miten kyseisen sovelluksen kohdalla toimitaan ja luotu vain sen hetkiset ryhmät. Hetken ajan päästä on huomattu, että on viisi saman tyyppistä ryhmää, jotka on heikosti dokumentoitu. Käyttäjähallinnassa on vuosikausien kerrostumaa havaittavissa. Ollaan joskus aloitettu tietyllä tavalla, jota on vain seurattu. Ei olla pysähdytty miettimään, miten käyttäjähallinta kokonaisuudessa pitäisi toteuttaa. Projektien yhteydessä on tehty käyttöönotettavalle sovellukselle käyttäjähallinta, mikä on ollut pakko toteuttaa jotenkin. (H6)

Ongelma on, että ei ole muodostunut käytäntöä, miten käyttäjäoikeuksia annetaan. Jokainen tapaus hoidetaan erikseen, eikä olla pohdittu isompaa kuvaa. Yritykseltä saattaa puuttua käyttäjäryhmät kokonaan. Oikeuksia annetaan vaan koska niitä pyydetään. Prosessin puuttumisen takia käyttäjiä saattaa jäädä lojumaan. Fiksusti tehtynä käyttäjät lisättäisiin käyttäjäryhmiin, joista käyttäjät saisivat oikeudet. Kun käyttäjä poistuu tai siirtyy muualle, niin käyttäjä poistetaan ryhmästä, jolloin ei tarvitse lähteä etsimään yksittäistä käyttäjää eri paikoista. (H5) Kohdeyrityksen nykyisessä systeemissä hoidetaan jokainen pääsyoikeus niin, kuin pitäisi hoitaa poikkeustilanteet. Poikkeustilanteille jäisi enemmän

aikaa hallinnoida automaation hoitaessa muut. AD:ssa tulisi olla roolit ja hyvin mietityt ryhmät, niin pystyttäisiin antamaan pääsyjä kaikkiin palveluihin eikä niin, että olisi hirveä nippu palvelu spesifejä ryhmiä. (H6)

Tällä hetkellä käyttäjähallinnan ylläpito ei toimi lainkaan kohdeyrityksessä. Ryhmä määrästä on tullut niin massiivinen. Operaattori taso ei osaa käyttäjähallintaa ollenkaan, koska prosessi on mennyt niin monimutkaiseksi vuosia sitten. Tällä hetkellä on 1line ja 2line operaattorit Service Deskissä, jotka laittavat ihmisiä oikeisiin ryhmiin pyynnön perusteella. Henkilö pyytää oikeuksia ja esihenkilö hyväksyy, minkä jälkeen henkilö laitetaan ryhmään. Sen lisäksi tarvitaan palvelukohtaiset asiantuntijat, jotka tietävät mitkä ryhmät antavat mihinkin oikeuksia tietyn palvelun sisällä. Infra puolelta tarvitaan henkilö, joka tekee automaatiota taustalla. (H6)

Operaattori taso ei osaa myötää oikeuksia, minkä takia liiketoiminnan pyytäessä pääsyjä joutuu sovellusasiantuntija osallistumaan mukaan joka kerta pääsyoikeuksien jakamiseen. Tämä on todella aikaa vievää, kun on mukana operaattori ja sovellus asiantuntija miettimässä yksittäisen käyttäjän pääsyoikeuksia. Yksittäisiä käyttäjiä putkahtelee kymmeniä kuukausi tasolla, minkä takia vie paljon useiden ihmisten aikaa käyttäjähallinnan pyörittämiseen. (H6) Ongelmana on myös, että tarvitsee viestitellä monta viikkoa mitä halutaan ja mitä puuttuu käyttäjäoikeuksia pyydettäessä. Oikeuksia pyydettäessä iso tehtävä on selvittää mitä pääsyjä tarvitaan. (H7)

Normaalin käyttäjän kanssa kohdeyrityksen käyttäjähallintaprosessi on aika suoraviivainen. Käyttäjätunnukselle ilmoitetaan missä yksikössä toimii, onko jokin tehdas mukana, mikä rooli kyseessä, minkä jälkeen annetaan oikeudet. Power BI käyttöoikeus pitäisi saada heti kun työt alkavat. Konsernin kohdalla ongelmia tuottaa, ettei tiedetä mistä pitäisi saada pääsyt johonkin. Mikäli controller vaihtuu asiat mutkistuvat. Voi kestää kuukausia, että saadaan pääsyt kuntoon. Esimerkkinä tapahtuma, jossa oltiin tilattu käyttäjätunnukset puolitoista kuukautta ennen käyttäjän töiden alkamista. Oli listattu kaikki mihin tarvitsee oikeudet ja pyydetty niitä käyttäjätunnukselle. Todellisuudessa IT oli laittanut aikataulutavoitteeksi viikko aloituspäivän jälkeen. Kommunikointi ongelmat IT:n kanssa hidastavat ja monimutkaistavat prosessia entisestään. Kohdeyrityksen Service Deskiä ollaan siirtämässä palveluntuottajalle. Haastateltava ei osannut sanoa miten kommunikointi ja palvelu toimii palveluntuottajan toimesta. (H7)

Prosessi toimisi hyvin, jos henkilölle pystyisi antamaan helposti oikeudet ja selvittämään mihin hänen pitäisi päästä. IT kanssa on vaikea päästä yhteisymmärrykseen mihin käyttäjän pitäisi päästä. IT ei ymmärrä käyttäjien viestiä ja kommunikoinnissa on hankaluuksia. On tilanteita, joissa on pyydetty pääsyjä käyttäjälle ja IT ei ole ymmärtänyt mihin

oikeuksia pitäisi antaa. Tässä tilanteessa IT ei kysynyt lisätietoa tapauksesta. Ongelmia lisäsi se, että tiketille saatettiin laitta viestiä vasta kun sitä oltiin sulkemassa ja tarkistettiin, onko tiketti enää aktiivinen. Pääsyryhmien monimutkaisuus aiheuttaa IT henkilöilläkin paljon hankaluuksia. Ryhmät ovat evoluution aikaansaannosta. Organisaatio, hallinta ja kaikki muu muuttuvat ajan myötä. Mikäli jotain evoluution kerrosta muuttaa eivät muut kerrokset enää välttämättä toimi. Evoluution aikaansaannosten muuttaminen vaatisi resursseja. (H7)

Kohdeyrityksen käyttäjähallintaprosessi on aivan täynnä pullonkauloja. Sovellusasiantuntijan ollessa poissa tiketti odottaa kolmekin viikkoa. Välillä joku nohevaoperaattori kiertää sitä kopioimalla oikeuksia lähellä olevalta profiililta, mikä on mennyt usein vikaan. On myönnetty lisenssiallokaatioita järjestelmiin, mitä henkilö ei ole koskaan käyttänyt. Asia on huomattu parin vuoden päästä auditoinnissa, että henkilölle on myönnetty lisenssi, mitä hän ei ole koskaan käyttänyt. (H6)

Toinen ongelma lisenssin suhteen on, että ilman niitä ei päästä resursseihin käsiksi. Kohdeyrityksessä käyttäjä tarvitsee Power BI Pro -lisenssin, jotta voi edes päästä tarkastelemaan raportteja. Raportteja ei pysty edes tarkastelemaan, vaikka olisi myönnetty pääsy, jos käyttäjällä ei ole Pro lisenssiä. Tällä hetkellä Power BI:n oikeudet on annettu käyttäjä kohtaisesti. Parempi tapa olisi antaa oikeudet ryhmäkohtaisesti. Siirto Power BI Premiumiin on jossain tytäryrityksissä työn alla. Perus käyttäjälle ei pitäisi tarvita hankkia Pro lisenssiä, sillä he eivät tee raportteja, pelkkä tarkasteluoikeus riittää. Power BI:ssä pitäisi olla siis kahden tyyppisiä rooleja, raportoijat ja katselijat. Joka tytäryrityksessä on suurin piirtein 1-2 käyttäjää, jotka tekevät raportteja. Kohdeyrityksen pitäisi siirtyä Power BI:n Premiumin alle, jotta ei tarvita pro lisenssiä kaikille. Siirto Premiumin käyttöön on työn alla. (H7)

Konserni tason organisaatiossa ongelmia saattaa aiheutua, kun ei ymmärretä eri käyttäjäoikeus tasoja. Siinä käy helposti niin, että joko ollaan liian tiukkoja oikeuksien antamisessa. Kun annetaan jokainen oikeus erikseen, pitää olla pyytämässä lisää oikeuksia tukipalvelusta, kun oikeuksia tarvitaan lisää. Tällöin prosessista riippuen voidaan joutua odottelemaan viikkoja. Vaikka ajatellaankin, että tarpeeksi tiukalla prosessilla voidaan pysyä turvassa, niin on tässä skenaariossa havaittu suuri ongelma. Kun ollaan liian tarkkoja käyttäjäoikeuksien jakamisen suhteen, niin lopulta voi käydä niin, että joku turhautuu prosessiin ja jakaa liikaa oikeuksia väärälle henkilölle. (H5)

Kohdeyrityksessä on ilmentynyt ongelmia myös konserni tason seurauksesta. Kun on selvitelty miten asioita pitäisi tehdä, on huomattu paljon selityksiä miksi asioita ei ole hoidettu järkevästi. Esimerkiksi AD on rämettynyt suo ja liiketoimintayksiköillä on täysin

erilaisia boarding prosesseja. Käyttäjiä muodostetaan eri tavalla ja laitetaan erilaisia tietoja. Tällöin roolipohjainen käyttäjähallinta AD roolin perusteella on hankalaa. Ihmisiltä puuttuu oleellisia tietoja profiilista. Konserni tasosta johtuen on paljon paikallisia sovelluksia liiketoimintayksiköissä, joihin on käyttäjähallinta aina täytynyt jollain tasolla hoitaa. Tämä on lisännyt käyttäjähallinnan yhtenäistämisen haasteellisuutta. Konsernin IT miettii aina konsernin sovelluksia. Aina välillä tulee rikottua jotain mitä on paikallisesti rakennettu. (H6)

Kohdeyrityksessä oli huomattu, että EU-rajojen sisäpuolella käytetään yhtä HR-sovellusta, mutta jos konserniin kuuluu EU:n ulkopuolisia maita, niin tulee haasteita käyttää vain yhtä HR-järjestelmää, jolloin ratkaisu on usein käyttää montaa eri HR-järjestelmää. Tämä tuottaa haasteita hallinnon tasolle. Pienillä yrityksillä kaikki tietää, ketkä on töissä ja kenen kuuluu tehdä mitäkin. Tämä luo idealistisemman tilanteen, eikä hyväksymisprosessi ole niin hierarkkinen kuin konserni tasoisessa yrityksessä. (H8)

Yrityksen koko ei sinällään ole ongelma, vaan se miten on totuttu tekemään ja kuinka monimutkaisia prosessit ovat. Jos yksinkertaistaa ja toteutetaan asiat, niin kuin jollain tuotteella on suunniteltu tehtävän ei yrityksen koolla ole väliä. Yrityksen rakenne ja miten rakennetta on totuttu käyttämään vaikuttavat kokoa enemmän onnistumiseen. Jos on rakennettu monimutkainen AD rakenne, niin sen yksinkertaistaminen olisi kannattavaa. Muutoshalukkuus vaikuttaa paljon uuden teknologian käyttöönotossa. Prosessin uusimista vaikeuttaa, jos halutaan pitää paljon vanhoista monimutkaisista rakenteista kiinni. (H2)

6.7 Uuden käyttäjähallintaprosessin suunnittelu

Kun mietitään uuden käyttäjähallintaprosessin käyttöönottoa, täytyy se suunnitella perusteellisesti. Haastateltavilta kysyttiin mitä uuden käyttäjähallintaprosessin suunnittelussa tulisi ottaa huomioon. Haastateltavat määrittelivät kaikki hieman eri tavalla mitä ensimmäisenä tulisi huomioida. Haastateltavien vastausten pohjalta tehtiin prosessikuva yhdistäen vastaukset yhdeksi prosessiksi. Seuraavaksi käydään vastauksia läpi ja vertaillaan haastateltavien mielipiteitä keskenään.

Kuvassa 17 on esitelty haastateltava 5 määrittelemät vaiheet. Käyttäjähallinnan prosessiin kuuluu ensinnäkin käyttäjän perustaminen ja siihen liittyvät kompleksisuudet. Aktivointi riippuu järjestelmistä, onko niissä omia kompleksisuuksia. Lähdejärjestelmässäkin, esimerkiksi AD:ssa, voi olla mahdollista ajastetusti aktivoida käyttäjätunnus. Ajastetulla

aktivoinnilla voidaan määritellä koska tunnuksella voi kirjautua sisälle. Muissa järjestelmissä ajastus taas ei välttämättä ole niin helppoa. Tästä voi seurata integraatio ongelma, kun toinen järjestelmä ei tuo ajastettua aktivointia. (H5)

Aina pitäisi ottaa kaikki tarpeet huomioon. On erilaisia käyttäjätyyppejä. On ikään kuin kuluttaja tai loppukäyttäjä. Loppukäyttäjällä todennäköisesti ei ole juurikaan mitään oikeuksia. On olemassa kehittäjiä ja konsultteja, jotka käyttävät järjestelmää. Näille täytyy antaa enemmän oikeuksia mutta rajata kuitenkin siten, ettei ihan kaikkeen pääse käsiksi. Käyttäjien elinkaari täytyy huomioida. On oltava suunnitelma, kun käyttäjä luodaan, miten se luodaan, mihin se luodaan ja mitä oikeuksia annetaan. Oikeuksia voidaan muuttaa ajan mittaan. Täytyy huomioida, miten se heijastuu järjestelmiin. (H5)

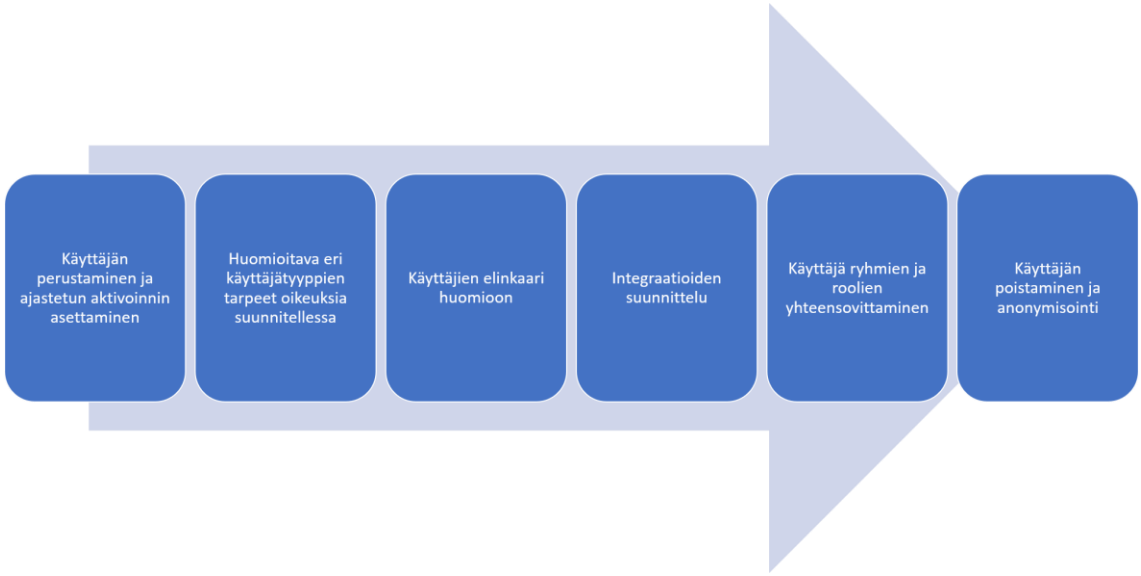
Integraatioiden suhteen täytyy miettiä, mistä data saadaan ja onko päällekkäisyys ongelmia. Jos jonkun datan perusteella lähdetään käyttäjiä luomaan automatiikan avulla, niin kuinka paikkansapitävää materiaali on. Voiko käydä niin että ollaan luomassa kahta päällekkäistä käyttäjää. Kun järjestelmää suunnitellaan, niin pitää miettiä roolit. Minkälaisia rooleja kyseinen sovellus tai järjestelmä tarvitsee ja kuinka niitä luvitetaan. Aika usein käytetään käyttäjäryhmiä oikeuksien jakamiseen järjestelmään. (H5)

Ylläpidossa käyttäjätiedot kulkevat järjestelmien välillä. Voi kuitenkin olla tilanteita, joissa käyttäjä on master tiedon ulkopuolella. Normaalisti käyttäjätieto tulee AD:sta joka puolelle. Saattaa olla kuitenkin erikoistapauksia, että tieto ei tulekaan AD:sta. Sotkuisen datan yhdistäminen voi olla vaikeata. Yksi selkeä ongelma käyttäjätiedon päivittämisessä ja on sähköpostiosoite. Vaikka pitäisi rakentaa moderneja järjestelmiä, niin tunnistetieto on yleensä sähköpostiosoite. Ongelmana on, että sähköpostiosoite saattaa vaihtua. Toinen on nimenvaihdokset, ihmisillä vaihtuu sukunimet ja välillä myös etunimet. Tällaisia ei ole välttämättä otettu huomioon. Sähköpostiosoite on valitettavan usein edelleenkin se tunnistetieto mitä ei pysty muuttamaan. Se saattaa muuttua UI:ssa mutta ei esimerkiksi kirjautumistiedoissa. Haastateltava 5 oli huomannut, että edelleen on paljon riippuvuutta sähköpostiin. (H5)

Vähemmälle jäänyt mutta erittäin tärkeä osa on, kun jossain vaiheessa poistetaan käyttöoikeudet. Mitä silloin tehdään, kun pitää poistaa ja käyttäjä lakkaa olemasta. On valitettavan usein unohdettu asia, johon ei kiinnitetä huomiota. Kun järjestelmiä suunnitellaan, huomioidaan se, että kuinka saadaan käyttäjille oikeudet. Kun tulee pyyntö, että käyttäjä pitäisi poistaa, tulisi olla suunnitelma valmiina, mistä pitää tiedot poistaa ja kuinka se toteutetaan. Poistamisessa on kompleksisuuksia monesti ihan jo sen takia, koska järjestelmään käytettäessä jää käyttäjästä jälkiä järjestelmään eri paikkoihin.

Näistä muodostuu riippuvuuksia datan keskuudessa käyttäjään. On huomioitava se, että monissa tapauksissa ei pystytä kokonaan poistamaan käyttäjää. (H5)

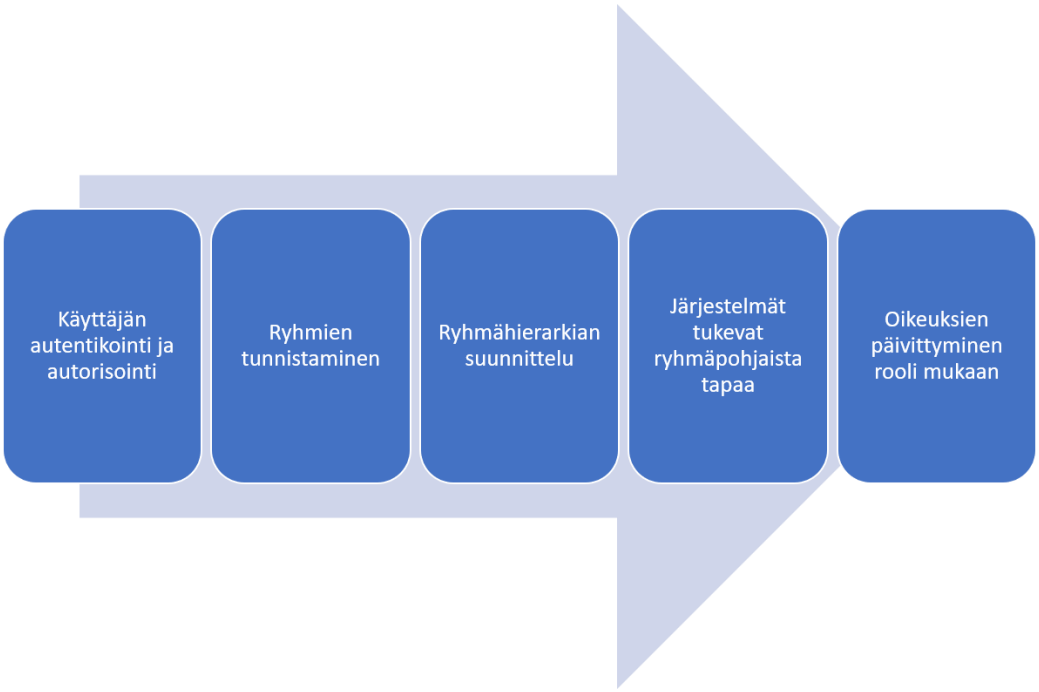
Käyttäjä voidaan disabloida eli kytkeä pois päältä, mutta periaatteessa sitä ei pysty kuitenkaan poistamaan kokonaan järjestelmän näkökulmasta. Tähän liittyy anonymisointi, eli pitäisi pystyä poistamaan henkilötiedot ja tehdä käyttäjästä anonyymi. Todennäköisesti käyttäjällä on jokin käyttäjänumero, mikä säilyy. Numeroon todennäköisesti on liitetty kaikennäköisiä muita henkilötietoja, mitkä pitäisi poistaa siinä vaiheessa. Hallinnollisesta näkökulmasta ei ole näkynyt sellaisia työkaluja, joilla voisi lakkauttaa käyttäjä. Siihen ei olla samalla tavalla keskitytty niin paljon kuin pitäisi. Vaikka anonymisointi on hankala vaihe tulisi se etukäteen huomioida, jotta tiedetään, miten se voidaan toteuttaa. (H5)



Kuva 17 Haastateltava 5 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Kuvassa 18 on esitelty haastateltava 4 määrittelemät vaiheet. Yleensä kun tehdään palveluita, puhutaan autentikaatiosta ja autorisaatiosta. Jos käyttäjällä on tunnus, hän pystyy kirjautumaan sisään ja todistamaan henkilöllisyytensä. Autorisoinnissa selvitetään kuka saa tehdä ja mitä kirjauduttuaan sisälle, mikä monesti laiminlyödään. Saatetaan vain kelpuuttaa, että kunhan henkilö on yrityksellä töissä, niin saa oikeudet. Nykyään halutaan, että käyttäjät kuuluvat johonkin ryhmään. Jolloin jos käyttäjä kuuluu tiettyyn ryhmään, saa se tietyt käyttöoikeudet. Tällöin palvelu toimii siten, että se tarkistaa kuuluuko käyttäjä tiettyyn ryhmään myöntäessään oikeuksia päästä käyttämään palvelua. Roolia vaihdettaessa yrityksen sisällä, täytyy miettiä mihin käyttäjä tarvitsee lisää ja mihin vähemmän oikeuksia. Harvoin tarvitsee välttämättä ottaa oikeuksia pois, yleensä lisätään. (H4)

Esimerkkinä oikeuksien saamisesta lisää, voidaan joutua pyytämään yksitellen lisää oikeuksia. Mikä saattaa olla tapahtuma useissa tapauksissa. Joudutaan pyytämään tiketillä oikeudet tai henkilökohtaisesti ylläpitäjää lisäämään tiettyyn AD-ryhmään. Ryhmäpuuta käytettäessä ryhmät kuuluisivat ryhmänä johonkin, jolloin yksittäisiä käyttäjiä ei hallittaisi. Voisi esimerkiksi olla projektipäälliköt ryhmä, josta projektipäälliköt saisivat sen tasoiset oikeudet mihin tarvitsee. Tietyn roolin perusteella voitaisiin antaa toimivasti sen tarvitsemat oikeudet. Ryhmien tunnistaminen on haasteellista. Kun tunnistetaan ryhmähierarkia, onnistuisi käyttäjän siirtäminen ryhmästä toiseen ryhmähierarkian sisällä. Tällöin roolin muuttuessa oikeudet päivittyisi roolin mukaiseksi. Tämä vaatii, että kaikki järjestelmät, joita yritys käyttää tukevat ryhmäpohjaista ja valittua tapaa. (H4)

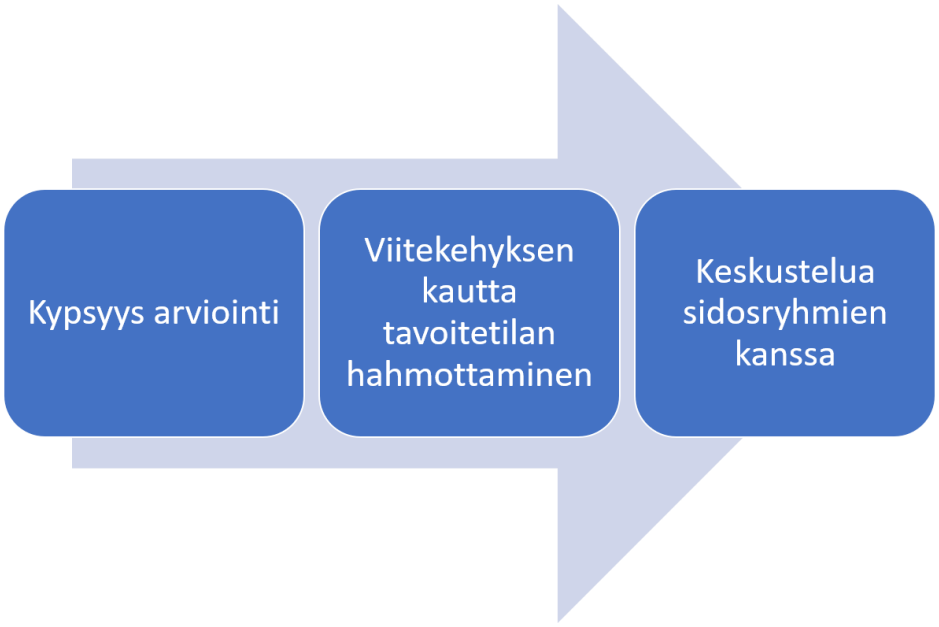


Kuva 18 Haastateltava 4 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Kuvassa 19 on esitelty haastateltava 2 määrittelemät vaiheet. Alkuun olisi hyvä tehdä kypsyysarviointi, jossa selvitetään yrityksen nykytilanne. Kun tiedetään missä ollaan, niin tiedetään mitä lähteä parantamaan. Viitekehyksen kautta kannatta lähteä miettimään sitä tavoitetilaa ja mihin halutaan päästä. On tärkeää, että asiakkaan puolelta löytyy henkilö, kenellä on omistajuus asioista. Tällöin pystytään tekemään päätöksiä ja vastuut ovat selkeät. (H2)

Muutos organisaatiossa, jossa prosessi ja järjestelmä otetaan käyttöön, vaatii useiden sidosryhmien kanssa keskusteluita. Mikäli on viisikin integraatiota järjestelmien välillä, täytyy keskustella liiketoiminta tasolla ja teknisellä tasolla järjestelmän omistajien

kanssa. Aika usein halutaan järjestelmissä perustelut, miksi tarvitaan niinkin suuret pääsyoikeudet kyseisiin järjestelmiin. Keskusteluissa menee yleensä aika kauan aikaa, että saadaan kaikki vakuuttuneiksi, että ratkaisusta on hyötyä kaikille. (H2)



Kuva 19 Haastateltava 2 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Kuvassa 20 on esitelty haastateltava 6 määrittelemät vaiheet. Haastateltava 6 mukaan ensimmäinen lähtökohta olisi, että AD on ajan tasalla ja on toimivat onboarding ja offboarding prosessit. On selvitettävä, mistä tulee kaikki relevantit tiedot käyttäjälle, joita tarvitaan yleisesti käyttäjähallintaan henkilölle. Käyttäjillä tulisi olla jonkin näköinen rooli, mikä olisi jollain määrin yrityksen standardi. Tällöin käyttäjähallintaa olisi paljon helpompi lähteä toteuttamaan roolipohjaisesti. Jolloin valtaosa käyttäjähallinnan tehtävistä voitaisiin hoitaa automaation avulla käyttäjää perustaessa. (H6)

Kohdeyrityksen liiketoimintayksiköt operoivat itsenäisesti. Konsernin strategiassa on, että liiketoimintayksiköt raportoivat itsenäisesti, jotka ovat omia itsenäisiä entiteettejä, joilla on tukifunktioita jatkeena. Konsernin näkökulmasta toimintokohtaiset ryhmät tulisi pystyä pitämään standardisina läpi konsernin. Talous, myynti, operaatio ovat kriittisemmät dimensiot, joiden alapuolelle tulee pienempiä ryhmiä. Toiminto ryhmien pitäisi olla pääasialliset ryhmät mitkä jakavat oikeuksia käyttäjille, sen mukaan mihin funktioon, liiketoimintayksikköön tai osastoon kuuluu. (H6)

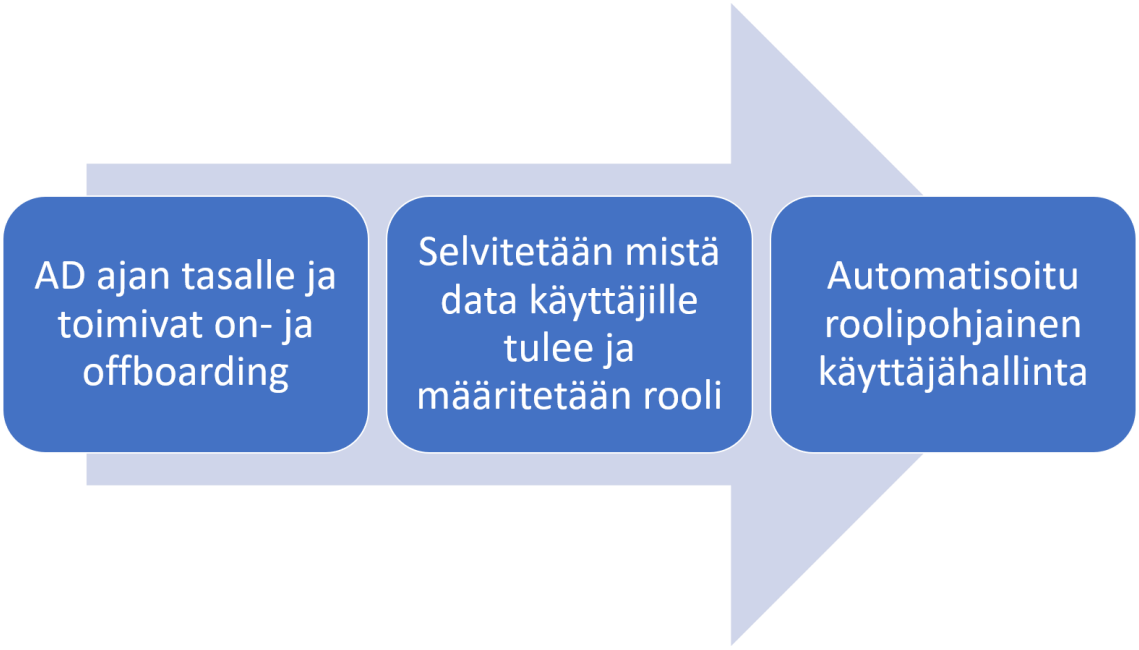
Roolipohjaisen käyttäjähallinnan prosessin ylläpito pitäisi hoitua Service Deskin kautta. Prosessi pitäisi olla hyvin kuvattu palvelu kohtaisesti, minkä ryhmien yhdistelmänä käyttöoikeus jaetaan. Service Deskin kautta käyttäjä pyytää ja käyttäjän liiketoiminto hyväksyy pääsyn palveluun. Service Desk hoitaa käyttäjän ryhmiin mihin pitää. Tavoitteena

olisi minimoida sovellus asiantuntijoiden käyttämää aikaa. Kun tulee tilanne, että käyttäjä tarvitsee oikeuksia, mitkä eivät vastaa millään tavalla työnkuvan roolia, ei ole järkevää lisätä käyttäjää ryhmiin mistä oikeudet automaattisesti tulee. Sovellus asiantuntija voisi manuaalisesti tehdä poikkeuksia. (H6)

AD-ryhmät pysyvät tulevaisuudessa hallinnassa, kun ryhmät pidetään konsernin standardeissa. Tällöin ryhmien määrät eivät lähde laajenemaan ja jokaisella tytäryhtiöllä ei ole aivan erilaiset ryhmät. Jos kaikki yritykset loisivat ryhmiä omien sääntöjen mukaan, säännöt millä oikeuksia jaettaisiin, muuttuisivat todella monimutkaisiksi. Ryhmien täytyy olla riittävän yksinkertaiset, jotta säännötkin pysyvät yksinkertaisina, jolloin operaattori tasollakin pysyy toiminta helppona. IT infran tehtävänä olisi luoda uusia ryhmiä. Uusien ryhmien tarve voi syntyä lähtökohtaisesti projektien kautta, sovellus asiantuntijalta tai projektipäälliköltä, tai ulkoiselta konsultilta. Jokaisessa projektisuunnitelmassa tulisi olla yhtenä komponenttina, miten käyttäjähallinta toteutetaan. IT infran pitäisi hyväksyä suunnitelma. On mahdollista, että pyyntöjä tulee lokaaleilta liiketoiminoilta. (H6)

Osasta tytäryrityksistä käyttäjiltä löytyy AD:sta rooli ja osasta tytäryrityksistä henkilöiltä saattaa puuttua jopa esihenkilö tieto, jolloin AD:sta löytyy vain etunimi, sukunimi, sähköposti. On kuitenkin vaihtelevaa, missä kunnossa eri puolilla käyttäjien tiedot ovat. Vaikea sanoa IT näkökulmasta. Kolmevuotta sitten tehtiin yhdelle tytäryhtiölle sinlge sign-on. Tämän seurauksena tehtiin pieni AD projekti, jossa käytiin läpi ja laitettiin AD:t kuntoon. Mitään uutta prosessia ei kuitenkaan tehty käyttäjien onboardingiin, joten tieto on todennäköisesti näin 3 vuoden jälkeen jo jälleen rämettynyttä. (H6)

Jotta käyttäjille saataisiin roolit AD:hen pitäisi lähteä liikkeelle siitä, että mikä tieto on pakollista siinä vaiheessa, kun tunnusta luodaan. Prosessi puolen kysymys mitä on pakko laittaa paikalleen onboardingissa. Käyttäjien roolien muuttuessa on tilanne hankalampi mutta siihenkin pitäisi olla oma prosessi, jolloin käyttäjän itse tai esihenkilön on ylläpidettävä tietoja. Aika isolta osalta BI käyttäjiä oletetaan löytyvän relevantti rooli ja relevantit tiedot. Riittävällä dokumentaatiolla liian vähäisen tiedon puuttuessa ratkaisu ei olisi vain, että päästetään henkilö järjestelmään, vaan ratkaisu on ylläpitää roolia ja sitä kautta päästä ryhmiin. Toinen osa on, että saada uusi onboarding uusille käyttäjille. Lähdetään uusimaan prosessia painottaen sitä, että niissä tilanteissa missä puuttuu tietoja ei tehdä poikkeuksia vaan kyseessä on puutteellinen AD-tieto ja ylläpidetään sitä AD:ta. (H6)



Kuva 20 Haastateltava 6 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Kuvassa 21 on esitelty haastateltava 3 määrittelemät vaiheet. Haastateltava 3 mukaan käyttäjähallinnan suunnittelu lähtee lähdejärjestelmästä liikkeelle. Prosessi täytyy suunnitella hyvin, ettei vyörytetä vääränlaista tietoa. Automatisoidaan vain ajan tasalla olevaa tietoa. Käyttäjähallintaprosessissa täytyy tehdä roolittaminen. Suunnitelmaa tehdessä pitää olla pitkän juoksun suunnitelma, esimerkiksi roadmap. Roadmapissa käsitellään, mitä identiteetinhallinnalla tavoitellaan pitkässä juoksussa. Selvitetään antaako tehty suunnitelma tukea liiketoimintaan. On keskityttävä oleellisimpiin asioihin, jotta saadaan suunniteltu prosessi tuotantoon mahdollisimman nopeasti. Vähemmän tärkeät ominaisuudet ja osat jätetään myöhemmäksi. (H3)

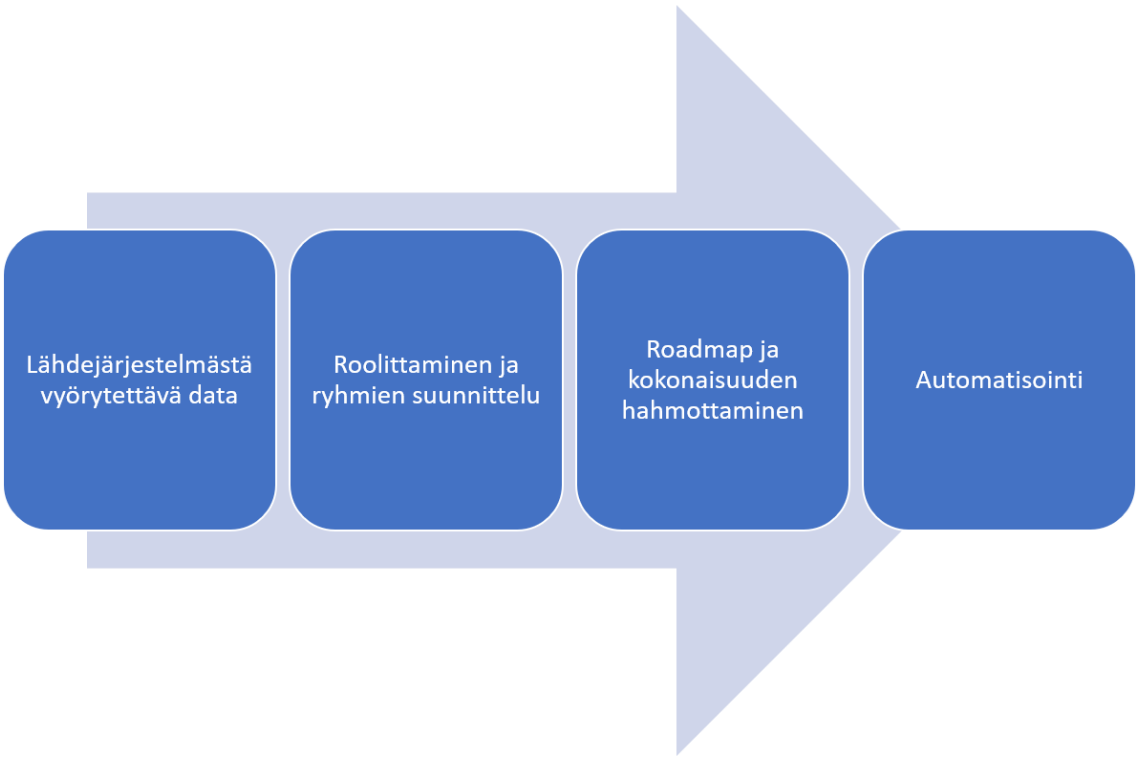
Jos käyttäjähallintaa ei rooliteta, häviää prosessin hallittavuus. Täytyy pystyä ryhmitelmään, jotta voidaan antaa ryhmille tarpeelliset oikeudet. Identiteetinhallinnassa voidaan hallita ryhmien pääsyjä erilaisiin järjestelmiin ja millaisia käyttövaltuutuksia myönnetään. Jos hallitaan yksittäisiä käyttövaltuutuksia ryhmien sijaan, menetetään hallittavuus kokonaan. Esimerkiksi 20 000 identiteetinhallitseminen erikseen on huomattavasti vaikeampaa kuin ryhmien, joissa nämä identiteetit sijaitsevat. (H3)

Käyttäjähallinnan suunnittelussa iso virhe on, että ei katsota kokonaisuutta, vaan lähdetän yksittäisen tarpeen mukaan toteuttamaan. Myöhemmin huomataan, että olisi pitänyt ottaa huomioon tiettyjä asioita ja osia. Alkukartoitus ja tavoitteiden luominen on oleellista suunnitteluprosessissa. Ei kannata yrittää tunkea kaikkea mahdollista ensimmäiseen toteutukseen. Roadmapin ja prioriteettien määrittelyn avulla pyritään tunnistamaan oleellisimmat ominaisuudet ja vaiheet. (H3)

Paras olisi, että käyttäjähallintaprosessi lähtee lähdejärjestelmästä, parhaassa tapauksessa HR järjestelmästä. Kun tulee uusi työntekijä, hänen tiedot viedään HR järjestelmään. HR järjestelmästä tiedot vyörytetään identiteetinhallinta järjestelmään, jonka takana on kohdejärjestelmät. Kohdejärjestelmiin annetaan oikeuksia käyttäjälle työrooliin liittyen. HR ei välttämättä riitä ainoaksi lähdejärjestelmäksi. Kun on useita lähdejärjestelmiä, asia muuttuu monimutkaisemmaksi. Olisi hyvä, että joudutaan tekemään vain yhteen paikkaan muutos, josta muutokset siirtyvät automaattisesti muihin järjestelmiin. Henkilön poistuessa talosta täytyy oikeudet poistaa. Kun muutos tehdään yhdestä järjestelmästä, saadaan oikeudet deprovisioitua takaisin päin. Muutos HR-järjestelmästä välittyisi muihin järjestelmiin ja oikeudet poistettaisiin, jolloin tietoturva paranee. (H3)

Kun käyttäjähallinta on hallittua, käyttäjät pääsevät vain niihin kohteisiin, mihin heidän pitää työroolinsa takia päästä. Tällöin ei pääse syntymään vaarallisia yhdistelmiä, missä esimerkiksi käyttäjä tilaa ja hyväksyy tilauksen itse. Tällaisia vaarallisia yhdistelmiä ei pääse syntymään, kun asiat on hoidettu oikein. identiteetinhallintaroolit päivittyvät sitä mukaan, kun henkilön työrooli päivittyy. Identiteetinhallinta ja pääsynhallinta puoli parantaa auditointia ja raportointia, jossa tarvitaan raportteja todistusaineistoksi. Manuaalisen työn vähentäminen on merkittävää. Aikaisemmin käyttäjähallinta vei paljon aikaa, kun kaikki tehtiin manuaalisesti. Jos saadaan muutokset menemään yhdellä muutoksella automaattisesti kaikkiin järjestelmiin, säästetään aikaa. (H3)

Pohjatyön laiminlyöminen voi estää automatisoinnin. Mikäli roolitusta ei ole tehty lähdejärjestelmä tasolla, on hyvin vaikeaa automatisoida käyttäjähallintaprosessia. Tällöin ei saada hyötyjä irti. Täytyy tehdä pohja määritykset ja roolittaa käyttäjät erilaisiin ryhmiin. On myös sellaisia järjestelmiä, joita on vaikea integroida identiteetinhallinnan kanssa. Nykypäivänä kuitenkin on todella hyvin valmiita liittimiä, jolla pystytään toteuttamaan integroiminen. Joidenkin järjestelmien kanssa liitoksen tekeminen saattaa olla hyvinkin aikaa vievää. (H3)



Kuva 21 Haastateltava 3 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Kuvassa 22 on esitelty haastateltava 8 määrittelemät vaiheet. Haastateltava 8 mukaan ensimmäisenä määritellään käyttäjähallinnassa data, mitä tarvitaan käyttäjä kohtaisesti. Sen jälkeen jokaiselle data alueelle tehdään retentio säilytettävyydestä ja tarkistetaan sen sensitiivisyys sekä otetaan ristiin tarkistus identiteetinhallinnan ja lainsäädäntöjen kanssa. Huomioitavia lainsäädäntöjä on muun muassa GDPR, EU-lainlainsäädäntö ja Suomen IT-lainsäädäntö. Lainsäädäntö nousee isompaan rooliin, kun tehdään monikansallista käyttäjien hallintaa. Täytyy tehdä periaate päätös, halutaanko minimoida HR-järjestelmät vai halutaanko, että jokaisella yrityksellä konsernissa on oma HR-järjestelmä. Tämä kasvattaa mahdollisten integraatioiden määrää, niiden validiointia ja hyväksyntää. Datan validointi ja mitä tarvitaan, on erittäin tärkeää määritellä. (H8)

Sen jälkeen, kun on selvitetty datan sensitiivisyys, tarkistetaan kuinka hyvin oma sensitiivisyys ja säilytettävyysmalli istuu lakeihin ja säädöksiin vai tarvitseeko mallia muokata. Datan pitää olla selkeästi luokiteltu ja määritelty, kuinka kauan sitä säilötään. Sen jälkeen on tärkeää datalle, jota käyttäjän- ja identiteetinhallinnassa tarvitaan, että sille on kaavat ja säännöt, minkä tyyppistä data on. Näin voidaan validoida ja varmistaa, että data on varmasti oikean tyyppistä. Esimerkiksi sähköposti on oikeassa muodossa, miten etu- ja sukunimet kirjotetaan, otetaanko ääkköset mukaan. Sen jälkeen organisaatio rakenteen tai tehtävänannon mukaan pyritään rakentamaan suhteellisen tarkka RBAC-malli ja konvertoidaan sitä mahdollisuuksien mukaan DRBAC-malliin. Tämän jälkeen on helpompi

lähteä provisioimaan käyttäjää ja muuta eteenpäin, kun ollaan varmoja siitä, että data on validia, sääntöjen mukaista ja on määritelty hallintamalli. (H8)

Tällä hetkellä yrityksellä on kaksi identiteetinhallintaprosessia, joista toinen on HR-prosessi, joka liittyy työsopimukseen ja palkanmaksuun ja kaikki muut HR. Toinen on IT-prosessi eli HR-prosessin jälkeen sama tieto välitetään IT:lle. IT hallitsee tunnuksia parhaansa mukaan sillä aikataululla, millä pystyy. IT aktivoi ja deaktivoi tunnuksia. Jos käyttäjä tarvitsee pääsyä sisäisiin tai kolmannen osapuolen järjestelmiin niin työpyyntö välitetään järjestelmä vastaajille, jotka aktivoivat tunnuksia. Vastuurooleja ovat HR, tekniset roolit: IT ja sovellusvastaavat sekä hyväksymisroolit: käyttäjien esihenkilöt ja heidän esihenkilöt. (H8)

Ideaalitilanteessa, HR-järjestelmään luodaan uusi identiteetti, ja valitaan, mihin tunnusta jatko provisioidaan. Kaikki sisäiset identiteetit hallinnoitaisiin HR-järjestelmästä ja IT-järjestelmät ja työkalut vain välittävät identiteettiä ja provisioivat eteenpäin, miten HR-puolella on valittu. Eli hyväksyntä ja luonti tapahtuisi HR:ssä ja kaikki muu on automaattista taustalla tapahtuvaa sekä luodessa tunnuksia että päivittäessä oikeuksia. Esimerkiksi, kun työntekijä vaihtaa roolia A:sta B:hen, niin pääsyt määräytyvät roolin mukaan HR-järjestelmästä. Tämänhetkinen tilanne automatisoimisen taustalla on huonolla tasolla yrityksellä. Suomen tytäryrityksessä valmistellaan automatisointia, mikä toivottavasti saadaan käyttöön ennen kesälomia. Datan validointi on tuottanut paljon haasteita. (H8)

Uudistuksen yhteydessä on tarkoitus selkeyttää rooleja. Tarvitaan hyvä ja tarkka organisaatiokaavio, jotta voidaan toteuttaa onnistuneet rooliryhmät käyttäjien hallintaan, provisiointiin ja deprovisiointiin. Mitä tarkempi ja parempi organisaatiokaavio on, niin sitä paremmat rooliryhmät pystytään toteuttamaan, joita tarvitaan, jos on role-based access control (RBAC) tai dynamic role-based access control (DRBAC) käytössä. Tarkoituksena on Suomen yksikössä laittaa roolit vastaamaan organisaatiokaaviota. (H8)

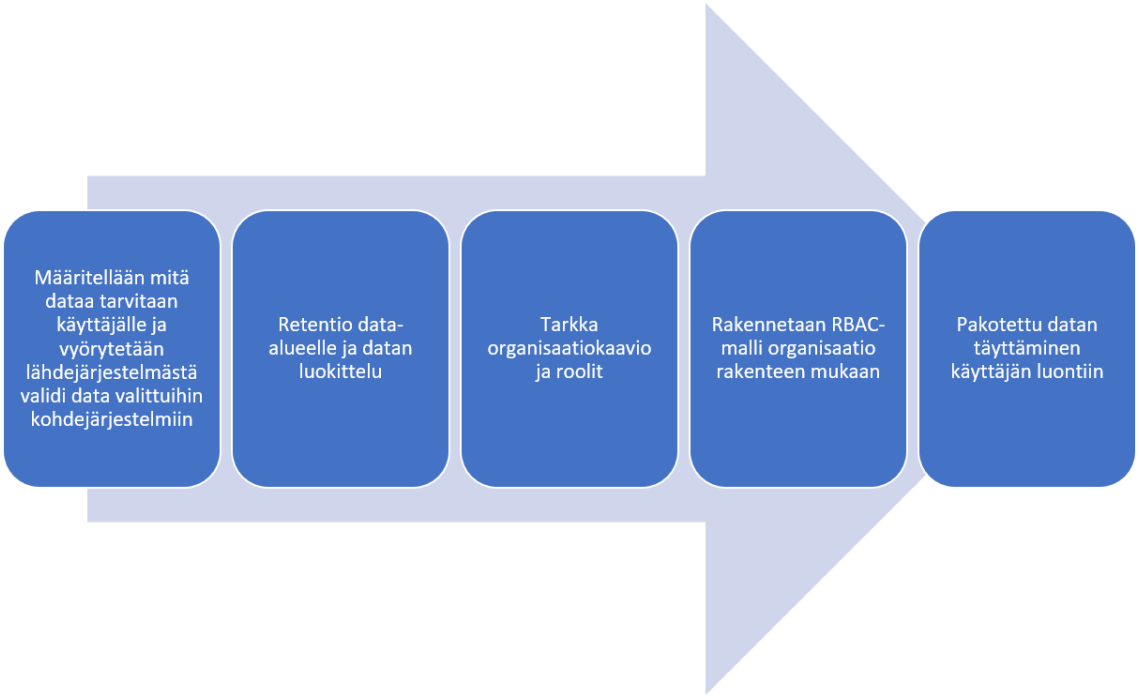
Oikeuksien jakamisessa on useita pullonkauloja. Esimerkiksi yksi pullonkaula on, ettei tiedetä, mitä oikeuksia tulisi antaa. Muita pullonkauloja ovat muun muassa se, että työntekijän esihenkilöt eivät kerkeä hyväksymään oikeuksia sekä järjestelmän omistajat ja tukihenkilöt eivät tiedä mitä oikeuksia pitää antaa, jotta saadaan tarvittavat resurssit käyttöön. (H8)

On olemassa kolme eri tapaa hallita käyttäjiä, manuaalinen, automaattinen ja yhdistelmä molempia. Osa oikeuksista voidaan antaa järjestelmiin joko roolipohjaisesti ja osa annetaan suoraan, mikä voi olla hyvin sekaista. Roolipohjainen käyttäjähallinta on ehdottomasti kannattavin. Kohdeyrityksellä on aina ollut roolipohjainen, mutta se ei ole aina toiminut hyvin. Joidenkin järjestelmien osalta ollaan sekavassa käytössä roolien ja suoraan

jaettavien oikeuksien kanssa. Tämä on osaksi liiketoimintayksikkö sidonnainen eikä järjestelmä sidonnainen eli riippuu yksikön IT ja järjestelmäomistajien tavasta ja halusta toimia. (H8)

Ei roolipohjaisen tavan yleisin riski on, että vaikka käyttäjä on poistettu käytöstä sisäisistä järjestelmistä, niin tunnus voi jäädä aktiiviseksi esimerkiksi pilvityökaluun eli käyttäjä pääsee kirjautumaan palveluun, ellei tunnusta manuaalisesti deaktivoida, koska käyttäjähallinnassa ei ole roolipohjaisuutta. Esimerkiksi yrityksen sisällä, kun vaihdetaan työroolia niin voi jäädä tunnuksia edellisestä tehtävästä. Roolipohjaisessa käyttäjähallinnassa tuottaa haasteita epäselvä organisaatiomalli tai, jos ei löydetä mitään selkeätä mallia, jota voidaan käyttää roolien tekemisessä ja ylläpitämisessä. Myös se, että data ei ole validia esimerkiksi HR-järjestelmässä luo haasteita. Data ei ole validia esimerkiksi, jos käyttäjä on luotu esimerkiksi ilman jotain tietoja. (H8)

Kohdeyrityksessä roolipohjaisen käyttäjähallinnan automatisoinnin toteuttamisen tilanne riippuu liiketoimintayksiköstä. Osassa liiketoimintayksikössä tilanne on hyvällä tasolla datan oikeellisuuden suhteen, mutta toisissa liiketoimintayksiköissä tilanne on erittäin huonolla tolalla. Ideaaliin tilanteeseen pääseminen vaatii aikaa IT:ltä ja HR:ltä, jotta voidaan varmistaa, että datat vastaavat toisiaan. Tämä tehdään manuaalisti ja vaatii siksi paljon aikaa. (H8)



Kuva 22 Haastateltava 8 vastausten pohjalta esille tulleet vaiheet käyttäjähallinnan suunnittelussa

Validia dataa ylläpidetään pakottamalla data. Esimerkiksi pakotetaan lomakkeeseen täyttämään tiedot ennen kuin voi edetä. Tämä on jäykkä ja jyrkkä tapa mutta toisaalta

ainut tapa tehdä. Dataa ei ole aikaisemmin pakotettu kohdeyrityksessä, koska on haluttu saada jokin järjestelmä käyttöön eikä ole laitettu tarpeeksi vaivaa ja aikaa. Ei ole nähty mahdollisia seurauksia. Suurin ongelma käyttäjähallinnassa on ollut aika. On haluttu ottaa uusia järjestelmiä mutta ei ole laitettu tarpeeksi aikaa käyttäjähallintaan. Halutaan ottaa koko ajan kiireellisellä aikataululla uusia järjestelmiä. Jolloin ei olla mietitty miten käyttäjähallinta käyttäjän näkökulmasta toimisi. (H8)

Seuraavassa luvussa vedetään yhteen tuloksissa kaikkien haastateltavien haastatteluista poimitut vaiheet ja tärkeät pointit onnistuneen käyttäjähallinnan suunnittelussa. Käyttäjähallinnan suunnittelusta ja prosessista on muodostettu prosessikuva, jossa on yhdistetty teorian ja haastatteluiden tulokset.

7. TULOKSET JA YHTEENVETO

Tässä luvussa käsitellään tutkimuksen tuloksien yhteenveto ja vastataan tutkimuksen alussa esitettyihin tutkimuskysymyksiin. Tulosten jälkeen arvioidaan tutkimuksen toteutumista ja luotettavuutta. Viimeisenä kappaleena käsitellään tulevaisuuden tutkimuskohteita, joihin voitaisiin syventyä tämän työn jälkeen.

7.1 Tulosten yhteenveto ja tutkimuskysymyksiin vastaaminen

Yrityksen käyttäjähallinnasta tunnistettiin kaksi pääongelmaa. Ensimmäisenä ongelmana oli, että käyttäjillä oli joko liikaa oikeuksia tai ei ollenkaan. Toisena pääongelmana oli, että käyttöoikeuksien antaminen oli todella työlästä. Lisäksi ongelma oli oikeuksien poistaminen. Tutkimuksen tavoitteena oli luoda ymmärrys yrityksen tämänhetkisestä käyttäjähallinnasta ja sen epäkohdista. Tutkimuksen tulosten tavoitteena oli selvittää miten yritys voisi parantaa käyttäjähallintaansa. Tavoitteena oli löytää tehokas ja tietoturvallinen tapa hallita käyttäjiä eri järjestelmien välillä. Tutkimustulosten perusteella yrityksen ongelmat ratkaisisi automatisoitu roolipohjainen käyttäjähallinta.

Mitä on käyttäjähallinta?

Mohammed (2019) mukaan identiteetin- ja pääsynhallinnalla (IAM) valvotaan, kenellä on pääsy yrityksen resursseihin käyttäjien roolien, käyttöoikeuksien ja tarpeiden hallinnalla, mikä vastaa haastatteluiden tuloksia. Identiteetin- ja pääsynhallinnan ydin on käyttäjäidentiteettien, attribuuttien ja roolien käsittelyssä. Lee ja Sawyer (2019) mukaan käyttäjien käyttöoikeuksien hallinta on järjestelmien ja datan oikeuksien kontrollointia. Jokaiselle työntekijälle luodaan digitaalinen identiteetti (Soh *et al.* 2020). IAM käsittelee digitaalisia identiteettejä ja käyttäjien pääsyä organisaation sisällä (Mohammed 2017). Käyttäjän identiteettiä on säilytettävä, päivitettävä ja valvottava koko käyttäjän olemassa olon ajan (Mohammed 2019).

Haastatteluissa ilmeni, että käyttäjähallinnan prosessi riippuu pitkälti siitä, minkälaisia käyttäjiä ollaan luomassa, mutta yleensä siihen liittyy jonkinnäköiset käyttöoikeudet ja roolit. Yrityksellä pitää olla jokin paikka missä voidaan hallita käyttäjien tietoja. On yrityskohtaista, miten itse käyttäjähallintaprosessi toimii. Kuitenkin käyttäjähallinnan perus prosessin runko ei yritysten kesken eroa toisistaan paljoa. Prosessissa saattaa olla muita polkuja mutta runko on lähinnä sama kaikissa tapauksissa.

IAM on hyvä jakaa eri osiin, jolloin IAM kokonaisuutta on helpompi tarkastella. Kokonaisuutta tarkastellessa nousee kysymyksiä esiin, miten kyseinen osa-alue on toteutettu ja miten sitä voidaan kehittää. Teoriassa huomattiin, että IAM jaettiin hieman eri osiin eri lähteestä riippuen.

CSAn mukaan (2012) IAM prosessi sisältää muutakin kuin pelkän käyttöoikeuksien hallinnan. Identiteetin- ja pääsynhallinta prosessiin kuuluu keskitetyt hakemistot, pääsynhallinta, identiteetinhallinta, roolipohjainen pääsynvalvonta, käyttöoikeuksien sertifikaatit, ylläpitäjäkäyttäjien ja käyttöoikeuksien hallinta, tehtävien erottaminen sekä identiteetti- ja käyttöoikeusraportointi. Kun taas AbidHussain ja Praveen Kumar Sharma (2020) mukaan pääsynhallinnan kuusi eri komponenttia ovat, käyttäjän identiteetti, monivaiheinen todennus, hakemistopalvelut, raportointi, tarkastus ja vaatimustenmukaisuus ja käyttäjien käyttöoikeuksien hallinta.

AbidHussain ja Praveen Kumar Sharman (2020) pääsynhallinnan komponentteja verrattuna CSA (2012) määrittelemiin huomattiin, että pääsynhallinta ei ole pelkästään oikeuksien myöntämistä ja rajaamista. Yhteiset komponentit turvallisen pääsynhallinnan takaamiseksi olivat identiteetinhallinta ja siihen liittyvät toimet, keskitetty hakemisto, pääsynhallinta sekä identiteetin- ja käyttöoikeuksienraportointi.

Roolipohjainen pääsynhallinta nousi esille useamman haastateltavan vastauksessa. Roolipohjaisen pääsynhallinnan (RBAC) ajatuksena on oikeuksien myöntäminen käyttäjille heidän roolinsa perusteella organisaatiossa. RBAC tarjoaa yksinkertaisen, hallittavan lähestymistavan pääsynhallintaan, mikä on vähemmän altis virheille kuin käyttöoikeuksien myöntäminen käyttäjille yksittäin. (Auth0, n.d.)

Teorian märittelemien osa-alueiden lisäksi haastatteluissa nousi esille osa-alueita, joita ei tullut teoriassa käsiteltyä. IAMin sisäisiä prosesseja ovat muun muassa onboarding, offboarding ja joiner-mover-leaver -prosessit. Jatkuvia toimintoja ovat muun muassa roolien, attribuuttien, käyttöoikeuksien, sertifiointien ja valvonnan hallinta. Muita keskeisiä toimintoja ovat pääsynhallinta, SSO, federointi ja yhä enemmän API hallinta sekä API käyttötapaukset. IAM on osa IT-hallintoa, joka voidaan hoitaa sisäisesti ja ulkoisesti. IAM sisältää IT-strategioita, tukiprosesseja, hallintoja ja itsepalveluita. Itsepalvelut ovat usein läsnä IAM puollella, koska jos kyseessä on tuhansia tai jopa miljoonia käyttäjiä, ei IT-hallinto pysty manuaalisesti tekemään kaikkea.

Käyttäjähallinta lähtee liikkeelle siitä, kun tulee uusi työntekijä tai työntekijä vaihtaa uuteen rooliin ja syntyy tarve päästä sovellukseen, dataan, järjestelmään tai tiloihin käsiksi. Mohammed (2017) mukaani identiteetinhallinta aloitetaan tunnuksen luomisesta eli re-

kisteröinnistä. Haastatteluissa nousi esille, että työntekijälle luodaan käyttäjätunnus ennen työsuhteen alkamista. Aloitus päivänä aktivoidaan tunnukset, jotta työntekijällä olisi tunnukset ja oikeudet jo ensimmäisenä työpäivänä. Jotta saadaan tarvittavat tiedot käyttäjän identiteetille, voidaan pakottaa identiteetin luomisvaiheeseen täyttämään halutut tiedot.

Haastateltavat kertoivat, että käyttäjät luodaan master järjestelmään, mikä usein on HR-järjestelmä. HR järjestelmästä tiedot vyörytetään identiteetinhallinta järjestelmään, jonka takana on kohdejärjestelmät. Kohdejärjestelmiin annetaan oikeuksia käyttäjälle työrooliin liittyen. Mikäli HR ei välttämättä riitä ainoaksi lähdejärjestelmäksi, muuttuu prosessi monimutkaisemmaksi. Olisi hyvä, että joudutaan tekemään vain yhteen paikkaan muutos, josta muutokset siirtyvät automaattisesti muihin järjestelmiin. Henkilön poistuessa talosta täytyy oikeudet poistaa. Kun muutos tehdään yhdestä järjestelmästä, saadaan oikeudet deprovisioitua takaisin päin. Muutos HR-järjestelmästä välittyisi muihin järjestelmiin ja oikeudet poistettaisiin, jolloin tietoturva paranee. Integraatioiden avulla voidaan viedä käyttäjätietoja HR järjestelmän, ADn, ERPin ja CRMn järjestelmän välillä.

IAMin sisällä on erilaisia prosesseja, joita ovat onboarding, offboarding ja Joiner-Mover-Leaver. Mover-prosessissa henkilö voi vaihtaa roolia yrityksen sisällä, mikä vaikuttaa oikeuksiin. Uudelleen palkkaus lasketaan myös mover-prosessiksi, jolloin henkilölle voidaan antaa jo suljetut käyttäjätunnukset takaisin. Vaikka joiner on osa onboardingia ja leaver osa offboardingia, on ne eritelty omiksi prosesseiksi. Joiner-Mover-Leaver ajatellaan koskevan enemmän käyttäjiä ja muutoksia käyttäjäkunnassa.

Onboarding prosessia on, kun tulee kokonaan uusi käyttäjä tai organisaatio. Esihenkilö tai vastuuhenkilö huolehtii, että identiteetti tulee perustettua oikein HR järjestelmään, mistä se integraation avulla kulkeutuu AD:hen. Onboarding prosessissa käyttäjän annetaan pääsyt roolin kannalta relevantteihin paikkoihin. Käyttäjän roolin ja vastuiden muuttuessa pitää ylläpitää käyttäjän oikeuksia. Pääsyt tulisi jakaa ryhmien kautta eikä niin, että lisättäisiin yksitellen käyttäjälle oikeuksia. Kun käyttäjä tai organisaatio poistuu, on se silloin offboarding prosessi. Offboarding prosessissa huolehditaan käyttäjän oikeuksien poistaminen ja käyttäjätilin sulkeminen.

Mohammed (2017) mukaan käyttäjän luomisen jälkeen on provisioinnin vuoro. Provisioinnissa uusi henkilö tulee organisaatioon, olemassa oleva työntekijä siirtyy toiselle osastolle tai olemassa oleva työntekijä lähtee yrityksestä. Provisiointi sisältää käyttäjän koko elinkaaren vaiheiden ylläpidon. Käyttäjän tietoja ja oikeuksia tulee päivittää niiden

muuttuessa. Kun käyttäjä ei enää tarvitse oikeuksiaan tulee oikeudet poistaa. Haastatteluissa nousi esille, että provisioinnit ovat oleellinen osa identiteettihallintaa. Provisiointi voi olla molempiin suuntiin, lähdejärjestelmiin tai kohdejärjestelmiin.

Mikäli identiteetti on jo olemassa, voidaan suoraan siirtyä identiteetin tunnistamiseen (Mohammed 2017). Tunnistuksessa käyttäjä yksilöidään omaksi identiteetiksi. Tunnistamiselle on useita eri mekanismeja ja tapoja.

Kun identiteetti on tunnistettu seuraa identiteetin todennus eli autentikointi. Identiteetinhallinta todentaa käyttäjän pyytämällä tunnistetietoja, käyttäjän pyytäessä pääsyä resurssiin. Tunnistetiedot voivat olla käyttäjänimi ja salasana, digitaalinen varmenne, älykortti tai biometrisia tietoja (AbidHussain & Praveen Kumar Sharma 2020). Todennuksessa varmistetaan, että käyttäjä on se, kuka hän väittää olevansa. Haastateltavan mukaan, todennus prosessien avulla tarkastetaan, että käyttäjät ovat heitä keiden heidän pitää olla ja käyttöoikeudet ovat kohdillaan. Yrityksellä tulee olla tapa tehdä autentikointi. Sen jälkeen käyttäjälle valtuutetaan sopiva määrä käyttöoikeuksia käyttäjän identiteetin ja attribuuttien perusteella (AbidHussain & Praveen Kumar Sharma 2020).

Todennuksen jälkeen seuraa identiteetin valtuutus (Mohammed 2017). Valtuutus on prosessi, jossa myönnetään käyttöoikeudet tiettyihin resursseihin tietylle identiteetille (Trnka, Cerny & Stickney 2018). Käyttäjälle myönnetään oikea käyttöoikeus taso. Käyttäjällä on tietty vastuu toimia ennalta sovittujen sääntöjen mukaan käyttäessään järjestelmiä, dataa, sovelluksia tai tiloja. (Yang *et al.* 2014) Identiteetin- ja pääsynhallinta antaa oikeat käyttöoikeudet oikeille käyttäjille oikeaan aikaan ja varmistaa, että käyttäjät ovat niitä, joita he sanovat olevansa autentikoinnin kautta (AbidHussain & Praveen Kumar Sharma, 2020).

Haastatteluissa nousi esille, kuinka IAMin logitiedot tuottavat tärkeää tietoa käyttäjistä, valtuuksista ja pääsyistä raportoinnin, tietoturvan, liiketoiminnan kehittämistä varten sekä pystytään vastaamaan ulkoisiin vaatimuksiin raportoinnissa. Seuranta- ja raportointitoimenpiteiden avulla pystytään ennakoimaan ja ennustamaan altistumisia riskeille. Raportit tarjoavat auditoinnissa käytettäviä mittareita. Tarkastuslokit ovat tärkeä osa IAM-prosessia. Prosessien ja tukijärjestelmien pitäisi pystyä tarjoamaan raportteja, jotka sisältävät yksityiskohtaisia käyttöoikeuksia ja tarkastuksia. Sekä datan, että prosessin raportointi on yhtä tärkeää. (CSA 2012) Tiedonkeruu, raportointi ja käyttöoikeuksien tarkistus ovat kaikki automatisoitavissa IAM-hallintaratkaisujen avulla. Vaatimustenmukaisuuden auditoinnit tuovat esiin puutteet ja tarjoavat organisaatioille mahdollisuuden korjata haavoittuvuuksia ja ratkaista vaatimustenmukaisuusrikkomukset. (Mohammed 2017)

Identiteetinhallintajärjestelmä tallentaa tietoja, joiden avulla se tarjoaa valtuutuksen, todentamisen, käyttäjien rekisteröinnin, salasanojen hallinnan, auditoinnin, keskushallinnon ja delegoidun hallinnan. Identiteetti hallintajärjestelmä tallentaa tietoja resursseista, joita voivat olla muun muassa sovellukset, tietokannat, laitteet, tilat, ryhmät, käyttöjärjestelmät, ihmiset, politiikka ja roolit. Järjestelmä tunnistaa ja valtuuttaa sekä sisäiset että ulkoiset käyttäjät. (AbidHussain & Praveen Kumar Sharma 2020)

Miten käyttäjähallinta vaikuttaa tietoturvaan?

Identiteetin- ja pääsynhallinta on yksi tärkeimmistä osista tietoturvan ylläpitämisessä pilvessä (Mohammed 2019). Identiteetin- ja käyttöoikeuksien hallinta vastaa vaatimukseen varmistaa asianmukainen pääsy resursseihin (Alhija 2020). Identiteetinhallinnan avulla voidaan parantaa toimintaprosesseja, parantaa raportointikykyä ja varmistaa säännösten noudattaminen (Mohammed 2017). Kyberturvallisuuden pääpilarit muodostuvat, kun tunnetaan resurssit, käyttöoikeudet ja identiteetit. Kyberturvallisuuden takaamiseksi tavoitteena on varmistaa, että ihmisillä on asianmukainen pääsy resursseihin, organisaatio tietää aina, kenellä on pääsy mihinkin, miten pääsyä voidaan käyttää ja onko pääsy käytäntöjen mukainen. (Haber & Rolls 2019)

Tietoturvakehys identiteetinhallinnalle nimeltä ” The Five A’s of Enterprise IAM” helpottaa ja tekee identiteetinhallinnasta turvallisempaa. Viisi A:ta koostuu todennuksesta (Authentication), valtuutuksesta (Authorization), hallinnasta (Administration), tarkastuksesta (Audit) ja analytiikasta (Analytics). Todennuksella vahvistetaan, onko käyttäjä se, kuka sanoo olevansa. Valtuutus antaa oikeudet suorittaa toiminto, mikä perustuu todentamiseen. Identiteetinhallinnan tehtävä on keskittää hallintaominaisuuksien tarjoaminen kaikille pääsyjärjestelmille. Tarkastus prosessi voi olla käyttäjien pääsyn varmentamisohjelma, määritellä ja toteuttaa ennaltaehkäisevää ja etsivää politiikkaa tai todistaa hallintoprosessien ja -käytäntöjen määritelmät, käytössä olo ja niiden noudattaminen. Kattava analyysi IAM-järjestelmän toiminnasta antaa tietoa toiminnallisuus ja turvallisuus ominaisuuksista. (Haber & Rolls 2019)

Haastatteluiden tuloksena selvisi, että käyttäjä on suuri tietoturva riski. Heikolla käyttäjähallinnalla luodaan paljon riskejä. Sen takia käyttäjiä ei tulisi päästää resursseihin, mihin he eivät tarvitse oikeuksia. Käyttäjiä ei saa päästää sellaisiin paikkoihin missä käyttäjät pystyisivät tekemään vahingossa tai tarkoituksella paljon tuhoa. On riskienhallintaa, olla jakamatta pääsyjä liikaa. Pääsyjä tulisi jakaa vaan ja ainoastaan todelliseen tarpeeseen. Tietoturvallisuuden kannalta on tärkeää, että tiedetään, miten tieto liikkuu ja kenellä on pääsy, sekä auditoidaan sitä. Mikäli vanhalla työntekijällä on tarvetta saada jotain tuhoa

aikaiseksi, on se mahdollista, mikäli käyttäjätunnukset toimivat työsuhteen päättymisenkin jälkeen. Tietoturvallisuuteen vaikuttaa paljon myös käytössä olevat prosessit. Työkalu itsessään ei paranna tietoturvallisuutta. Tietokannoissa voi olla lokeja, joiden perusteella voidaan selvittää ketkä ovat käyneet tietoja tarkastelemassa.

Mitä ongelmia käyttäjähallinnassa esiintyy?

Tutkimuksen tuloksena selvitettiin, mitä ongelmia käyttäjähallinnassa yleisesti esiintyy. Organisaatiot ovat usein havahtuneet siihen, että käyttäjähallinta on liian hankalaa tai siihen menee liikaa aikaa. Käyttäjä ryhmien jäsenten hallinta on haasteellista manuaalisen lisäämisen takia (Centero Oy 2012). Manuaalisen prosessin takia on mahdollista, että vääriä oikeuksia jaetaan vahingossa (Francis 2021). Kun yksinkertaiset ja toimivat prosessit puuttuvat voidaan joutua hoitamaan jokainen pääsyoikeus niin kuin pitäisi hoitaa poikkeustilanteet. Tämä tekee käyttäjähallinnasta raskasta ja vie älyttömästi aikaa. Se myös työllistää useita ylimääräisiä työntekijöitä, kun jokainen käyttöoikeustapaus hoidetaan poikkeustapauksena. Mikäli järjestelmäasiantuntija tai joku muu avainasemassa oleva henkilö on poissa, pitkittyy oikeuksien saaminen. Isoissa organisaatioissa usein käyttöoikeuksia hallinnoiva henkilö ei edes välttämättä tiedä mitä dataa resurssi sisältää, minkä takia on vaikeaa tehdä päätöksiä, voidaanko käyttäjälle myöntää oikeudet kyseiseen resurssiin (Centero Oy 2012).

Ison kuvan puuttuminen aiheutuu, kun ei mietitä miten käyttäjähallinta yleisesti toteutettaisiin, vaan käyttäjähallinta toteutetaan projektikohtaisesti omilla toimintatavoilla. Tällöin syntyy useita eri toimintatapoja ja paljon ryhmiä. Ryhmät eivät välttämättä ole millään tavalla linjassa ja ajan saatossa kenelläkään ei ole tietoa mitkä ryhmät ovat aktiivisia ja mihin niitä käytetään.

Toistuva haaste yrityksien sisäisissä järjestelmissä on, ettei ole RBAC-malli tai ei ole DRBAC-mallia, mitä voitaisiin käyttää käyttäjän provisiointiin ja deprovisiointiin eri järjestelmien välillä. IAM käyttöönotossa ongelmia on aiheuttanut se, että on ajateltu, että kyseessä on vain tuote, mikä otetaan käyttöön ja sillä ratkaistaan kaikki ongelmat. IAM projekteissa täytyisi olla ajatusmalli, jossa ymmärretään, että kyseessä ei ole pelkän teknologian käyttöönotto vaan paljon muutakin. Käyttäjän onboarding ja offboarding prosessin toteuttaminen turvallisesti ja oikea-aikaisesti on ollut haasteellista (AbidHussain & Praveen Kumar Sharma 2020).

Kun prosessit ovat jollain tasolla hallussa, niin seuraava ongelma on organisaation data. Jokaisella organisaatiolla on oma käyttötapa datalle. Datan laadusta aiheutuu paljon ongelmia. Ongelmana usein on, että nykyiset oikeuksienvalvontamenetelmät perustuvat

oletuksiin eikä täysin dataan (Mohammed 2021). Haastatteluissa huomattiin, että dataa hyödyntäessä suurimmat ongelmat yleensä johtuvat datan puutteellisuudesta tai päällekkäisyydestä, mikä tekee automaation puolesta hankalampaa toteuttaa. Prosessien ja datan ymmärrys täytyy olla kunnossa, jotta IAM projekti voi onnistua. Haastavinta IAM projektissa on se kaikki muu tekniikan ympärillä.

Yleinen ongelmia aiheuttava tapahtuma on, kun käyttäjät vaihtavat työtehtävää yrityksessä ja vanhojen oikeuksia jää käyttäjille roikkumaan. Käyttäjäoikeuksien jäädessä roikkumaan tarpeettomana aiheutuu riski, mikäli käyttäjä siirtyy jossain vaiheessa toisen yrityksen palvelukseen, ja pääsee edelleen vanhan yrityksen tietoihin käsiksi. Käyttäjien oikeuksien poistamiselle pitäisi olla prosessi. Ongelmana on myös menettelyjen puute tai nykyisten menettelyjen tehottomuus, kun työntekijöiden asema organisaatiossa muuttuu (Lee & Sawyer 2019). Single sign-onin tai integraatioiden puuttuminen järjestelmien välillä aiheuttaa sen, että täytyy luoda omia käyttäjätunnuksia eri järjestelmille. Tämä tekee käyttäjähallinnasta raskaampaa, kun on enemmän tunnuksia hallittavana. Abid-Hussain ja Praveen Kumar Sharma (2020) huomasivat, että organisaatioiden on vaikea seurata erilaisia kirjautumistunnuksia, joita työntekijät ylläpitävät työsuhteensa aikana. Käyttöoikeuksien hallinnassa ongelmia saattaa aiheuttaa vaikeus selvittää kenellä on pääsy mihinkin.

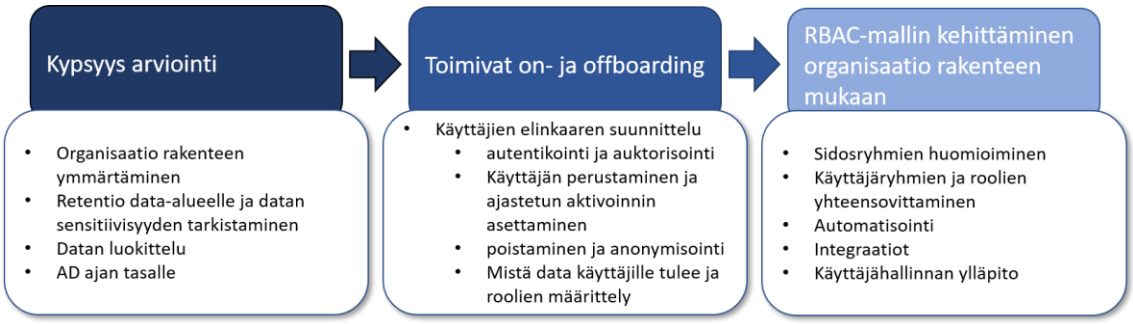
Ongelmia konserni tasoisen organisaation käyttäjähallinnassa saattaa syntyä, kun ei ymmärretä eri käyttäjäoikeus tasoja. Voi helposti käydä niin, että ollaan liian tiukkoja oikeuksien antamisessa. Ongelmia on aiheutunut myös, kun tytäryritykset ovat luoneet omia toimintatapoja ja konserni jalkauttaa uuden toimintamallin, mikä saattaa rikkoa paikallisesti kehitettyjä prosesseja. Konsernin sisällä saattaa aiheutua ongelmia, kun joudutaan käyttämään maantieteellisesti eri alueilla eri järjestelmiä. Esimerkiksi kohdeyrityksessä oli huomattu, että EU-rajojen sisäpuolella käytetään yhtä HR-sovellusta. Mutta EU:n ulkopuoliset maat käyttävät eri HR-järjestelmää. Tämä niin tulee haasteita käyttää vain yhtä HR-järjestelmää, jolloin ratkaisu on usein käyttää montaa eri HR-järjestelmää. Usean HR-järjestelmän käyttö konsernissa tuottaa haasteita hallinnon tasolle. Monimutkaiset prosessit aiheuttavat kuitenkin ongelmia enemmän kuin yrityksen koko. Mikäli yrityksen rakenne on selvillä ja rakennetta on totuttu käyttämään, ei yrityksen koosta pitäisi aiheuttaa ongelmia.

Miten toteuttaa tehokas ja käyttäjäystävällinen käyttäjähallinta konsernin tasoisessa organisaatiossa, jossa useita järjestelmiä ja liiketoimintayksiköitä?

Tehokkaan ja käyttäjäystävällisen käyttäjähallinnan toteuttamisessa täytyy käyttäjähallintaprosessin suunnitteluun käyttää paljon aikaa ja vaivaa. Suunnittelua ei tulisi laiminlyödä. Organisaation tulisi hahmottaa oman käyttäjähallinnan iso kuva, jotta saadaan prosessista kokonainen. Roolipohjainen käyttäjähallinta koettiin erittäin hyödylliseksi tavaksi toteuttaa käyttäjähallinta. Jotta roolipohjainen käyttäjähallinta voidaan toteuttaa ja suunnitella, on ymmärrettävä organisaation rakenne ja dokumentoida se selkeästi. Automatisoitu käyttäjähallinta vähentää työtä ja nopeuttaa prosessia, mikä kuitenkin vaatii hyvin suunnitellun prosessin.

Haastatteluiden pohjalta saatujen vastausten ja teorian perusteella luotiin yhteenveto, mitä tulee huomioida käyttäjähallintaa suunnitellessa. Yhteenveto on esitetty kuvassa 23. Kaikki lähtee liikkeelle sen hetkisen tilan selvittämisestä. Kypsyys arviolla saadaan tärkeää tietoa missä ollaan ja mihin halutaan päästä. Organisaatiorakenteen ymmärtäminen on erittäin tärkeää onnistuneen käyttäjähallinnan kannalta. On selvitettävä, miten sen hetkinen AD-ryhmä hierarkia vastaa organisaation rakennetta. Ryhmien hierarkian tulisi vastata organisaatiorakennetta mahdollisimman hyvin. Ryhmähierarkia täytyy suunnitella huolellisesti, jotta voidaan varmistaa, että tiedot pysyvät turvassa ja samalla parantaa käyttäjähallinnan tehokkuutta (DNSstuff 2019). Ryhmien suunnittelussa on paljon muutakin muistettavaa. Suunnitellessa sisäkkäisiä ryhmiä on huolehdittava lupien periytymisistä (DNSstuff 2019).

Data-alueen retentiossa tehdään selvitys, miten, kuinka kauan, missä ja minkä takia tietoja säilötään (Callaghan 2020). Datan sensitiivisyys on tarkistettava, jotta arkaluontoista ja henkilödataa käsitellään oikein. Kypsyys arviointi vaiheessa olisi myös hyvä selvittää AD:n tila. Onko AD:ssa käyttäjätiedot oikein tai ylipäätään onko käyttäjille määritelty tarpeeksi tietoja. Tietoja voidaan pakottaa täytettäväksi käyttäjää luodessa. Mikäli tilanne on huono, on kannattavaa päivittää AD ajan tasalle ja määrittää tulevaisuuden kannalta toimintamalli, miten jatkossa toimitaan. Hyvä tapa on pakottaa täyttämään tarvittavat tiedot käyttäjälle tilin luonnin yhteydessä. Näin voidaan jatkossa varmistaa, ettei tilanne lähde huonompaan suuntaan. On kuitenkin huomioitava, että käyttäjien roolit ja tiedot voivat ajan myötä muuttua. Tietojen päivittämiselle pitäisi olla oma toimintamalli, minkä mukaan tulisi toimia.



Kuva 23 Haastateltavien ja teorian määrittämät vaiheet käyttäjähallinnan suunnitteluun

Kypsyysarviointiin olisi voitu sisällyttää onboarding ja offboarding prosessien toimivuuden tarkistaminen, mutta tultiin siihen tulokseen, että ne ovat enemmän oma kokonaisuus. Onboarding ja offboarding prosessien läpikäynti ja päivittäminen puutteita löydettäessä on suositeltavaa. On ymmärrettävä käyttäjän elinkaari, jotta voidaan suunnitella toimivat prosessit. Sen lisäksi täytyy ymmärtää mitä vaiheita on käyttäjän luonnista käyttäjän tilin poistamiseen. Käyttäjätili luodaan ja sille annetaan tarvittavat tiedot. Käyttäjätilin aktivointi voidaan ajastaa työsuhteen ensimmäiselle päivälle, jolloin käyttäjällä ei ole pääsyjä ennen työnsuhteen alkamista mutta on käyttäjätili jo ensimmäisenä päivänä. On käytävä läpi, miten käyttäjä tunnistautuu kirjautuessaan sisälle ja miten pääsyoikeuksien valtuutus tapahtuu.

Käyttäjän elinkaareen mahtuu myös käyttäjän päivittämistä. Kuten aikaisemmin jo käytiin läpi, voivat käyttäjän tiedot muuttua. Käyttäjätiliä on päivitettävä ajan myötä. Käyttäjätilin tullessa elinkaaren loppuun, on käsiteltävä, miten tili poistetaan ja anonymisoidaan. Käyttäjästä on jäänyt käytön aikana jälkiä eri järjestelmiin, eikä kaikkia jälkiä voida poistaa. Tämän takia on suunniteltava miten anonymisointi onnistuu käyttäjän poistuessa. On tiedettävä mistä data käyttäjille tulee. Yleensä data saattaa tulla HR järjestelmästä integraation avulla muihin järjestelmiin. On kuitenkin tiedettävä mistä data tulee, syöttääkö joku sen manuaalisesti vai tuleeko se jostain toisesta järjestelmästä. Mahdollisten roolien määrittely olisi hyvä jo tehdä käyttäjähallinnan suunnittelu vaiheessa. Olisi hyvä selvittää mitä rooleja tarvitaan, mitä vastuita rooleille annetaan, ja mille työtehtävälle mikäkin rooli määritellään.

Kun käyttäjän elinkaari on ymmärretty ja suunniteltu, voidaan sovittaa ne omiin onboarding ja offboarding prosesseihin. Prosesseissa on käytävä läpi, miten käyttäjän tullessa organisaatiolle töihin luodaan identiteetti, miten käyttäjälle annetaan oikeuksia ja perehdytetään organisaation säädöksiin ja politiikkoihin sekä vastavuoroisesti, miten prosessi kulkee, kun poistutaan organisaation työtehtävistä. Onboarding prosessi sisältää useita vaiheita, vaikka prosessi onkin yritys kohtainen (Krasman 2015). Vaikka prosessit ovat

yrityskohtaisia, on runko niissä hyvinkin samanlainen. Onboarding prosessi on dokumentoitava ja toistettava uusien käyttäjien kohdalla (Krasman 2015). Näin voidaan varmistaa, että kaikkien uusien käyttäjien kohdalla toimintaan saman prosessin mukaisesti. Onboarding prosessi alkaa siitä, kun uusi työntekijä hyväksyy työtarjouksen (Krasman 2015). Offboarding prosessiin pätee myös dokumentointi ja toistettavuus. Offboarding prosessi on käänteinen onboarding prosessiin nähden. Siinä käydään läpi mitä poistuvan käyttäjän kohdalla tulisi tehdä.

Nykytilanteen ja prosessien tarkistamisen jälkeen voidaan siirtyä roolipohjaisen käyttäjähallinnan suunnittelun pariin. RBAC-malli tarvitsee sen, että organisaatio rakenne on selvitetty ja käyttäjille on määritelty roolit ja tarvittavat tiedot. Koska nämä on tehty aikaisemmissa vaiheissa suunnittelua, on RBAC-mallin kehittäminen helpompaa ja selvempää. Kaikkien sidosryhmien huomioiminen ja sidosryhmien näkökulmien ymmärtäminen kannattaa selvittää keskustelemalla sidosryhmien kanssa. Sidosryhmiä ovat esimerkiksi eri järjestelmien järjestelmäasiantuntijat, Service Desk, tietoturvaosasto ja käyttäjät. Organisaatiorakenteen pohjalta suunniteltiin AD-ryhmät ja tarvittavat tiedot. On tarkistettava, että ryhmähierarkia, roolit ja organisaatiorakenne vastaa toisiaan ja tehtävä muutoksia ryhmiin ja rooleihin, mikäli ne eivät sovi yhteen. Kun on yhteensovitettu ryhmät ja roolit, on helpompi lähteä suunnittelemaan roolipohjaisen käyttäjähallinnan automatisointia.

Automatisoinnin suunnittelussa selvitetään, mitä halutaan lähteä automatisoimaan ja miksi. Jos kyseessä on esimerkiksi oikeuksien päivittyminen roolin mukaan, tarvitaan selkeä suunnitelma ennen kuin teknistä ratkaisua lähdetään toteuttamaan. Kun on selkeä suunnitelma mitä automatisoidaan ja miten, on integraation suunnittelu enää teknistä osuutta vaille valmis. Kun käyttäjähallintaprosessiin liittyen kaikki on suunniteltu, täytyy vielä suunnitella, miten käyttäjähallintaa ylläpidetään. On tehtävä selkeät ohjeet siitä, kuka hoitaa käyttäjien luonnin, pyytää, myöntää ja hyväksyy oikeuksia ja kuka poistaa oikeuksia, mikäli kyseisiä vaiheita ei ole automatisoitu. Ohjeissa tulisi olla myös kohta, miten ongelmatilanteissa toimitaan.

7.2 Työn arviointi ja rajoitteet

Työn menetelmät pyrittiin kirjottamaan mahdollisimman hyvin ja tarkasti, jotta työ olisi mahdollista toteuttaa uudelleen esimerkiksi toiselle yritykselle. Aineiston analyysi on esitelty myös tarkasti, jotta on mahdollista tietää, miten tulokset on saatu. Keräysmenetelmän sekä haastattelurungon esittely mahdollistaa tutkimuksen siirrettävyyden. Haastat-

telut olivat anonymisoitu, mikä estää tässä työssä haastateltujen haastateltavien haastattelun uudelleen. Myös haastattelutallenteiden ja haastatteluiden purkutekstien uudelleen hyödyntäminen on luottamussyistä estetty.

Käyttäjähallinnan ongelmat ja haasteet olivat tutkimustulosten mukaan todella saman tyyppisiä. Mikäli toteutettaisiin vastaava tutkimus, todennäköisesti saataisiin erittäin saman tyyppisiä tuloksia. Tässä työssä haastateltavien vastaukset olivat hyvinkin samanlaisia, vaikka haastateltavien työtehtävät erosivat hieman toisistaan, mikä osoittaa sen, että käyttäjähallinnassa oli törmätty hyvin samanlaisiin ongelmiin ja ratkaisuehdotukset olivat työtehtävistä riippumatta hyvinkin samankaltaisia. On kuitenkin mahdollista, että tulevaisuudessa esiintyy kokonaan uudenlaisia ongelmia, mitä vielä ei esiintynyt.

Tutkimus on toteutettu diplomityöohjeita noudattaen ja jaettu selkeiksi osakokonaisuuksiksi. Työn tavoitteet esiteltiin tutkimuksen ensimmäisessä luvussa. Tavoitteisiin vastattiin tutkimuksen viimeisessä luvussa. Vaikka tutkimus aihe oli kohdeyrityksen nykytilan kohdalta rajattu BI-alueen järjestelmien käyttäjähallinnan parantamiseen, olivat saadut tuloksen yleisesti käyttäjähallinnan kehittämisestä. Teoriaosuudessa käytettiin mahdollisimman uusia lähteitä, jotta voitiin olla varmoja, että teoria olisi ajankohtainen.

Tutkimuksen tulokseksi saatiin, että roolipohjainen käyttäjähallinta olisi kannattava tapa toteuttaa käyttäjähallintaa. Lähteitä lukiessa ja teoriaosuutta kirjoittaessa ei osattu nostaa enemmän esille mahdollisia relevantteja aiheita, minkä takia kaikkia mahdollisia tärkeitä aiheita ei tullut käsiteltyä. Yhtenä esimerkkinä on roolipohjainen käyttäjähallinta. CSA (2012) mukaan roolipohjainen pääsynhallinta on osa identiteetin- ja pääsynhallintaa. Roolipohjaisuus oli listattuna muiden osa-alueiden mukana, mutta sitä ei ollut avattu teoriassa sen enempää. Mikäli teoriassa olisi pohdittu roolipohjaista käyttäjähallintaa enemmän, olisi haastattelukysymyksiin saatettu osatta ottaa roolipohjaisuudesta kysymyksiä. Ja tuloksissa voisi olla tarkemmin kuvattuna miksi roolipohjaisuus on hyvä tapa toteuttaa käyttäjähallinta. Mahdollisesti olisi myös saatu muun muassa roolipohjaisuuden haasteista enemmän tietoa. Nyt kuitenkin roolipohjaisuudesta osattiin kysyä ainoastaan, jos haastateltavan vastauksessa roolipohjaisuus oli pääosassa. Tällöin saatettiin kysyä lisää ja tarkentavia kysymyksiä roolipohjaisuudesta.

Haastattelut onnistuivat suhteellisen hyvin. Haastatteluissa käytettiin suunniteltua kysymysrunkoa pohjana. Haastatteluita suunnitelleessa pohdittiin kahta eri kysymysrunkoa, kohdeyrityksen edustajille ja tutkijan työnantajayrityksen edustajille. Valittu tapa oli loppujen lopuksi erittäinkin toimiva, sillä haastateltavat pääsivät vastaamaan yrityksestä riippumatta samoihin kysymyksiin. Näin saatiin vertailukelpoisia tuloksia kohdeyrityk-

sestä ja yleisesti muista yrityksistä. Osassa haastatteluissa ei ehditty käymään yhtä paljon haastattelukysymyksiä läpi, koska haastateltava vastasi niin laajasti kysymyksiin. Tämä toisaalta oli hyvä asia, sillä saatiin kattava vastaus kysyttyyn kysymykseen mutta toisaalta se vähensi kysyttävien kysymysten määrää. Se taas vaikutti siihen, että tiettyihin kysymyksiin ei saatu yhtä monelta haastateltavalta vastausta, koska kysymyksiä ei keritty kysyä kaikilta. Mikäli huomattiin, että haastateltava vastasi erittäin kattavasti kysymyksiin ja tiedettiin, että kysymysrungon alkupäässä oleviin kysymyksiin oli saatu jo kattavasti vastauksia, saatettiin siirtyä suoraan kysymyksiin, joihin ei oltu kaikkien aikaisempien haastateltavien kanssa päädytty. Näin saatiin tasoitettua tilannetta ja saatiin vastauksia myös niihin kysymyksiin, mitkä olisivat muuten ajan puutteen takia saattanut jäädä kysymättä. Eri aihealueiden painottaminen oli sallittua, koska kyseessä oli puolistrukturoitu haastattelu. Puolistrukturoidussa haastattelussa eri teemojen painottaminen haastattelu kohtaisesti on sallittua (Saunders et al. 2016).

Haastateltavien valinta onnistui kohtuullisen hyvin. Haasteltavat olivat poimittu kohdeyrityksestä ja tutkijan työnantajayrityksestä. Haastateltavat olivat useasta eri taustasta, mikä teki kerätystä aineistosta kattavaa. Kohdeyrityksen haastateltavat peilasivat vastauksiaan kohdeyrityksen tilanteeseen ja kokemiin ongelmiin, joita oli käyttäjähallinnan monimutkaisuus ja oikeuksien myöntäminen oikeissa määrin. Tulokset osoittivat, että kohdeyrityksen ongelmat olivat hyvinkin saman tyyppisiä kuin muillakin yrityksillä koetut ongelmat. Mikä vahvisti sitä, että haastatteluissa esille nousseet kehitysehdotukset vastaavat hyvinkin kohdeyrityksen ongelmiin. Haastateltavat pystyivät vastaamaan haastattelu kysymyksiin tarkasti ja antoivat monipuolisia vastauksia. Joidenkin haastateltavien kohdalla osa kysymyksistä oli haastateltavan tietämyksen ulkopuolta, jolloin siirryttiin suosiolla vain seuraavaan kysymykseen. Vaikka haastateltavilla oli kokemusta eri näkökulmista käyttäjähallintaan, olivat vastaukset saman tyyppisiä ja tulokset täydensivät toinen toisiaan. Haastateltavat saattoivat mainita samoja asioita painottaen kukin eri asiaa. Kuitenkin roolipohjaisuus oli vastausten keskiössä niiden haastateltavien kesken, jotka roolipohjaisuuden olivat nostaneet esille.

7.3 Tulevaisuuden tutkimuskohteet

Tutkimuksen aiheen rajaus jätti jatko tutkimus aiheille hyvin tilaa. Tutkimuksen jatko tutkimus aiheet nousivat esille tutkimuksen kehitysehdotuksista sekä syventymällä tutkimus aiheen eri osa-alueisiin. Tässä tutkimuksessa tutkittiin käyttäjähallintaa yleisesti ja pintapuolisesti. Mikäli nyt lähdettäisiin tekemään jatko tutkimusta, voitaisiin syventyä tar-

kemmin johonkin käyttäjähallinnan osa-alueeseen. Tutkimuksessa saatu tietämys käyttäjähallinnasta auttaisi syventymään tarkemmin johonkin tiettyyn käyttäjähallinnan osaan.

Tutkimuksen tulosten mukaan hyvinkin monella yrityksellä on vastaavia ongelmia. Käyttäjähallinta laiminlyödään hyvinkin useissa tapauksissa, minkä takia aihe onkin hyvin tärkeä. Jatkossakin on varmasti yrityksiä, joilla on samoja ongelmia. Tulevaisuudessa varmasti tulee esille myös ongelmia, mitä ei tässä työssä esiintynyt. Mahdollisiin ongelmiin tarvitsee löytää ja kehittää uusia ratkaisuja jatkossakin. Tutkimusongelma saattaisi olla hyvinkin samanlainen mutta teknologian kehityksen myötä saattaisi olla hyvinkin uusia tuloksia. On myös hyvin mahdollista, että teknologian kehityksen myötä tutkimusongelma saattaisi olla erilainen.

Tutkimus toteutettiin kohdeyrityksen BI alueen järjestelmille. Mielenkiintoista olisi tietää onko samanlaisia ongelmia kohdeyrityksellä muidenkin järjestelmien käyttäjähallinnassa. Tämä olisi hyvä jatko tutkimus aihe. Tämä tutkimus toteutettiin konsernia koskevalle BI-alueelle. Olisi myös mielenkiintoista tutkia tytäryrityksien käyttäjähallintaa. Esiintyykö samoja ongelmia konserni tasolla ja tytäryritys tasolla? Onko tytäryrityksillä lokaaleita järjestelmiä ja käyttäjätunnuksia paljon? Miten ne on hoidettu ja esiintyykö niiden kanssa mitään ongelmia? Eri tytäryritysten käyttäjähallinnan ratkaisuja olisi mielenkiintoista vertailla. Eroaako ne paljon toistensa tai konsernin asettamista tavoista?

Tässä työssä ei osattu nostaa roolipohjaista käyttäjähallintaa tutkimuksen keskiöön. Jatkotutkimus aiheena toimisi hyvin roolipohjaisen käyttäjähallinnan toteuttaminen. Tässä työssä tulokset eivät kertoneet tarkasti mitä pitäisi huomioida roolipohjaisen käyttäjähallinnan toteuttamisessa. Ei myöskään käsitelty onko valmiita työkaluja roolipohjaisen käyttäjähallinnan toteuttamiseen. Jatko tutkimuksissa voitaisiin keskittyä edellä mainittuihin aiheisiin. Myös roolipohjaista käyttäjähallintaa voisi vertailla muiden vaihtoehtoisten tapojen kanssa, mikäli sellaisia on.

Onboarding ja offboarding prosesseista yritettiin löytää selkeää runkoa käyttäjähallinnan näkökulmasta, mikä olisi hyvä pohja yrityksille prosesseja suunnitellessa. Tallaista ei kuitenkaan löydetty tätä työtä tehdessä. Aihetta olisi hyvä tutkia lisää ja muodostaa suunnittelua varten toimiva runko, jota yritykset voisivat soveltaa suunnitellessa omia onboarding ja offboarding prosesseja. Kyseisistä prosesseista löytyi tutkimuksia mitkä sisälsivät vaiheita uuden työntekijän palkkauksesta perehdyttämiseen, mutta tutkimuksissa ei havaittavasti käsitelty prosesseja käyttäjähallinnan ja oikeuksien näkökulmasta.

Yrityksellä oli ongelma käyttäjä identiteettien tietojen ylläpitäminen. AD:ssa käyttäjätiedot saattoivat olla vanhentunutta tai puutteellisia. Tätä ongelmaa olisi hyvä tutkia syvemmin.

Jotta tiedot olisivat ajan tasalla, tulisi muodostaa jokin näköinen toimintamalli tietojen päivittämiselle. Roolipohjaisuutta miettien on tärkeää selvittää mitkä tiedot ovat vaadittavia, jotta käyttäjähallintaa voidaan roolien perusteella toteuttaa. Tietojen pakottaminen käyttäjän luonnin yhteydessä mahdollistaisi käyttäjistä riittävien tietojen saannin. Pitäisi tietää mitkä tiedot ovat tarvittavia ja miten niitä päivitetään käyttäjän elinkaaren myötä, jotta roolipohjainen käyttäjähallinta on mahdollista.

LÄHTEET

AbidHussain and Praveen Kumar Sharma (2020) 'Defence Mechanism for Access Management in Cloud Computing', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* [Preprint].

Ahmad, M. *et al.* (2015) 'Oblivious user management for cloud-based data synchronization', *Journal of Supercomputing*, 71(4), pp. 1378–1400. Saatavilla: https://doi.org/10.1007/s11227-014-1369-5.

Alhija, M. (2020) 'Cyber security: Between challenges and prospects', pp. 1019–1028. Saatavilla: https://doi.org/10.24507/icicelb.11.11.1019.

Amaya, N. (2017) *Active Directory Tutorial - A Comprehensive Overview of AD*, *Tutorials*. Saatavilla at: https://ittutorials.net/microsoft/windows-server-2016/active-directory/ (Luettu: 21.2.2022).

Amazon Web Services (2015) *How to Connect Your On-Premises Active Directory to AWS Using AD Connector*, *Amazon Web Services*. Saatavilla at: https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/ (Luettu: 24.2.2022).

Arley, A. (2021a) 'Active Directory Basics', *Medium*. Saatavilla at: https://medium.com/@alan6arley/active-directory-basics-f468687cc3a6 (Luettu: 21.2.2022).

Arley, A. (2021b) 'Azure AD Group Management', *Medium*. Saatavilla: https://medium.com/@alan6arley/azure-ad-group-management-eac8a8707a27 (Luettu: 22.2.2022).

Auth0 (no date) *Role-Based Access Control*, *Auth0 Docs*. Saatavilla: https://auth0.com/docs/ (Luettu: 16.5.2022).

Berkouwer, S. (2019) *Active Directory Administration Cookbook*. Packt Publishing. Saatavilla: https://learning.oreilly.com/library/view/active-directory-administration/9781789806984/ (Luettu: 17.2.2022).

Bhardwaj, R. (2020) *Domain Controller vs Active Directory - Detailed Comparison*. Saatavilla: https://ipwithease.com/active-directory-vs-domain-controller/ (Luettu: 21.2.2022).

Brad, L. and Munteanu, A. (2012) *Cyber Security: Between Challenges and Prospects*.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3, pp. 77–101. Saatavilla: https://doi.org/10.1191/1478088706qp063oa.

Callaghan, P. (2020) *What Is the Difference Between Data Retention and Data Preservation?* Saatavilla: https://blog.pagefreezer.com/difference-data-retention-data-preservation (Luettu: 4.9.2022).

Centero Oy (2012) 'Pääsynhallintaa ryhmillä ja sen automatisointi', *Centero Oy*. Saatavilla: https://centero.fi/blogi/paasynhallintaa-ryhmilla-ja-sen-automatisointi/ (Luettu: 18.2.2022).

Clines, S. and Loughry, M. (2008) *Active Directory for Dummies*. Hoboken, UNITED STATES: John Wiley & Sons, Incorporated. Saatavilla: http://ebookcentral.proquest.com/lib/tampere/detail.action?docID=353374 (Luettu: 31.1.2022).

CSA (2012) *SecaaS Category 1 // Identity and Access Management*, *CSA*. Saatavilla: https://cloudsecurityalliance.org/artifacts/secaas-category-1-identity-and-access-management-implementation-guidance/ (Luettu: 1.3.2022).

Datta, A. and Thomas, H. (1999) 'The cube data model: a conceptual model and algebra for on-line analytical processing in data warehouses1A related paper introducing this model was presented at the Workshop on Information and Technology (WITS), Atlanta, GA, December 1997.1', *Decision Support Systems*, 27(3), pp. 289–301. Saatavilla: https://doi.org/10.1016/S0167-9236(99)00052-4.

Desmond, B. *et al.* (2013) *Active Directory, 5th Edition*. O'Reilly Media, Inc. Saatavilla: https://learning.oreilly.com/library/view/active-directory-5th/9781449361211/ (Luettu: 17.2.2022).

DNSstuff (2019) *The Ultimate Guide to Active Directory Best Practices - DNSstuff*, *Software Reviews, Opinions, and Tips - DNSstuff*. Saatavilla: https://www.dnsstuff.com/active-directory-best-practices (Luettu: 23.2.2022).

Fisher, C. (2018) 'Cloud versus On-Premise Computing', *American Journal of Industrial and Business Management*, 08(09), p. 1991. Saatavilla: https://doi.org/10.4236/ajibm.2018.89133.

Francis, D. (2021) *Mastering Active Directory - Third Edition*. Saatavilla: https://learning.oreilly.com/library/view/mastering-active-directory/9781801070393/ (Luettu: 16.2.2022).

George, A.M. (2021) *Top 12 FAQ - Microsoft Power Platform*. Saatavilla: https://www.linkedin.com/pulse/top-12-faq-microsoft-power-platform-ajith-mathew-george/ (Luettu: 28.2.2022).

Google Cloud (2019) *Patterns for using Active Directory in a hybrid environment | Cloud Architecture Center*, *Google Cloud*. Saatavilla: https://cloud.google.com/architecture/patterns-for-using-active-directory-in-a-hybrid-environment (Luettu: 24.2.2022).

Guimonet, P. (2019) 'A Beginner's Guide to Microsoft PowerApps', *AvePoint Blog*. Saatavilla: https://www.avepoint.com/blog/office-365/microsoft-powerapps/ (Luettu: 24.2.2022).

Haber, M.J. and Rolls, D. (2019) *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. Saatavilla: https://learning.oreilly.com/library/view/identity-attack-vectors/9781484251652/html/480623_1_En_3_Chapter.xhtml (Luettu: 22.2.2022).

Heimo, A., Juvonen, T. and Kurvinen, H. (2021) 'Opas muistitietohaastettelun tekemiseen'. Työväen historian ja perinteen tutkimuksen seura.

Hugos, M.H. and Hulitzky, D. (2010) *Business in the Cloud: What Every Business Needs to Know about Cloud Computing*. Hoboken, UNITED STATES: John Wiley & Sons, Incorporated. Saatavilla: http://ebookcentral.proquest.com/lib/tampere/detail.action?docID=624431 (Luettu: 28.2.2022).

ISO/IEC 27002 (2005) *ISO/IEC 27002:2005(en), Information technology — Security techniques — Code of practice for information security management*. Saatavilla: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-1:v1:en (Luettu: 25.2.2022).

Kabiru Hamza, M., Abubakar, H. and Danlami, Y.M. (2018) 'Identity and Access Management System: a Web-Based Approach for an Enterprise', *Path of Science*, 4(11), pp. 2001–2011. Saatavilla: https://doi.org/10.22178/pos.40-1.

Karnes, J. (2017) 'Microsoft PowerApps: What is it? What does it do? Is it easy to use?', *Centric Consulting*. Saatavilla: https://centricconsulting.com/blog/microsoft-powerapps-introduction_portal/ (Luettu: 24.2.2022).

Krasman, M. (2015) 'Three Must-Have Onboarding Elements for New and Relocated Employees', *Employment Relations Today*, 42(2), pp. 9–14. Saatavilla: https://doi.org/10.1002/ert.21493.

Lee, L. and Sawyer, R. (2019) 'IT General Controls Testing: Assessing the Effectiveness of User Access Management', *AIS Educator Journal*, 14(1), pp. 15–34. Saatavilla: https://doi.org/10.3194/1935-8156-14.1.15.

Lin, J. *et al.* (2010) 'VegaWarden: A Uniform User Management System for Cloud Applications', in *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*. *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*, pp. 457–464. Saatavilla: https://doi.org/10.1109/NAS.2010.34.

Microsoft (2018) *What Is Active Directory Lightweight Directory Services*. Saatavilla: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/adam/what-is-active-directory-lightweight-directory-services (Luettu: 21.2.2022).

Microsoft (2021a) *Active Directory Security Groups*. Saatavilla: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups (Luettu: 13.2.2022).

Microsoft (2021b) *Add or remove a group from another group*. Saatavilla: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal (Luettu: 23.2.2022).

Microsoft (2021c) *What is hybrid identity with Azure Active Directory?* Saatavilla: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity.

Microsoft (2022a) *Active Directory Domain Services Overview*. Saatavilla: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (Luettu: 13.2.2022).

Microsoft (2022b) *Azure Bot Service – Conversational AI application | Microsoft Azure*. Saatavilla: https://azure.microsoft.com/en-gb/services/bot-services/ (Luettu: 14.4.2022).

Microsoft (2022c) *Azure identity & access security best practices*. Saatavilla: https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices (Luettu: 16.2.2022).

Microsoft (2022d) *LUIS (Language Understanding) - Cognitive Services - Microsoft*. Saatavilla: https://www.luis.ai/ (Luettu: 14.4.2022).

Microsoft (2022e) *Mikä Power BI on? - Power BI*. Saatavilla: https://docs.microsoft.com/fi-fi/power-bi/fundamentals/power-bi-overview (Luettu: 24.2.2022).

Microsoft (2022f) *Power Appsin kuvaus*. Saatavilla: https://docs.microsoft.com/fi-fi/powerapps/powerapps-overview (Luettu: 24.2.2022).

Microsoft (2022g) *Power Automate -dokumentaatio - Power Automate*. Saatavilla: https://docs.microsoft.com/fi-fi/power-automate/ (Luettu: 14.4.2022).

Microsoft (2022h) *What is Azure Active Directory?* Saatavilla: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis (Luettu: 18.2.2022).

Microsoft (2022i) *What is IaaS? Infrastructure as a Service | Microsoft Azure*. Saatavilla: https://azure.microsoft.com/en-us/overview/what-is-iaas/ (Luettu: 28.2.2022).

Miyachi, C. (2018) 'What is "Cloud"? It is time to update the NIST definition?', *IEEE Cloud Computing*, 5(3), pp. 6–11. Saatavilla: https://doi.org/10.1109/MCC.2018.032591611.

Mohammed, I.A. (2015) 'The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study', *SSRN Electronic Journal*, 3, pp. 668–671.

Mohammed, I.A. (2017) 'Systematic review of Identity Access Management in information security', *SSRN Electronic Journal*, 4, pp. 1–7.

Mohammed, I.A. (2019a) ‘Cloud Identity and Access Management - a Model Proposal’, *SSRN Electronic Journal*, 6, pp. 1–8.

Mohammed, I.A. (2019b) ‘Cloud identity and access management - A model proposal’, *SSRN Electronic Journal*, 6, pp. 1–8.

Mohammed, I.A. (2021) ‘Identity Management Capability Powered by Artificial Intelligence to Transform the Way User Access Privileges Are Managed, Monitored and Controlled’, *SSRN Electronic Journal*, 9, pp. 4719–4723.

Mokych, A. and Semeniak, E. (2020) *Explaining Cloud Computing Models: SaaS, PaaS, and IaaS*, *Apriorit*. Saatavilla: https://www.apriorit.com/white-papers/405-saas-iaas-paas (Luettu: 28.2.2022).

Naik Bukht, T.F. *et al.* (2020) ‘Importance of Cyber security and its sub-domains’, *Journal of Information and Computational Science*, 10, pp. 473–485.

Nowell, L.S. *et al.* (2017) ‘Thematic Analysis: Striving to Meet the Trustworthiness Criteria’, *International Journal of Qualitative Methods*, 16(1), p. 1609406917733847. Saatavilla: https://doi.org/10.1177/1609406917733847.

OLAP.com (no date) *What is OLAP cube? Definition of OLAP cube*, *OLAP.com*. Saatavilla: https://olap.com/learn-bi-olap/olap-bi-definitions/olap-cube/ (Luettu: 24.2.2022).

R, S. (2019) ‘Azure AD Automation Bot’. Saatavilla: http://localhost:8080/xmlui/handle/123456789/10754 (Luettu: 14.4.2022).

Rani, D. and Ranja, R.K. (2014) ‘A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing’, *International Journal of Advanced Research in Computer Science and Software Engineering* [Preprint].

Rathod, B. (2019) ‘Role of Identity and Access Management (IAM) in Cyber Security’, *Cyber Defense Magazine*. Saatavilla: https://www.cyberdefensemagazine.com/role-of-identity-and-access-management-iam-in-cyber-security/ (Luettu: 1.3.2022).

RedHat (2020) *What is provisioning?*, *RedHat*. Saatavilla: https://www.redhat.com/en/topics/automation/what-is-provisioning (Luettu: 15.2.2022).

Rongstad, K. and Zhang, R. (2021) ‘Enterprise network security from cloud computing perspective’, *Issues In Information Systems* [Preprint]. Saatavilla: https://doi.org/10.48009/3_iis_2021_120-126.

Rubenstein, B. (2012) *Active Directory domain (AD domain)*, *SearchWindowsServer*. Saatavilla: https://www.techtarget.com/searchwindowsserver/definition/Active-Directory-domain-AD-domain (Luettu: 13.2.2022).

Sahay, R. (2020) *Microsoft Azure Architect Technologies Study Companion: Hands-on Preparation and Practice for Exam AZ-300 and AZ-303*. Saatavilla: https://learning.oreilly.com/library/view/microsoft-azure-architect/9781484262009/html/500070_1_En_10_Chapter.xhtml (Luettu: 21.2.2022).

Salminen, A. (2011) ‘Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin.’ Vaasan Yliopisto.

Saunders, M., Lewis, P. and Thornhill, A. (2016) *Research Methods for Business Students*. Seventh edition.

Shea, S. (2014) *What is identity governance? - Definition from WhatIs.com*, *SearchSecurity*. Saatavilla: https://www.techtarget.com/searchsecurity/definition/identity-governance (Luettu: 28.2.2022).

S'Heeren, N. (2020) 'The Impact of Artificial Intelligence on Identity & Access Management', *Elimity | Library*, 3 January. Saatavilla: https://library.elimity.com/insights/the-impact-of-artificial-intelligence-on-identity-access-management/ (Luettu: 18.4.2022).

Soh, J. *et al.* (2020) *Microsoft Azure: Planning, Deploying, and Managing the Cloud*. Saatavilla: https://learning.oreilly.com/library/view/microsoft-azure-planning/9781484259580/html/336094_2_En_7_Chapter.xhtml (Luettu: 16.2.2022).

von Solms, B. and von Solms, R. (2018) 'Cybersecurity and information security – what goes where?', *Information and Computer Security*, 26(1), pp. 2–9. Saatavilla: http://dx.doi.org/10.1108/ICS-04-2017-0025.

von Solms, R. and van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security*, 38, pp. 97–102. Saatavilla: https://doi.org/10.1016/j.cose.2013.04.004.

Taylor, D. (2020) *What is OLAP? Cube, Analytical Operations in Data Warehouse*. Saatavilla: https://www.guru99.com/online-analytical-processing.html (Luettu: 24.2.2022).

Torres-Corral, A. (2021) *On-Premises vs. Cloud: What's the Difference?*, *Alert Logic*. Saatavilla: https://www.alertlogic.com/blog/on-premises-vs-cloud-whats-the-difference/ (Luettu: 28.2.2022).

Trnka, M., Cerny, T. and Stickney, N. (2018) 'Survey of Authentication and Authorization for the Internet of Things', *Security and Communication Networks*, 2018, p. e4351603. Saatavilla: https://doi.org/10.1155/2018/4351603.

Vaismoradi, M., Turunen, H. and Bondas, T. (2013) 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', *Nursing & Health Sciences*, 15(3), pp. 398–405. Saatavilla: https://doi.org/10.1111/nhs.12048.

Windows Active Directory (2021) 'Active Directory Nested Groups Explained', *Windows Active Directory*. Saatavilla: https://www.windows-active-directory.com/nesting-groups-in-active-directory.html (Luettu: 23.2.2022).

Wright, N. (2019) *Everything you ever wanted to know about Microsoft Power BI*, *Nigel Frank*. Saatavilla: https://www.nigelfrank.com/insights/everything-you-ever-wanted-to-know-about-microsoft-power-bi (Luettu: 24.2.2022).

Yang, Y. *et al.* (2014) 'An Identity and Access Management Architecture in Cloud', in *2014 Seventh International Symposium on Computational Intelligence and Design*. *2014 Seventh International Symposium on Computational Intelligence and Design*, pp. 200–203. Saatavilla: https://doi.org/10.1109/ISCID.2014.221.

LIITE A: HAASTATTELU KYSYMYSRUNKO

Haastateltavan taustatiedot

Tehtävä, organisaation tiedot, tehtävänimike, kerro muutamalla sanalla työtehtävistäsi?

Haastateltavan kokemukset käyttäjähallinnasta

Millaisissa käyttäjähallinta projekteissa olet ollut mukana?
Mikä on yleisin ongelma käyttäjähallinnan suhteen, mihin olet törmännyt?

Käyttäjähallinta yleisesti

Mitä on IAM? (Identity and Access Management)
Mitä käyttäjähallintaprosessiin kuuluu?
Mitä hyötyä/ haasteita käyttäjähallinnan yrityksille?

Käyttäjähallinta prosessi

Mitä haasteita on ilmennyt konsernin tasoisen yrityksen käyttäjähallinnan toteuttamisessa?
Mitä tulee huomioida, kun suunnitellaan uutta käyttäjähallinta prosessia/mallia?

Käyttäjähallinnan vaikutus tietoturvallisuuteen

Miten käyttäjähallinta vaikuttaa tietoturvallisuuteen?

Azure AD

Mitä hyötyjä/haittaa Azure AD:sta on käyttäjähallinnassa?

Käyttäjältä oikeuksien poistaminen

Onko jotain helppoa tapaa järjestää käyttäjien poistaminen, kun käyttäjä ei enää tarvitse oikeuksia siirtyessään konsernin sisällä?

Käyttäjähallinnan automatisointi

Mitä käyttäjähallintaprosessin vaiheita yleensä automatisoidaan?
- Mitä hyötyjä automatisoinnissa on?
- Mitä riskejä automatisoinnissa on?